Lagrådsremiss

De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 16 december 2010

Beatrice Ask

Ari Soppela
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Hemlig teleavlyssning och hemlig teleövervakning ska i fortsättningen benämnas hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

Bestämmelserna i lagen (2003:389) om elektronisk kommunikation och offentlighets- och sekretesslagen (2009:400) om de brottsbekämpande myndigheternas tillgång till uppgifter som angår särskilda elektroniska meddelanden upphävs. Dessa ersätts dels av bestämmelser i rättegångsbalken som under vissa förutsättningar möjliggör hemlig övervakning av elektronisk kommunikation i en förundersökning även om det inte finns någon som skäligen är misstänkt för brott, dels av bestämmelser i en ny lag om inhämtning av sådana uppgifter i underrättelseverksamhet. Syftet bakom dessa förändringar är att stärka rättssäkerheten och integritetsskyddet vid inhämtning av övervakningsuppgifter.

Tillstånd till hemlig övervakning av elektronisk kommunikation ska även fortsättningsvis lämnas av allmän domstol. Det införs dock en möjlighet för åklagare att i vissa brådskande fall fatta interimistiska beslut. I polisens och Tullverkets underrättelseverksamhet ska beslut om inhämtning fattas av myndigheten. Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn över inhämtningen. För att uppgifter som har inhämtats i underrättelseverksamhet ska få användas i en förundersökning krävs ett tillstånd till hemlig övervakning av elektronisk kommunikation.

Vidare införs en möjlighet att inhämta lokaliseringsuppgifter avseende en viss elektronisk kommunikationsutrustning som är påslagen men som vid det aktuella tillfället inte används eller har använts för kommunikation. Det blir också möjligt att inhämta uppgift om vilka sådana kommunikationsutrustningar som har funnits i ett visst område. De brottsutredande myndigheterna ges dessutom en något utökad tillgång till abonnemangsuppgifter. Slutligen införs utvidgade möjligheter för polisen att få tillgång till bl.a. lokaliseringsuppgifter för efterforskning av försvunna personer.

Förslagen föreslås träda i kraft den 1 juli 2011.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,
2. lag (0000:00) om ändring i lag (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,
3. lag om ändring i brottsbalken,
4. lag om ändring i rättegångsbalken,
5. lag om ändring i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.,
6. lag om ändring i lagen (1991:572) om särskild utlänningskontroll,
7. lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål,
8. lag om ändring i lagen (2003:389) om elektronisk kommunikation,
9. lag om ändring i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott,
10. lag om ändring i lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott,
11. lag om ändring i offentlighets- och sekretesslagen (2009:400).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Härigenom föreskrivs följande.

1 § Denna lag innehåller bestämmelser om befogenhet för polismyndighet och Tullverket att i underrättelseverksamhet i hemlighet hämta in uppgifter om elektronisk kommunikation eller om lokaliseringen av elektronisk kommunikationsutrustning från den som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

2 § Inhämtning får avse uppgifter om

1. meddelanden som i ett elektroniskt kommunikationsnät har överförts till eller från ett telefonnummer eller annan adress,
2. vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller
3. i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

3 § Uppgifter får hämtas in om omständigheterna är sådana att

1. åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, och
2. skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

4 § Uppgifter får också, under de förutsättningar som anges i 3 § 2, hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

1. sabotage enligt 13 kap. 4 § brottsbalken,
2. kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,

4. spionerі, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet, grovt brott, enligt 19 kap. 5, 8 eller 10 § tredje stycket brottsbalken, eller

5. grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.

5 § Beslut om inhämtning av uppgifter fattas av myndigheten. Myndighetschefen får delegera rätten att fatta beslut om inhämtning till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs.

6 § I ett beslut om inhämtning av uppgifter ska det anges vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet avser. Tiden får inte bestämmas längre än nödvändigt och får, när det gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.

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

7 § Säkerhets- och integritetsskyddsnämnden ska underrättas om ett beslut om inhämtning av uppgifter enligt denna lag. Underrättelsen ska lämnas senast en månad efter det att ärendet om inhämtning avslutades.

8 § Om det vid inhämtning av uppgifter enligt denna lag har kommit fram uppgifter om annan brottslig verksamhet än som omfattas av beslutet om inhämtning, får uppgifterna användas för att förhindra brott.

9 § Uppgifter som har kommit fram vid inhämtning enligt denna lag får användas i en förundersökning endast efter tillstånd till hemlig övervakning av elektronisk kommunikation. Utan ett sådant tillstånd får dock inhämtade uppgifter ligga till grund för att inleda en förundersökning.

10 § Upptеckningar av uppgifter ska granskas snarast möjligt.

Upptеckningar ska, i de delar de är av betydelse för att förebygga, förhindra eller upptäcka brottslig verksamhet som omfattas av beslutet om inhämtning eller för att förhindra annat brott, bevaras så länge det behövs för något av dessa syften. De ska därefter förstöras.

Det som sägs i andra stycket hindrar inte att brottsbekämpande myndigheter behandlar uppgifter från upptеckningar i enlighet med vad som är särskilt föreskrivet i lag.

Denna lag träder i kraft den 1 juli 2011.

2.2 Förslag till lag (0000:00) om ändring i lag (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Härigenom föreskrivs att 4 § lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska upphöra att gälla vid utgången av december 2012.

2.3 Förslag till lag om ändring i brottsbalken

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

Nuvarande lydelse	*Föreslagen lydelse*
	4 kap.
	8 §[1]
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 *i ett elektroniskt kommunikationsnät,* döms för *brytande av post- eller telehemlighet* till böter eller fängelse i högst två år.

Denna lag träder i kraft den 1 juli 2011.

[1] Senaste lydelse 1993:601.

2.4 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs i fråga om rättegångsbalken

dels att 27 kap. 18–20, 21–26, 28, 31 och 32 §§ och rubriken till 27 kap. ska ha följande lydelse,

dels att det i lagen ska införas en ny paragraf, 27 kap. 21 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
27 kap.	
Om beslag, *hemlig teleavlyssning* m.m	**Om beslag, *hemlig avlyssning av elektronisk kommunikation* m.m.**
18 §[2]	
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 *avlyssning av elektronisk kommunikation* innebär att *meddelanden,* som *i ett elektroniskt kommunikationsnät överförs* eller har *överförts* till eller från ett telefonnummer eller annan *adress,* i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.
Hemlig *teleavlyssning* får användas vid förundersökning *angående*	Hemlig *avlyssning av elektronisk kommunikation* får användas vid förundersökning *som avser*
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 till hemlig avlyssning av elektronisk kommunikation ger också rätt att vidta sådana åtgärder som anges i 19 §.

[2] Senaste lydelse 2003:1146.

19 §[3]

Hemlig *teleövervakning* innebär att uppgifter i hemlighet hämtas in om *telemeddelanden som befordras eller har befordrats till eller från en viss teleadress eller att sådana meddelanden hindras från att nå fram.*

Hemlig *övervakning av elektronisk kommunikation* innebär att uppgifter i hemlighet hämtas in om

1. meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress,

2. vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller

3. i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

Genom hemlig övervakning av elektronisk kommunikation får sådana meddelanden som avses i första stycket 1 även hindras från att nå fram.

Hemlig *teleövervakning* får användas vid förundersökning *angående*

Hemlig *övervakning av elektronisk kommunikation* får användas vid förundersökning *som avser*

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

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

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

I fall som avses i 20 § andra stycket får hemlig övervakning av elektronisk kommunikation dock användas endast vid förundersökning som avser brott som kan föranleda hemlig avlyssning av elektronisk kommunikation enligt 18 § andra stycket.

20 §[4]

Hemlig *teleavlyssning* och

Hemlig *avlyssning av*

[3] Senaste lydelse 2003:1146.
[4] Senaste lydelse 2003:1146.

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

1. *en teleadress* som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte, eller

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

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

elektronisk kommunikation och hemlig *övervakning av elektronisk kommunikation* får, *om inte annat följer av andra stycket, endast ske* om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får endast avse

1. *ett telefonnummer eller annan adress eller en viss elektronisk kommunikations-utrustning* 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. *ett telefonnummer eller annan adress eller en viss elektronisk kommunikations-utrustning* som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Hemlig övervakning av elektronisk kommunikation får, utöver vad som anges i första stycket, ske i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Övervakning som innebär att uppgifter hämtas in om meddelanden får dock endast avse förfluten tid.

Avlyssning eller övervakning får inte avse meddelanden som endast överförs eller har överförts 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 §[5]

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

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

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

Frågor om hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* och hemlig kameraövervakning prövas av rätten på ansökan av åklagaren.

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

I ett tillstånd till hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* ska det anges *vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område* tillståndet avser. Det ska vidare särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga *elektroniska kommunikationsnät.*

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

21 a §

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

Har åklagaren gett ett sådant tillstånd ska han eller hon genast göra en skriftlig anmälan om åtgärden till rätten. I anmälan ska skälen för åtgärden anges. Rätten

[5] Senaste lydelse 2008:855.

	ska skyndsamt pröva om det finns skäl för åtgärden. Finner rätten att det inte finns sådana skäl, ska den upphäva beslutet. *Har åklagarens beslut verkställts innan rätten gjort en sådan prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Finner rätten att det saknats sådana skäl får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av övervakningen.*
22 §[6]	
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.	Hemlig *avlyssning av elektronisk kommunikation* får *inte* ske av telefonsamtal eller andra *meddelanden* mellan den misstänkte och hans *eller hennes* försvarare. Om det framkommer under avlyssningen att det är fråga om ett sådant samtal eller meddelande, *ska* avlyssningen avbrytas.
Upptagningar och uppteckningar *skall*, i den mån de omfattas av förbudet, omedelbart förstöras.	Upptagningar och uppteckningar *ska*, i den mån de omfattas av förbudet, omedelbart förstöras.
23 §[7]	
Om det inte längre finns skäl för ett beslut om hemlig *teleavlyssning,* hemlig *teleövervakning* eller hemlig kameraövervakning, ska åklagaren eller rätten omedelbart häva beslutet.	Om det inte längre finns skäl för ett beslut om hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning, ska åklagaren eller rätten omedelbart häva beslutet.
23 a §[8]	
Om det vid hemlig *teleavlyssning,* hemlig *teleövervakning* eller hemlig kameraövervakning har kommit fram uppgifter om ett annat brott	Om det vid hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning har kommit

[6] Senaste lydelse 1989:650.
[7] Senaste lydelse 2008:855.
[8] Senaste lydelse 2008:855.

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	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 §[9]

En upptagning eller uppteckning som har gjorts vid hemlig *teleavlyssning* eller hemlig *teleövervakning* eller en upptagning som har gjorts vid hemlig kameraövervakning ska granskas snarast möjligt. I fråga om sådan granskning tillämpas 12 § första stycket.	En upptagning eller uppteckning som har gjorts vid hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* eller en upptagning som har gjorts vid hemlig kameraövervakning ska granskas snarast möjligt. I fråga om sådan granskning tillämpas 12 § första stycket.
Upptagningar och uppteckningar från hemlig *teleavlyssning* eller hemlig *teleövervakning* ska, i de delar de är av betydelse från brottsutredningssynpunkt, bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I de delar upptagningarna och uppteckningarna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott. De ska därefter förstöras.	Upptagningar och uppteckningar från hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* ska, i de delar de är av betydelse från brottsutredningssynpunkt, bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I de delar upptagningarna och uppteckningarna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott. De ska därefter förstöras.

Upptagningar från hemlig kameraövervakning som saknar betydelse från brottsutredningssynpunkt ska förstöras omedelbart efter det att de har granskats. I de delar upptagningarna är av betydelse från brottsutredningssynpunkt ska de bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I

[9] Senaste lydelse 2008:855.

de delar upptagningarna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott. De ska därefter omedelbart förstöras.

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

Lydelse enligt prop. 2010/11:46	*Föreslagen lydelse*
25 §	
Har rätten lämnat tillstånd till hemlig teleavlyssning eller hemlig teleövervakning, får de tekniska hjälpmedel som behövs för *avlyssningen eller övervakningen* användas.	*När tillstånd till hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation har lämnats,* får de tekniska hjälpmedel som behövs för *åtgärden* användas.
I 6 kap. lagen (2003:389) om elektronisk kommunikation finns bestämmelser om *hemlig teleavlyssning* och *hemlig teleövervakning* som gäller för den som driver verksamhet som avses i den lagen.	I 6 kap. lagen (2003:389) om elektronisk kommunikation finns bestämmelser om hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation* som gäller för den som driver verksamhet som avses i den lagen.

Nuvarande lydelse	*Föreslagen lydelse*
26 §[10]	
Offentliga ombud ska bevaka enskildas integritetsintressen i ärenden hos domstol om hemlig *teleavlyssning* och hemlig kameraövervakning.	Offentliga ombud ska bevaka enskildas integritetsintressen i ärenden hos domstol om hemlig *avlyssning av elektronisk kommunikation* och hemlig kameraövervakning.

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 §[11]	
När en ansökan om hemlig *teleavlyssning* eller hemlig kameraövervakning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde.	När en ansökan om hemlig *avlyssning av elektronisk kommunikation* eller hemlig kameraövervakning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i

[10] Senaste lydelse 2008:855.
[11] Senaste lydelse 2008:855.

Vid sammanträdet ska åklagaren och det offentliga ombudet närvara.	ärendet och hålla ett sammanträde. Vid sammanträdet ska 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.

31 §[12]

Den som är eller har varit misstänkt för brott ska, om inte annat följer av 33 §, underrättas om hemlig *teleavlyssning,* hemlig *teleövervakning* eller hemlig kameraövervakning som han eller hon har utsatts för. Om *teleavlyssning eller teleövervakning* har avsett *en teleadress* som innehas av någon annan än den misstänkte, ska, om inte annat följer av 33 §, även innehavaren *av teleadressen* underrättas. Om kameraövervakning har avsett en plats som innehas av någon annan än den misstänkte och som allmänheten inte har tillträde till, ska, om inte annat följer av 33 §, även innehavaren av platsen underrättas.	Den som är eller har varit misstänkt för brott ska, om inte annat följer av 33 §, underrättas om hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning som han eller hon har utsatts för. Om *avlyssning* eller *övervakning av elektronisk kommunikation* har avsett *ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning* som innehas av någon annan än den misstänkte, ska, om inte annat följer av 33 § *eller inhämtning har skett med stöd av 20 § andra stycket och integritetsintrånget för den enskilde kan antas vara ringa*, även innehavaren underrättas. Om kameraövervakning har avsett en plats som innehas av någon annan än den misstänkte och som allmänheten inte har tillträde till, ska, om inte annat följer av 33 §, även innehavaren av platsen underrättas.

En underrättelse ska lämnas så snart det kan ske utan men för utredningen, dock senast en månad efter det att förundersökningen avslutades.

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

[12] Senaste lydelse 2008:855.

32 §[13]

En underrättelse enligt 31 § ska innehålla uppgift om vilket tvångsmedel som har använts och när det har skett. Den som är eller har varit misstänkt för brott ska få uppgift om vilken brottsmisstanke som har legat till grund för åtgärden eller som åtgärden har föranlett. Den som inte är eller har varit misstänkt för brott ska få uppgift om detta.

En underrättelse om hemlig *teleavlyssning* eller hemlig *teleövervakning* ska även innehålla uppgift om *vilken teleadress* som avlyssningen eller övervakningen har avsett. En underrättelse om hemlig kameraövervakning ska även innehålla uppgift om platsen för åtgärden.

En underrättelse om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* ska även innehålla uppgift om *vilket telefonnummer eller annan adress eller vilken elektronisk kommunikationsutrustning* som avlyssningen eller övervakningen har avsett. En underrättelse om hemlig kameraövervakning ska även innehålla uppgift om platsen för åtgärden.

Denna lag träder i kraft den 1 juli 2011.

[13] Senaste lydelse 2008:855.

2.5 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. ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
28 §[1]	
Kan det befaras att inhämtande av rättens tillstånd till hemlig *teleavlyssning*, hemlig *teleövervakning* eller hemlig kameraövervakning enligt 27 kap. 18, 19 eller 20 a § rättegångsbalken, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, eller hemlig rumsavlyssning enligt lagen (2007:978) om hemlig rumsavlyssning 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 ska göras hos den som har fattat beslutet. Denne ska pröva beslagsfrågan.	Kan det befaras att inhämtande av rättens tillstånd till hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning enligt 27 kap. 18, 19 eller 20 a § rättegångsbalken, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, eller hemlig rumsavlyssning enligt lagen (2007:978) om hemlig rumsavlyssning 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 ska göras hos den som har fattat beslutet. Denne ska pröva beslagsfrågan.

Om undersökningsledaren eller åklagaren har meddelat ett beslut med stöd av första stycket, ska det genast anmälas hos rätten. Anmälan ska vara skriftlig och innehålla skälen för beslutet. Rätten ska pröva ärendet snabbt. Anser rätten att beslutet inte bör bestå, ska det upphävas.

Denna lag träder i kraft den 1 juli 2011.

[1] Senaste lydelse 2008:856.

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

Härigenom föreskrivs att 20, 21 a och 22 §§ lagen (1991:572) om särkskild utlänningskontroll ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
20 §[1]	
För ett sådant ändamål som avses i 19 § första stycket kan rätten, om det finns synnerliga skäl, meddela Säkerhetspolisen 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 Säkerhetspolisen eller en polismyndighet tillstånd enligt 27 kap. rättegångsbalken till hemlig *avlyssning av elektronisk kommunikation* eller, om det är tillräckligt, hemlig *övervakning av elektronisk kommunikation*.
Rätten kan för ett sådant ändamål som avses i 19 § första stycket, om det finns synnerliga skäl, även meddela Säkerhetspolisen 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.	Rätten kan för ett sådant ändamål som avses i 19 § första stycket, om det finns synnerliga skäl, även meddela Säkerhetspolisen 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 *eller henne* 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	I det tillstånd som avses i andra stycket kan rätten förordna att en försändelse som avses i tillståndet och som ankommer till ett befordringsföretag, *ska* hållas kvar till dess den närmare undersökts, öppnats eller granskats. Förordnandet *ska* innehålla underrättelse om att meddelande om åtgärden inte får lämnas till avsändaren, mottagaren eller någon annan, utan tillstånd av den

[1] Senaste lydelse 2005:720.

den som har begärt åtgärden.	som har begärt åtgärden.

21 a §[2]

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 hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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

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 §[3]

En upptagning eller uppteckning som har gjorts vid hemlig *teleavlyssning* ska granskas snarast möjligt. Granskningen får utföras endast av rätten, Säkerhetspolisen, en polismyndighet eller en åklagare.	En upptagning eller uppteckning som har gjorts vid hemlig *avlyssning av elektronisk kommunikation* ska granskas snarast möjligt. Granskningen får utföras endast av rätten, Säkerhetspolisen, en polismyndighet eller en åklagare.

Om upptagningen eller uppteckningen innehåller något som inte är av betydelse för det ändamål som har föranlett avlyssningen, ska 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 ska dock 27 kap. 24 § andra och fjärde styckena rättegångsbalken 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, Säkerhetspolisen, en polismyndighet eller en åklagare. En sådan handling ska undersökas snarast möjligt. När undersökningen har slutförts, ska 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.

[2] Senaste lydelse 2005:506.
[3] Senaste lydelse 2009:1545.

Denna lag träder i kraft den 1 juli 2011.

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

Härigenom föreskrivs att 1 kap. 2 § och 4 kap. 25–26 c §§ samt rubrikerna närmast före 4 kap. 25–25 b §§, 26 §, 26 a § och 26 c § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
2 §[1]	
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. hemlig *teleavlyssning* och hemlig *teleövervakning,*	6. hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation,*
7. tekniskt bistånd med hemlig *teleavlyssning* och hemlig *teleövervakning,*	7. tekniskt bistånd med hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation,*
8. tillstånd till gränsöverskridande hemlig *teleavlyssning* och hemlig *teleövervakning*,	8. tillstånd till gränsöverskridande hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation,*
9. hemlig kameraövervakning,	
10. hemlig rumsavlyssning,	
11. överförande av frihetsberövade för förhör m.m., och	
12. 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.

[1] Senaste lydelse 2007:982.

4 kap.

Rättslig hjälp och tekniskt bistånd med hemlig *teleavlyssning* och hemlig *teleövervakning*	**Rättslig hjälp och tekniskt bistånd med hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation***
Rättslig hjälp i Sverige med hemlig teleavlyssning och hemlig teleövervakning	*Rättslig hjälp i Sverige med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation*
25 §[2]	
En ansökan om hemlig *teleavlyssning* eller hemlig *teleövervakning* av någon som befinner sig i Sverige handläggs av åklagare. Av ansökan ska det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd till åtgärden.	En ansökan om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* av någon som befinner sig i Sverige handläggs av åklagare. Av ansökan ska det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd till åtgärden *eller, när så får ske, själv besluta om 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.	Upptagningar och uppteckningar behöver inte granskas enligt 27 kap. 24 § rättegångsbalken. *Om åklagaren har fattat beslut enligt första stycket, ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om hemlig övervakning av elektronisk kommunikation.* 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] Senaste lydelse 2009:487.

I fråga om underrättelse till en enskild enligt 27 kap. 31–33 §§ rättegångsbalken ska bestämmelserna i 27 kap. 31 § andra stycket och 33 § andra och tredje styckena samma balk inte tillämpas. Underrättelse ska lämnas så snart det kan ske efter det att åtgärden enligt första stycket har avslutats. Underrättelsen ska, utöver vad som följer av 27 kap. 33 § första stycket rättegångsbalken, skjutas upp om sekretess gäller enligt 18 kap. 17 § offentlighets- och sekretesslagen (2009:400). Om det på grund av sekretess inte har kunnat lämnas någon underrättelse inom ett år från det att åtgärden avslutades, får underrättelsen underlåtas. Underrättelse ska inte lämnas om utredningen gäller brott som motsvarar brott som anges i 27 kap. 33 § tredje stycket rättegångsbalken.

Omedelbar överföring av telemeddelanden eller uppgifter om telemeddelanden från Sverige till den ansökande staten	*Omedelbar överföring av meddelanden eller uppgifter om meddelanden från Sverige till den ansökande staten*
25 a §[3]	
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 och bestämmelserna i 27 kap. 31–33 §§ rättegångsbalken ska inte tillämpas.	Rättens beslut enligt 25 § att tillåta hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* får verkställas genom omedelbar överföring av *meddelanden* eller uppgifter om *meddelanden* 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 och bestämmelserna i 27 kap. 31–33 §§ rättegångsbalken ska inte tillämpas.
Tekniskt bistånd i Sverige med hemlig teleavlyssning och hemlig teleövervakning	*Tekniskt bistånd i Sverige med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation*

[3] Senaste lydelse 2007:982.

25 b §[4]

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 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,

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

3. omedelbar överföring av *telemeddelanden* eller uppgifter om *telemeddelanden* 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,

Tekniskt bistånd med hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* i form av omedelbar överföring av *meddelanden* eller uppgifter om *meddelanden* 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 hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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 *ska* det framgå under vilken tid åtgärden önskas. Ansökan *ska* vidare innehålla sådana uppgifter som behövs för att åtgärden *ska* kunna genomföras. Om den person som ansökan avser inte befinner sig i den ansökande staten, *ska* det också framgå av ansökan att ett sådant tillstånd som avses i 26 a § har lämnats av den stat där personen finns.

Ansökan *ska* prövas av åklagare. För beslutet om tekniskt bistånd tillämpas bestämmelserna i 27 kap. 18 § första *och tredje styckena,* 19 § första stycket, 20 §

[4] Senaste lydelse 2005:491.

21 § andra och tredje styckena samt 23 § rättegångsbalken.	*tredje* 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 §[5]	
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 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.	Om en stat har begärt tekniskt bistånd enligt 25 b § men omedelbar överföring inte kan ske, *ska* åklagaren ge den ansökande staten tillfälle att få ansökan behandlad som en ansökan enligt 25 §. Prövningen av rättslig hjälp med hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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, *ska* 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 hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation*
26 §[6]	
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.	Åklagare får ansöka hos en utländsk myndighet om rättslig hjälp eller tekniskt bistånd med hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* av någon som befinner sig i en annan stat eller i Sverige.
Om den andra staten kräver att ansökan först ska prövas av	Om den andra staten kräver att ansökan först ska prövas av

[5] Senaste lydelse 2005:491.
[6] Senaste lydelse 2007:982.

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.

domstol i Sverige, får rätten på begäran av svensk åklagare pröva frågan om att tillåta den hemliga *avlyssningen* eller hemliga *övervakningen* som ansökan enligt första stycket avser.

Av ansökan enligt första stycket ska det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Om den andra staten kräver ett tillstånd enligt andra stycket, ska 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, ska det av ansökan framgå att ett sådant tillstånd som avses i 26 c § har lämnats av den stat där personen finns.

Om tillstånd lämnas enligt andra stycket, ska bestämmelserna om underrättelse till enskild i 27 kap. 31–33 §§ rättegångsbalken tillämpas endast när upptagning eller uppteckning av avlyssningen eller övervakningen sker i Sverige.

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

Tillstånd till gränsöverskridande hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation*

Tillstånd i Sverige till gränsöverskridande hemlig teleavlyssning och hemlig teleövervakning

Tillstånd i Sverige till gränsöverskridande hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation

26 a §[7]

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

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 *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* av någon som befinner sig i Sverige. Ansökan handläggs av åklagare. Av ansökan *ska* det framgå under vilken tid åtgärden beräknas pågå. Ansökan *ska* också innehålla en

[7] Senaste lydelse 2005:491.

teleövervakning har meddelats i den ansökande staten.	bekräftelse på att ett beslut om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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.	Åklagaren *ska* genast pröva om det finns förutsättningar för hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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.	De förutsättningar som gäller enligt 27 kap. *18–20, 21 och 22* §§ rättegångsbalken *ska* tillämpas vid tillståndsprövningen. Rätten *ska* även tillämpa motsvarande förfarande som anges i 27 kap. 26 och 28–30 §§ samma balk. Tingsrättens beslut får inte överklagas.
26 b §[8]	
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.	Ett beslut enligt 26 a § *ska* 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 *ska* genast underrätta den ansökande staten när ett beslut enligt 26 a § har meddelats. Om tillstånd vägras, *ska* underrättelsen ange att *avlyssningen* eller *övervakningen* inte får ske eller omedelbart *ska* upphöra. I sådant fall *ska* 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	*Tillstånd från en annan stat till gränsöverskridande hemlig avlyssning av elektronisk*

[8] Senaste lydelse 2005:491.

teleövervakning	*kommunikation och hemlig övervakning av elektronisk kommunikation*
26 c §[9]	
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	Har beslut om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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* eller uppgifter om *meddelanden* som överförs 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 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.	Ansökan om tillstånd görs av åklagare. Av ansökan *ska* det framgå under vilken tid åtgärden beräknas pågå. Ansökan *ska* också innehålla en bekräftelse på att ett svenskt beslut om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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	Om beslut om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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, *ska* tillstånd från den andra staten sökas innan avlyssningen eller övervakningen påbörjas. Har avlyssningen eller övervakningen redan påbörjats i Sverige och vill åklagaren att

[9] Senaste lydelse 2005:491.

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 tillståndet.

avlyssningen eller övervakningen *ska* fortsätta i den andra staten, *ska* 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.

Denna lag träder i kraft den 1 juli 2011.

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

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

dels att 6 kap. 8, 19 och 21–23 §§ samt rubriken närmast före 6 kap. 19 § ska ha följande lydelse,

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

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
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 hemlig avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation*, tekniskt bistånd med *sådan avlyssning* eller *övervakning*, *inhämtning av uppgifter enligt lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,* eller
3. i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.	
	10 a §
	Lokaliseringsuppgifter som omfattas av beslut om inhämtning av uppgifter enligt 27 kap. rättegångsbalken eller lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, får behandlas utan hinder av bestämmelserna i 9–10 §§.

[1] Senaste lydelse 2005:493

Lydelse enligt prop. 2010/11:46	*Föreslagen lydelse*
	16 c §
Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2 *eller 3 eller* enligt 27 kap. 19 § rättegångsbalken.	Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2, 27 kap. 19 § rättegångsbalken *eller lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.*
Nuvarande lydelse	*Föreslagen lydelse*
Hemlig *teleavlyssning* m.m.	**Hemlig *avlyssning av elektronisk kommunikation* m.m.**
	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 *ska* bedrivas så att beslut om hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation* 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.	Innehållet i och uppgifter om avlyssnade eller övervakade *meddelanden ska* 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.

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,

2. angelägenhet som avser användning av hemlig *teleavlyssning* eller hemlig *teleövervakning* enligt 27 kap. 18 eller 19 § rättegångsbalken eller tekniskt bistånd med hemlig *teleavlyssning* eller med hemlig *teleövervakning* enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål, *och*	2. angelägenhet som avser användning av hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* enligt 27 kap. 18 eller 19 § rättegångsbalken eller tekniskt bistånd med hemlig *avlyssning av elektronisk kommunikation* eller med hemlig *övervakning av elektronisk kommunikation* enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål,
3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet.	3. angelägenhet som avser inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet,
	4. inhämtning av uppgifter enligt lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, och
	5. begäran om utlämnande enligt 22 § första stycket 2.
Lydelse enligt Justitieutskottets betänkande 2010/11:JuU2	*Föreslagen lydelse*

22 §

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

1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (2010:000), om myndigheten finner att det kan antas att

[2] Senaste lydelse 2008:719.

den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,

2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet, *om fängelse är föreskrivet för brottet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter,*	2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet,
3. uppgift som avses i 20 § första stycket 3 *och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år,*	3. uppgift som avses i 20 § första stycket *1 och* 3 *samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits 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 Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

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

6. uppgift som avses i 20 § första stycket 1 till polismyndighet, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten *ska* 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 ska kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och

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

Ersättning för att lämna ut uppgifter enligt första stycket 8 ska vara skälig med hänsyn till kostnaderna för utlämnandet.

Nuvarande lydelse	*Föreslagen lydelse*
	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 i ett elektroniskt kommunikationsnät* som inte är avsett för honom eller henne själv eller för allmänheten får inte obehörigen föra det vidare.

Denna lag träder i kraft den 1 juli 2011.

2.9 Förslag till lag om ändring i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott

Härigenom föreskrivs att 1, 2, 8, 9, 11, 13, 16 och 17 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 §[1]
Tillstånd till hemlig *teleavlyssning* enligt 27 kap. 18 § första stycket rättegångsbalken, hemlig *teleövervakning* enligt 27 kap. 19 § första stycket rättegångsbalken eller hemlig kameraövervakning enligt 27 kap. 20 a § första stycket rättegångsbalken får meddelas, om det med hänsyn till omständigheterna finns särskild anledning att anta att en person kommer att utöva brottslig verksamhet som innefattar	Tillstånd till hemlig *avlyssning av elektronisk kommunikation* enligt 27 kap. 18 § första stycket rättegångsbalken, hemlig *övervakning av elektronisk kommunikation* enligt 27 kap. 19 § första stycket rättegångsbalken eller hemlig kameraövervakning enligt 27 kap. 20 a § första stycket rättegångsbalken får meddelas, om det med hänsyn till omständigheterna finns särskild anledning att anta att en person kommer att utöva brottslig verksamhet som innefattar

1. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,
2. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,
4. högförräderi, krigsanstiftan, spionerі, grovt spionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet enligt 19 kap. 1, 2, 5, 6 eller 8 § eller 10 § tredje stycket brottsbalken,
5. terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott,

grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, eller

6. mord, dråp, grov misshandel, människorov eller olaga frihetsberövande enligt 3 kap. 1, 2 eller 6 § eller 4 kap. 1 § eller 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

[1] Senaste lydelse 2010:405.

2 §

Hemlig *teleavlyssning* och hemlig *teleövervakning* enligt 1 § får endast avse

1. *en teleadress* som under den tid tillståndet avser innehas eller har innehafts av den som avses i 1 § eller annars kan antas ha använts eller komma att användas av honom eller henne, eller

2. en *teleadress* som det finns synnerlig anledning att anta att den som avses i 1 § under den tid 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.

Hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation* enligt 1 § får endast avse

1. *ett telefonnummer eller annan adress eller en elektronisk kommunikationsutrustning* som under den tid tillståndet avser innehas eller har innehafts av den som avses i 1 § eller annars kan antas ha använts eller komma att användas av honom eller henne, eller

2. *ett telefonnummer eller annan adress eller en elektronisk kommunikationsutrustning* som det finns synnerlig anledning att anta att den som avses i 1 § under den tid tillståndet avser har kontaktat eller kommer att kontakta.

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

8 §

I ett beslut om tillstånd till tvångsmedel ska det anges

1. vilket eller vilka tvångsmedel som får användas,

2. vilken eller vilka av punkterna i 1 § 1–6 som ligger till grund för tillståndet, och

3. under vilken tid tillståndet gäller.

I ett beslut om tillstånd till hemlig *teleavlyssning* eller hemlig *teleövervakning* ska det, förutom de uppgifter som framgår av första stycket, anges

1. *vilken teleadress* tillståndet avser, och

I ett beslut om tillstånd till hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* ska det, förutom de uppgifter som framgår av första stycket, anges

1. *vilket telefonnummer eller annan adress eller vilken elektronisk kommunikationsutrustning* tillståndet avser, och

2. om åtgärden får verkställas utanför allmänt tillgängliga *telenät*.	2. om åtgärden får verkställas utanför allmänt tillgängliga *elektroniska kommunikationsnät.*

I ett beslut om tillstånd till hemlig kameraövervakning ska, förutom de uppgifter som framgår av första stycket, den plats anges som tillståndet avser.

9 §

Vid hemlig *teleavlyssning* och hemlig *teleövervakning* får de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen användas.	Vid hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation* får de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen användas.

11 §[2]

Hemlig *teleavlyssning* får inte ske av telefonsamtal eller andra *telemeddelanden* där den som yttrar sig inte skulle ha kunnat höras som vittne, enligt 36 kap. 5 § andra–sjätte styckena rättegångsbalken, om det som har sagts eller på annat sätt framkommit. Om det av avlyssningen framgår att det är fråga om ett sådant samtal eller meddelande, ska avlyssningen omedelbart avbrytas.	Hemlig *avlyssning av elektronisk kommunikation* får inte ske av telefonsamtal eller andra *meddelanden* där den som yttrar sig inte skulle ha kunnat höras som vittne, enligt 36 kap. 5 § andra–sjätte styckena rättegångsbalken, om det som har sagts eller på annat sätt framkommit. Om det av avlyssningen framgår att det är fråga om ett sådant samtal eller meddelande, ska avlyssningen omedelbart avbrytas.
Upptagningar och uppteckningar från en hemlig *teleavlyssning* ska, i den utsträckning de omfattas av förbudet, omedelbart förstöras.	Upptagningar och uppteckningar från en hemlig *avlyssning av elektronisk kommunikation* ska, i den utsträckning de omfattas av förbudet, omedelbart förstöras.

13 §

En upptagning eller uppteckning som har gjorts vid hemlig *teleavlyssning* eller hemlig *teleövervakning* ska granskas snarast möjligt. Detsamma gäller en upptagning som har gjorts vid hemlig kameraövervakning. Granskningen får utföras endast av rätten, en åklagare, Rikspolisstyrelsen, Säkerhetspolisen eller en polismyndighet.	En upptagning eller uppteckning som har gjorts vid hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* ska granskas snarast möjligt. Detsamma gäller en upptagning som har gjorts vid hemlig kameraövervakning. Granskningen får utföras endast av rätten, en åklagare,

[2] Senaste lydelse 2010:405

Efter anvisning av rätten, en åklagare eller någon av de nämnda myndigheterna får granskningen utföras även av en sakkunnig eller någon annan som har anlitats i ärendet.

Rikspolisstyrelsen, Säkerhetspolisen eller en polismyndighet. Efter anvisning av rätten, en åklagare eller någon av de nämnda myndigheterna får granskningen utföras även av en sakkunnig eller någon annan som har anlitats i ärendet.

Upptagningar och uppteckningar ska, i de delar de är av betydelse för att förhindra förestående brott, bevaras så länge det behövs för att förhindra brott. I de delar upptagningarna och uppteckningarna innehåller sådana uppgifter om brott som enligt 12 § får användas för att utreda brott ska de bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. De ska därefter förstöras.

Trots vad som sägs i andra stycket får brottsutredande myndigheter behandla uppgifter från upptagningar och uppteckningar som rör förestående brott eller uppgifter om brott som enligt 12 § får användas för att utreda brott i enlighet med vad som är särskilt föreskrivet i lag.

16 §

Den som har varit utsatt för en åtgärd enligt 1 § 6 ska underrättas om åtgärden. Om åtgärden har avsett *en teleadress* eller en plats som innehas av någon annan, ska även denne underrättas. Vid hemlig kameraövervakning behöver dock innehavaren av en sådan plats till vilken allmänheten har tillträde inte underrättas.

Den som har varit utsatt för en åtgärd enligt 1 § 6 ska underrättas om åtgärden. Om åtgärden har avsett *ett telefonnummer eller annan adress, en elektronisk kommunikationsutrustning* eller en plats som innehas av någon annan, ska även denne underrättas. Vid hemlig kameraövervakning behöver dock innehavaren av en sådan plats till vilken allmänheten har tillträde inte underrättas.

Underrättelsen ska lämnas så snart det kan ske efter det att det ärende i vilket åtgärden vidtogs avslutades.

En underrättelse behöver inte lämnas till den som redan har fått del av eller tillgång till uppgifterna. En underrättelse behöver inte heller lämnas om den med hänsyn till omständigheterna uppenbart är utan betydelse.

17 §

En underrättelse enligt 16 § ska innehålla uppgift om vilket tvångsmedel som har använts och uppgift om tiden för åtgärden. Vid hemlig *teleavlyssning* och hemlig *teleövervakning* ska underrättelsen även innehålla uppgift om *vilken teleadress* som åtgärden har avsett. Vid hemlig kameraövervakning ska underrättelsen även innehålla uppgift om platsen för åtgärden.

En underrättelse enligt 16 § ska innehålla uppgift om vilket tvångsmedel som har använts och uppgift om tiden för åtgärden. Vid hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation* ska underrättelsen även innehålla uppgift om *vilket telefonnummer eller annan adress eller vilken elektronisk*

Den som har varit utsatt för en åtgärd enligt 1 § 6 ska få uppgift om vilken misstanke som har legat till grund för åtgärden. Den som inte är eller har varit misstänkt ska få uppgift om detta.	*kommunikationsutrustning* som åtgärden har avsett. Vid hemlig kameraövervakning ska underrättelsen även innehålla uppgift om platsen för åtgärden. Den som har varit utsatt för en åtgärd enligt 1 § 6 ska få uppgift om vilken misstanke som har legat till grund för åtgärden. Den som inte är eller har varit misstänkt ska få uppgift om detta.

Denna lag träder i kraft den 1 juli 2011.

2.10 Förslag till lag om ändring i lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott

Härigenom föreskrivs att 3 och 4 §§ lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	3 §
Tillstånd enligt 27 kap. rättegångsbalken till hemlig *teleavlyssning*, hemlig *teleövervakning* eller hemlig kameraövervakning får meddelas även om brottet inte omfattas av de krav som ställs upp i 27 kap. 18 § andra stycket, 19 § *andra* stycket eller 20 a § andra stycket rättegångsbalken.	Tillstånd enligt 27 kap. rättegångsbalken till hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning får meddelas även om brottet inte omfattas av de krav som ställs upp i 27 kap. 18 § andra stycket, 19 § *tredje* stycket, eller 20 a § andra stycket rättegångsbalken.
	4 §
Om det kan befaras att inhämtande av rättens tillstånd till hemlig *teleavlyssning,* hemlig *teleövervakning* eller hemlig kameraövervakning skulle medföra en sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden ges av åklagaren.	Om det kan befaras att inhämtande av rättens tillstånd till hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning skulle medföra en 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 juli 2011.

2.11 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs att 10 kap. 23 och 26 §§, 18 kap. 19 §, 29 kap. 2 §, 38 kap. 5 § och 44 kap. 4 § samt rubriken närmast före 29 kap. 2 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
10 kap.	
23 §	
Om inte annat följer av 19–22 §§ får en uppgift som angår misstanke om ett begånget brott och som är sekretessbelagd enligt 24 kap. 8 §, 25 kap. 1 §, 2 § andra stycket eller 3–8 §§, 26 kap. 1–6 §§, 29 kap. 1 *eller 2* §, 31 kap. 1 § första stycket, 2 eller 12 §, 33 kap. 2 §, 36 kap. 3 § eller 40 kap. 2 eller 5 § lämnas till en åklagarmyndighet, polismyndighet eller någon annan myndighet som har till uppgift att ingripa mot brottet endast om misstanken angår	Om inte annat följer av 19–22 §§ får en uppgift som angår misstanke om ett begånget brott och som är sekretessbelagd enligt 24 kap. 8 §, 25 kap. 1 §, 2 § andra stycket eller 3–8 §§, 26 kap. 1–6 §§, 29 kap. 1 §, 31 kap. 1 § första stycket, 2 eller 12 §, 33 kap. 2 §, 36 kap. 3 § eller 40 kap. 2 eller 5 § lämnas till en åklagarmyndighet, polismyndighet eller någon annan myndighet som har till uppgift att ingripa mot brottet endast om misstanken angår

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i ett år,
2. försök till brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, eller
3. försök till brott för vilket det inte är föreskrivet lindrigare straff än fängelse i ett år, om gärningen innefattat försök till överföring av sådan allmänfarlig sjukdom som avses i 1 kap. 3 § smittskyddslagen (2004:168).

Lydelse enligt Justitieutskottets betänkande 2010/11:JuU2	*Föreslagen lydelse*
26 §	
Sekretess hindrar inte att en uppgift om en enskilds adress, telefonnummer och arbetsplats eller uppgift i form av fotografisk bild av en enskild lämnas till en myndighet, om uppgiften behövs där för delgivning enligt delgivningslagen (2010:000).	
Om den enskilde hos en myndighet som *driver televerksamhet* har begärt att abonnemanget ska hållas hemligt	Om den enskilde hos en myndighet som *tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommuni-*

och om uppgiften är sekretessbelagd enligt 29 kap. 3 §, får den 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.

kationstjänst har begärt att abonnemanget ska hållas hemligt och om uppgiften är sekretessbelagd enligt 29 kap. 3 §, får den 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.

Nuvarande lydelse *Föreslagen lydelse*

18 kap.

19 §

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

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig *teleavlyssning,* hemlig *teleövervakning*, hemlig kameraövervakning eller hemlig rumsavlyssning på grund av beslut av domstol, undersökningsledare eller åklagare.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation*, hemlig kameraövervakning eller hemlig rumsavlyssning på grund av beslut av domstol, undersökningsledare eller åklagare *eller inhämtning av uppgifter enligt lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.*

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

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

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver vad som anges i andra

stycket följer av 7 kap. 3 § första stycket 1, 4 § 1–8 och 5 § 3 tryckfrihetsförordningen samt 5 kap. 1 § första stycket och 3 § första stycket 1 yttrandefrihetsgrundlagen.

29 kap.

Telemeddelande	*Elektroniskt meddelande*
	2 §
Sekretess gäller hos en myndighet som *driver televerksamhet* för *uppgift om ett särskilt telefonsamtal eller annat telemeddelande.* Om sekretess inte följer av någon 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.*	Sekretess gäller hos en myndighet som *tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst för uppgift om 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 elektronisk meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande. Detsamma gäller innehavaren av ett abonnemang som använts för ett elektronisk meddelande när det är fråga om uppgift om något annat än innehållet i meddelandet.*

38 kap.

	5 §
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 *ett elektroniskt meddelande* som utomstående utväxlar *i ett elektroniskt kommunikationsnät*.

44 kap.

4 §[1]

Rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer av

1. 2 kap. 14 § första stycket 1 och 3 postlagen (2010:1045),

[1] Senaste lydelse 2010:1048.

2. 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation, när det är fråga om uppgift om innehållet i ett elektroniskt meddelande eller som annars rör ett särskilt sådant meddelande, och

3. 6 kap. 21 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag *eller* om hemlig *teleavlyssning och* hemlig *teleövervakning* på grund av beslut av domstol, undersökningsledare eller åklagare.	3. 6 kap. 21 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig *avlyssning av elektronisk kommunikation eller* hemlig *övervakning av elektronisk kommunikation* på grund av beslut av domstol, undersökningsledare eller åklagare *eller om inhämtning av uppgifter enligt lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*.

Denna lag träder i kraft den 1 juli 2011.

3 Ärendet och dess beredning

Regeringen beslutade den 7 december 2000 att tillkalla en beredning med uppgift att verka för rättsväsendets utveckling (dir. 2000:90). Beredningen antog namnet Beredningen för rättsväsendets utveckling (BRU). En huvuduppgift för BRU var att undersöka möjligheterna att med bibehållen rättssäkerhet öka effektiviteten och kvaliteten i rättsväsendets arbete. Genom tilläggsdirektiv den 20 november 2003 fick BRU i uppdrag att göra en översyn av bl.a. det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till uppgifter om elektronisk kommunikation (dir. 2003:145).

BRU överlämnade i maj 2005 delbetänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38). BRU:s sammanfattning av delbetänkandet i nu aktuella delar finns i *bilaga 1*. Dess lagförslag i motsvarande delar finns i *bilaga 2*. Delbetänkandet har remissbehandlats. En remissammanställning finns tillgänglig i lagstiftningsärendet (Ju2005/4823/Å). En förteckning över remissinstanserna finns i *bilaga 3*.

Under betänkandets fortsatta beredning bedömdes det nödvändigt att komplettera underlaget i vissa delar. Regeringen beslutade därför den 20 december 2007 att tillsätta en särskild utredare för att överväga bl.a. vissa frågor om inhämtning av uppgifter om elektronisk kommunikation inom polisens underrättelseverksamhet och under förundersökning innan det finns någon skäligen misstänkt gärningsman (dir. 2007:185). Utredningen, som antog namnet Polismetodutredningen, har redovisat sina överväganden i nu nämnda delar i delbetänkandet En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen (SOU 2009:1). Utredningens sammanfattning av delbetänkandet finns i *bilaga 4*. Dess lagförslag finns i *bilaga 5*. Delbetänkandet har remissbehandlats. En remissammanställning finns tillgänglig i lagstiftningsärendet (Ju2009/834/Å). En förteckning över remissinstanserna finns i *bilaga 6*.

I denna lagrådsremiss behandlas Polismetodutredningens delbetänkande och de delar av BRU:s delbetänkande som avser rättegångsbalkens terminologi, tillgång till övervakningsuppgifter vid hemlig teleavlyssning, upphävande av vissa bestämmelser i sekretesslagen (numera offentlighets- och sekretesslagen), skyldighet för operatörer att lämna ut vissa uppgifter när personer har försvunnit samt skyldighet att registrera abonnemangsuppgifter för kontantkort.

4 Användning av hemliga tvångsmedel och elektronisk kommunikation, m.m.

4.1 Hemliga tvångsmedel

Allmänt om straffprocessuella tvångsmedel

Under en förundersökning får straffprocessuella tvångsmedel enligt 24–28 kap. rättegångsbalken användas (23 kap. 16 § rättegångsbalken). Tvångsmedlen används i brottsutredande syfte eller för att en rättegång i brottmål ska kunna genomföras. Normalt innefattar de tvång mot person eller egendom. Husrannsakan, kroppsvisitation, kroppsbesiktning och beslag utgör exempel på straffprocessuella tvångsmedel liksom gripande, anhållande och häktning. Samtliga dessa åtgärder har det gemensamt att de innebär ett intrång i en persons rättssfär och att de kan genomföras med direkt verkande tvång.

De hemliga tvångsmedlen (hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning, hemlig rumsavlyssning och kvarhållande av försändelse) intar en särställning bland de straffprocessuella tvångsmedlen eftersom de förutsätts äga rum i hemlighet. Att den misstänkte hålls ovetande om tvångsmedelsanvändningen är en förutsättning för att tvångsmedlet ska få avsedd effekt. Eftersom den som utsätts för ett hemligt tvångsmedel inte får kännedom om åtgärden kan han eller hon i praktiken inte heller överklaga beslutet. I stället finns särskilda rättssäkerhetsmekanismer vid användandet av hemliga tvångsmedel. Dessa behandlas närmare i avsnitt 4.3.

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

Hemlig teleavlyssning och hemlig teleövervakning enligt rättegångsbalken

Bestämmelser om hemlig teleavlyssning och hemlig teleövervakning finns i 27 kap. rättegångsbalken.

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 (27 kap. 18 §). Med telemeddelande avses detsamma som i 6 kap. 19 § tredje stycket lagen (2003:389) om elektronisk

kommunikation, 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. Hemlig teleavlyssning får användas vid förundersökning som 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, om sådan gärning är belagd med straff, samt vid förundersökning som gäller ett brott med lägre straffminimum, om brottets straffvärde bedöms överstiga fängelse i två år.

Hemlig teleövervakning innebär att det i hemlighet hämtas in uppgifter om telemeddelanden som befordras eller har befordrats till eller från en viss teleadress eller att sådana meddelanden hindras från att nå fram (27 kap. 19 §). Uppgifter om innehållet i telemeddelanden omfattas inte av detta tvångsmedel. Om hemlig teleövervakning avser ett telefonnummer, kan de brottsbekämpande myndigheterna genom övervakningen bl.a. få fram till vilka teleadresser samtal överförs från den övervakade teleadressen, från vilka teleadresser samtal överförs till den övervakade teleadressen, vid vilka tidpunkter samtalen sker och längden på samtalen. Regleringen är också tillämplig på datakommunikation, t.ex. kan de brottsbekämpande myndigheterna få uppgifter om vilka hemsidor en abonnent har besökt och mellan vilka e-postadresser kommunikation har skett. Hemlig teleövervakning får användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader samt vid förundersökning om dataintrång enligt 4 kap. 9 c § brottsbalken, barnpornografibrott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, narkotikabrott enligt 1 § narkotikastrafflagen (1968:64) eller narkotikasmuggling enligt 6 § första stycket lagen (2000:1225) om straff för smuggling. Hemlig teleövervakning får också användas vid misstanke om försök, förberedelse eller stämpling till ovannämnda brott, om en sådan gärning är straffbelagd.

Hemlig teleavlyssning och hemlig teleövervakning får enligt rättegångsbalken enbart beslutas av domstol. För båda slagen av tvångsmedel gäller att de får användas endast om någon är skäligen misstänkt för ett brott och åtgärden är av synnerlig vikt för utredningen om brottet (27 kap. 20 § rättegångsbalken). Tiden för tillstånd får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet (27 kap. 21 § andra stycket rättegångsbalken). Tiden kan förlängas på begäran av åklagaren. Åtgärden får avse en teleadress som, under den tid som tillståndet avser, innehas eller har innehafts av den misstänkte eller som annars kan antas ha använts eller komma att användas av den misstänkte eller 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.

För nu aktuella tvångsmedel gäller, som vid all tvångsmedelsanvändning, att åtgärden i fråga får beslutas endast om skälen för åtgärden uppväger det intrång och men som åtgärden innebär för den misstänkte eller något annat motstående intresse (27 kap. 1 § andra stycket rättegångsbalken, jfr ovan om proportionalitetsprincipen).

Övriga hemliga tvångsmedel

Regler om hemlig kameraövervakning finns i 27 kap. rättegångsbalken. Hemlig kameraövervakning innebär att fjärrstyrda TV-kameror, andra optisk-elektroniska instrument eller därmed jämförbar utrustning används för optisk personövervakning vid förundersökning i brottmål utan att upplysning om övervakningen lämnas (27 kap. 20 a §). Förutsättningarna för att sådan övervakning ska få ske är i huvudsak desamma som för hemlig teleavlyssning. Övervakningen får endast avse sådan plats där den skäligen misstänkte kan antas komma att uppehålla sig (27 kap. 20 b §). Om det inte finns någon skäligen misstänkt för brottet, får hemlig kameraövervakning användas för att övervaka den plats där brottet har begåtts eller en nära omgivning till denna plats i syfte att fastställa vem som skäligen kan misstänkas för brottet (27 kap. 20 c §). Ett beslut om hemlig kameraövervakning omfattar inte ljudupptagning.

Bestämmelser om hemlig rumsavlyssning finns i lagen (2007:978) om hemlig rumsavlyssning. Med hemlig rumsavlyssning avses att tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst som allmänheten inte har tillträde till i hemlighet avlyssnas eller tas upp genom tekniskt hjälpmedel för återgivning av ljud. Hemlig rumsavlyssning får användas vid förundersökning avseende brott som har ett minimistraff om fängelse i fyra år och vissa andra brott om straffvärdet överstiger fängelse i fyra år. Lagen är tidsbegränsad till utgången av år 2012.

Bestämmelser om hemlig teleavlyssning och hemlig teleövervakning finns i lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott (2008 års tvångsmedelslag). Lagen gäller i fråga om förundersökning som avser allmänfarliga brott, brott mot rikets säkerhet och terroristbrott. Enligt lagen kan bl.a. hemlig teleavlyssning och hemlig övervakning beslutas även vid vissa brott som inte kan ligga till grund för sådana åtgärder enligt rättegångsbalken. Lagen innehåller också regler som ger åklagaren möjlighet att under vissa förutsättningar fatta interimistiskt beslut om tvångsmedelsanvändning. Lagen är tidsbegränsad till utgången av år 2012.

Bestämmelser om hemlig teleavlyssning och hemlig teleövervakning finns vidare i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. Även enligt denna lag får åklagaren under vissa förutsättningar fatta interimistiska beslut om tvångsmedel.

Lagen (1991:572) om särskild utlänningskontroll innehåller också bestämmelser om hemlig teleavlyssning och hemlig teleövervakning. Sistnämnda bestämmelser har ett annat syfte än bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning i rättegångsbalken och 2008 års tvångsmedelslag. Bestämmelserna ska inte tillämpas för att utreda brott utan för att förebygga terroristbrott enligt vissa angivna rekvisit. Tvångsmedlen får användas om det är påkallat för att utröna om en utlänning eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott.

Enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott kan hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning under vissa förutsättningar användas i underrättelseverksamhet för att förhindra brott. Åtgärderna förutsätts vidtas i ett tidigt skede för att förhindra att allvarliga brott begås, dvs. innan en förundersökning har inletts. Tillstånd till åtgärderna får meddelas om det med hänsyn till omständigheterna finns särskild anledning att anta att en person kommer att utöva viss allvarlig brottslig verksamhet. Det gäller vissa allmänfarliga brott, brott mot rikets säkerhet och terroristbrott, dvs. den brottslighet som faller inom Säkerhetspolisens ansvarsområde. Lagen gäller även vissa andra allvarliga brott som mord och människorov om avsikten är att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd. I övrigt är förutsättningarna likartade dem i rättegångsbalken. Lagen är tidsbegränsad och gäller till utgången av år 2012.

Regeringen har tillsatt en utredning som har fått i uppdrag att utvärdera lagen om hemlig rumsavlyssning, lagen om åtgärder för att förhindra vissa särskilt allvarliga brott och 2008 års tvångsmedelslag samt att analysera om regleringen om hemliga tvångsmedel för särskilt allvarlig eller annars samhällsfarlig brottslighet bör förändras i något avseende (dir. 2010:62).

Lagen (2000:562) om internationell rättslig hjälp i brottmål innehåller regler om åklagares och domstolars samarbete över gränserna i brottsutredningar och brottmålsrättegångar. Lagen innehåller bl.a. bestämmelser som reglerar under vilka förutsättningar Sverige kan lämna bistånd med hemlig teleavlyssning och hemlig teleövervakning. Reglerna knyter an till vad som gäller för att motsvarande åtgärder ska få vidtas i en svensk förundersökning eller rättegång. Åtgärderna vidtas således under samma förutsättningar som enligt rättegångsbalken (prop. 1999/2000:61 s. 97). Dessutom innehåller lagen bestämmelser om rättslig hjälp som saknar motsvarighet i inhemska brottsutredningar och har tillkommit genom 2000 års konvention om ömsesidig rättslig hjälp mellan Europeiska unionens medlemsstater (prop. 2004/05:144). Dessa gäller tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning respektive tillstånd till gränsöverskridande hemlig teleavlyssning eller hemlig teleövervakning. I båda fallen genomförs avlyssningen eller övervakningen utomlands med stöd av ett beslut meddelat i den staten, men med viss teknisk hjälp eller ett tillstånd från Sverige.

4.2 Elektronisk kommunikation

Allmänt om elektronisk kommunikation

Elektronisk kommunikation innebär överföring av signaler i elektronisk form. Elektronisk kommunikation omfattar telefoni, datakommunikation samt utsändningar till allmänheten genom radio och TV. Gradvis växer dessa tre delar samman. Denna utveckling har framför allt möjliggjorts genom den s.k. digitaliseringen och den tekniska standardiseringen

genom framväxten av Internet. Detta 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 överförs ständigt en mycket stor 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.

Lagen om elektronisk kommunikation

Lagen (2003:389) om elektronisk kommunikation trädde i kraft i juli 2003 och syftade bl.a. till att genomföra flera EG-direktiv om elektronisk kommunikation. Den ersatte telelagen (1993:597) och lagen (1993:599) om radiokommunikation.

Telelagen infördes i samband med att verksamheten i Televerket överfördes till Telia AB. Eftersom den huvudsakliga televerksamheten inte längre skulle bedrivas av en myndighet utan av enskilda företag, infördes det i telelagen regler om bl.a. tystnadsplikt. Dessa överensstämde till stora delar med motsvarande regler i sekretesslagen (1980:100).

Lagen om elektronisk kommunikation gäller elektroniska kommunikationsnät och kommunikationstjänster med tillhörande installationer och tjänster samt annan radioanvändning (1 kap. 4 § första stycket). Elektroniskt kommunikationsnät definieras i lagen 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 (1 kap. 7 §). Med elektronisk kommunikationstjänst avses i lagen en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät (1 kap. 7 §).

Till skillnad från telelagen är lagen om elektronisk kommunikation tillämplig inte endast på telefoni och datakommunikation utan även på utsändningar till allmänheten av program i ljudradio och TV. Riksdagen beslutade i samband med att lagen om elektronisk kommunikation antogs om nya mål för sektorn elektronisk kommunikation. Målen är att enskilda och myndigheter ska få tillgång till effektiva och säkra elektroniska kommunikationer med största möjliga utbyte när det gäller urvalet av överföringstjänster samt deras pris och kvalitet.

Vissa bestämmelser i lagen om elektronisk kommunikation knyter an till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. I 6 kap. 19 § lagen om elektronisk kommunikation regleras anpassningsskyldigheten för operatörerna. Den innebär att vissa verksamheter ska bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas under sådana former att

verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand.

Lagen om elektronisk kommunikation innehåller vidare regler om tystnadsplikt (6 kap. 20 §). Av reglerna följer att 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, inte obehörigen får föra vidare eller utnyttja det han eller hon har fått del av eller tillgång till. Enligt lagen har dessutom operatörerna tystnadsplikt för uppgift som hänför sig till användning av vissa hemliga tvångsmedel, nämligen hemlig teleavlyssning, hemlig teleövervakning och kvarhållande av försändelser (6 kap. 21 §).

I lagen om elektronisk kommunikation finns dessutom bestämmelser som ger de brottsutredande myndigheterna vissa möjligheter att utan domstolsprövning få tillgång till uppgifter om elektroniska meddelanden (6 kap. 22 §). Reglerna innebär att operatörerna i vissa fall är skyldiga att på begäran lämna ut uppgifter om abonnemang, dvs. uppgifter som identifierar en abonnent eller ett abonnemang, framför allt namn, titel, adress och abonnentnummer. Uppgifterna om abonnemang ska lämnas ut, om fängelse är föreskrivet för brottet och brottet enligt den brottsutredande myndighetens bedömning kan föranleda annan påföljd än böter. Vidare innebär reglerna att operatörerna är skyldiga att lämna ut ”annan uppgift som angår ett särskilt elektroniskt meddelande”. Med sådan uppgift avses 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 uppgift om positionen hos en mobiltelefon när uppgiften samtidigt angår ett elektroniskt meddelande är sådan uppgift som anses omfattas av begreppet. Så kallad basstationstömning, dvs. uppgifter om samtliga de mobiltelefoner som haft kontakt med en basstation i närheten av en brottsplats vid en viss tidpunkt, anses, under förutsättning att mobiltelefonen har använts för kommunikation, i den praktiska tillämpningen vara en sådan ”annan uppgift som angår ett särskilt elektroniskt meddelande”. Uppgifterna ska lämnas ut till de brottsutredande myndigheterna om det är fråga om misstanke om brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år.

Det finns inte någon formell gräns för hur gammal information som får lämnas ut. En praktisk begränsning i möjligheten att få uppgifter utlämnade följer dock av skyldigheten för operatörerna att utplåna eller avidentifiera uppgifter. I lagen föreskrivs nämligen att trafikuppgifter som huvudregel ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande (6 kap. 5 §). Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring i direktiv 2002/58/EG syftar till att säkerställa att uppgifter om kommunikation med fast och mobil telefoni, Internetåtkomst, e-post och Internettelefoni lagras så att de brottsbekämpande myndigheterna kan få tillgång till uppgifterna för utredning, avslöjande och åtal som avser

allvarlig brottslighet. Regeringen har i propositionen Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG (prop. 2010/11:46) lämnat förslag till sådana regler om lagring av trafik- lokaliserings- och abonnemangsuppgifter som direktivet föreskriver. För de uppgifter som ska lagras i enlighet med direktivet föreslås en särskilt reglerad anpassningsskyldighet. Anpassningsskyldigheten i 6 kap. 19 § lagen om elektronisk kommunikation kommer således, efter att de föreslagna lagändringarna har trätt i kraft, att omfatta endast realtidsövervakning och historiska uppgifter som inte har lagrats med stöd av nämnda direktiv.

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 rättegångsbalken). Det är således inte nödvändigt, som vid hemlig teleavlyssning och hemlig teleövervakning, att det finns en skäligen misstänkt person för att en myndighet ska få en uppgift utlämnad från operatören. Inte heller behöver uppgifterna ha en anknytning till en eventuell misstänkt person.

Skyldigheten för operatörerna att enligt lagen om elektronisk kommunikation lämna ut uppgifter till brottsutredande myndigheter gäller enbart nu nämnda uppgifter. Lokaliseringsuppgifter som inte är trafikuppgifter och som rör användare som är fysiska personer omfattas t.ex. inte. Sådana uppgifter får enligt 6 kap. 9 § lagen om elektronisk kommunikation behandlas av operatörerna endast under vissa förutsättningar. Justitiekanslern har i ett beslut den 15 augusti 2008 (dnr 6545-06-21) konstaterat att regleringen innebär att operatörerna inte får lämna ut uppgifter till polisen om lokalisering av en mobiltelefon som är påslagen men som inte använts för en kommunikation utan att de berörda fysiska personerna först har avidentifierats eller gett sitt samtycke.

Offentlighets- och sekretesslagen

Även offentlighets- och sekretesslagen (2009:400), som reglerar handlingssekretess och tystnadsplikt i det allmännas verksamhet, innehåller bestämmelser om tillgång till uppgifter om telemeddelanden. Motsvarande bestämmelser fanns tidigare i sekretesslagen (1980:100). Enligt offentlighets- och sekretesslagen gäller sekretess hos myndighet som driver televerksamhet för uppgift som angår ett särskilt telefonsamtal eller annat telemeddelande (29 kap. 2 §). Sådana uppgifter som gäller misstanke om brott och som omfattas av sekretess enligt bl.a. 29 kap. 2 § får lämnas ut till åklagarmyndighet, polismyndighet eller annan myndighet som har till uppgift att ingripa mot brottet om det för brottet inte är föreskrivet lindrigare straff än fängelse i ett år (10 kap. 23 §). Bestämmelsen omfattar såväl historiska uppgifter som uppgifter i realtid. Offentlighets- och sekretesslagens regler innebär, på liknande sätt som reglerna för enskilt bedriven verksamhet i lagen om elektronisk kommunikation, att uppgifter om elektronisk kommunikation lämnas ut både om de har koppling till personer som är misstänkta för brott och om de har koppling till andra än misstänkta (jfr prop. 1983/84:142 s. 17).

4.3 Regler till skydd för den personliga integriteten

Regeringsformen

De straffprocessuella tvångsmedlen är exempel på lagreglerade undantag från det skydd mot intrång i den personliga integriteten som medborgarna har enligt regeringsformen.

Enligt 1 kap. 2 § fjärde stycket regeringsformen ska det allmänna värna den enskildes privatliv och familjeliv. Bestämmelsen har inte karaktären av en rättsligt bindande föreskrift utan anger ett mål för den samhälleliga verksamheten. Vidare anges i regeringsformen i dess lydelse fr.o.m. den 1 januari 2011 (prop. 2009/10:80, bet. 2009/10:KU19 och 2010/11:KU4) att var och en gentemot det allmänna är skyddad mot bl.a. ”husrannsakan och liknande intrång” och mot ”undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande” (2 kap. 6 § regeringsformen). Den 1 januari 2011 införs vidare en ny bestämmelse i regeringsformen som innebär att enskilda ges ett stärkt generellt grundlagsskydd för den personliga integriteten. Enligt 2 kap. 6 § andra stycket regeringsformen i dess nya lydelse ska var och en gentemot det allmänna vara skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Det skydd som avses i 2 kap. 6 § regeringsformen kan endast begränsas genom lag och i övrigt enligt vad som föreskrivs i 2 kap. 20–22 §§ regeringsformen i dess nya lydelse (tidigare 2 kap. 12 §). I 21 § anges att begränsningen får göras endast för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle. En begränsning får dock 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.

Europakonventionen m.m.

Enligt artikel 8:1 i den europeiska konventionen den 4 november 1950 om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) har var och en rätt till respekt för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Rätten till skydd för privatlivet enligt konventionen 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, såsom elektronisk post, omfattas av konventionens skydd för korrespondens (Danelius, Mänskliga rättigheter i europeisk praxis, 3 uppl. 2007 s. 344).

Av artikel 8:2 följer att inskränkningar får ske i dessa rättigheter under vissa förutsättningar. En inskränkning måste ha stöd i lag. Den måste vidare vara ägnad att tillgodose något av de i artikeln uppräknade allmänna eller enskilda intressena, däribland statens säkerhet, den allmänna säkerheten och förebyggande av oordning eller brott. Inskränkningen måste även anses vara nödvändig i ett demokratiskt samhälle för att tillgodose detta intresse. Detta 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 ska tillgodoses genom inskränkningen (a. a. s. 304 f.). Det lagstadgade undantaget måste vara utformat med sådan precision att inskränkningen av rättigheten är förutsebar i rimlig utsträckning.

I Europadomstolens praxis har slagits fast att hemlig teleavlyssning och hemlig teleövervakning utgör intrång i såväl skyddet för privatliv som skyddet för korrespondens. Sådana intrång har ansetts godtagbara då det är strängt nödvändigt för att skydda den nationella säkerheten eller att förhindra oordning eller brott. Det måste dock finnas en effektiv kontroll av att systemet inte missbrukas. När teleavlyssning har ansetts utgöra en kränkning av artikel 8, har i de flesta fall bristande lagenlighet utgjort grunden för kränkningen.

Enligt artikel 13 i Europakonventionen ska var och en, som fått sina i konventionen angivna fri- och rättigheter kränkta, ha tillgång till ett effektivt rättsmedel inför en nationell myndighet och detta även om kränkningen förövats av någon under utövning av offentlig myndighet. Ett ”effektivt rättsmedel” är ett rättsmedel som medger en tillfredsställande prövning av ett klagomål, oavsett om det leder till framgång för klaganden eller inte. Artikel 13 förutsätter inte rättsmedel inför domstol. Även administrativa rättsmedel kan vara tillräckliga för att uppfylla konventionskraven.

FN:s konvention om medborgerliga och politiska rättigheter

Förenta nationernas generalförsamling antog år 1948 en allmän förklaring om de mänskliga rättigheterna. I artikel 12 i förklaringen slås fast att ingen får utsättas för godtyckliga ingripanden i fråga om bl.a. privatliv, familj, hem eller korrespondens. Förklaringen är inte rättsligt bindande för staterna. Grundsatsen har emellertid även arbetats in i 1966 års FN-konvention om medborgerliga och politiska rättigheter (artikel 17) som trädde i kraft den 23 mars 1976 och som är rättsligt bindande för konventionsstaterna.

Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel

En parlamentarisk kontroll över tillämpningen av reglerna om hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål utövas av riksdagen på grundval av årliga skrivelser från regeringen (bet. 1981/82:JuU54, rskr. 1981/82:298 och prop. 1995/96:85 s. 37). Regeringens skrivelse grundar sig på underlag från Åklagarmyndigheten och Rikspolisstyrelsen, som årligen på uppdrag av regeringen lämnar en gemensam redovisning av användningen av hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning under föregående år. Skrivelsen omfattar dock inte förundersökningar som handläggs av Säkerhetspolisen.

Säkerhets- och integritetsskyddsnämnden inrättades den 1 januari 2008. Myndigheten ska bidra till att värna rättssäkerheten och skyddet för den personliga integriteten i förhållande till den brottsbekämpande

verksamheten. Nämnden har till uppgift att genom inspektioner och andra undersökningar utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och kvalificerade skyddsidentiteter och därmed sammanhängande verksamhet. Nämnden ska också utöva tillsyn över Säkerhetspolisens behandling av uppgifter enligt polisdatalagen, särskilt med avseende på känsliga personuppgifter. Tillsynen ska särskilt syfta till att säkerställa att de brottsbekämpande myndigheternas verksamhet bedrivs i enlighet med lag eller annan författning. Nämnden är också skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel eller varit föremål för Säkerhetspolisens behandling av uppgifter enligt polisdatalagen (1998:622) och om användningen av tvångsmedel och därmed sammanhängande verksamhet eller behandlingen av personuppgifter har skett i enlighet med lag eller annan författning. Tillsynen ska fr.o.m. den 1 mars 2012 även omfatta polisens behandling av personuppgifter enligt de föreslagna nya lagarna om polisens allmänna spaningsregister och polisdatalagen (prop. 2009/10:85).

4.4 De brottsbekämpande myndigheternas verksamhet

Rikspolisstyrelsen, Säkerhetspolisen, polismyndigheterna, Åklagarmyndigheten och Ekobrottsmyndigheten samt även Tullverket, Kustbevakningen och Skatteverket (skattebrottsenheterna) är brottsbekämpande myndigheter (jfr lagen [2000:1225] om straff för smuggling, lagen [1997:1024] om Skatteverkets medverkan i brottsutredningar och lagen [1982:395] om Kustbevakningens medverkan vid polisiär övervakning).

Förfarandet vid den utredning som föregår ett beslut om åtal, förundersökningen, regleras i rättegångsbalken och i förundersökningskungörelsen (1947:948). Förundersökning ska inledas så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats (23 kap. 1 § rättegångsbalken). Beslut att inleda förundersökning fattas oftast av polismyndighet eller av åklagare. Förundersökning kan dock i fråga om vissa brott även ledas av Tullverket eller Kustbevakningen. Om förundersökning har inletts av polismyndighet, Tullverket eller Kustbevakningen och saken inte är av enkel beskaffenhet, ska ledningen av förundersökningen övertas av åklagare så snart någon är skäligen misstänkt för brottet. Åklagare ska även i annat fall ta över ledningen av förundersökningen, om det finns särskilda skäl. Så är bl.a. fallet om det blir aktuellt att använda sig av hemliga tvångsmedel, t.ex. teleavlyssning. Förundersökningen har enligt 23 kap. 2 § rättegångsbalken huvudsakligen två syften; dels att utröna om brott föreligger, vem som skäligen kan misstänkas för brottet och att skaffa tillräckligt material för bedömning av frågan om åtal skall väckas, dels att bereda målet så att bevisningen kan förebringas i ett sammanhang vid en huvudförhandling i domstol.

Polisen, Säkerhetspolisen, Ekobrottsmyndigheten, Kustbevakningen, Tullverket och Skatteverket bedriver också underrättelseverksamhet. Denna verksamhet är i huvudsak inriktad på att avslöja om en viss, inte

närmare specificerad, brottslighet har ägt rum, pågår eller kan antas komma att begås. Ett övergripande mål med underrättelseverksamheten är att förse de brottsutredande myndigheterna med kunskap som kan omsättas i operativ verksamhet. Till exempel ska polisens kriminalunderrättelsetjänst vara delaktig i strategisk och operativ verksamhetsplanering och utgöra ett direkt stöd för operativ polisverksamhet, ge underlag till ledningsverksamheten på olika nivåer inom polisen samt medverka när effekterna av genomförda insatser analyseras. I underrättelseverksamheten samlar myndigheterna in, bearbetar och analyserar uppgifter som senare kan ha betydelse för att utreda, förebygga och förhindra brott. Det framtagna underrättelsematerialet kan också läggas till grund för ett beslut om att inleda en förundersökning. Verksamheten beskrivs närmare i avsnitt 6.3.1.

5 Begrepp och avgränsning

5.1 Modernare och mer enhetliga regler

Regeringens bedömning: Rättegångsbalkens terminologi avseende hemlig teleavlyssning och hemlig teleövervakning bör anpassas till ny lagstiftning och moderniseras.

BRU:s bedömning överensstämmer med regeringens bedömning.

Remissinstanserna har inte haft några invändningar mot BRU:s bedömning.

Skälen för regeringens bedömning: Som framgår av avsnitt 4.1 finns bestämmelser om hemlig teleavlyssning och hemlig teleövervakning i 27 kap. rättegångsbalken. Bestämmelserna innehåller begreppen telemeddelande, teleadress och telenät. Dessa anknyter till begrepp i den numera upphävda telelagen. När lagen (2003:389) om elektronisk kommunikation infördes år 2003 valde regeringen att, som en övergångslösning, använda begreppet telemeddelande i den lagen såvitt gällde operatörernas anpassningsskyldighet (prop. 2002/03:110 s. 269). I lagen om elektronisk kommunikation används dock även andra begrepp som inte överensstämmer med rättegångsbalkens eller telelagens terminologi. Termerna teleadress och telenät används t.ex. inte i lagen om elektronisk kommunikation. Mot den beskrivna bakgrunden finns behov av en anpassning och modernisering av rättegångsbalkens terminologi.

Den tekniska utvecklingen för elektronisk överföring och elektronisk kommunikation är oerhört snabb. Som BRU har framhållit är det därför angeläget att en reglering om tillgång till elektronisk kommunikation utformas så att den kan stå sig över tid (SOU 2005:38 s. 153). Det finns enligt regeringen därför anledning att ge de aktuella bestämmelserna en utformning som är mer generell än den nuvarande. Samtidigt bör bestämmelserna ges en så tydlig utformning att det inte råder någon oklarhet om deras tillämpningsområde. Dessutom bör den terminologi som används i rättegångsbalken om möjligt stämma överens med den

terminologi som används i andra författningar om elektronisk kommunikation.

5.2 Telemeddelande ersätts med meddelande i ett elektroniskt kommunikationsnät

Regeringens förslag: Begreppet telemeddelande ska i bestämmelser om hemlig teleövervakning och hemlig teleavlyssning samt i brottsbalken ersättas med begreppet meddelande. De meddelanden som avses i dessa sammanhang ska dessutom avgränsas på det sättet att de ska överföras eller ha överförts i ett elektroniskt kommunikationsnät. I offentlighets- och sekretesslagen (2009:400) ska begreppet telemeddelande ersättas med elektroniskt meddelande.

BRU:s förslag överensstämmer i sak med regeringens förslag.

Remissinstanserna: De flesta remissinstanserna har tillstyrkt eller inte haft några invändningar mot BRU:s förslag. *Kriminalvårdsstyrelsen* har dock ställt sig tveksam till att införa det teknikneutrala begreppet meddelande och *Tullverket* har förespråkat att i stället definitionen av telemeddelande i lagen om elektronisk kommunikation förs in i rättegångsbalken.

Skälen för regeringens förslag: I telelagen (1993:597) 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 (1 §). Trots att det inte ansågs finnas något behov av begreppet i den nya lagen om elektronisk kommunikation kom begreppet att användas som en övergångslösning när det gällde att reglera operatörernas anpassningsskyldighet (prop. 2002/03:110 s. 269). Skälet till det var att undvika rättsosäkerhet i fråga om tillämpningen av de författningar (bl.a. rättegångsbalken och brottsbalken) där begreppet används. Begreppet telemeddelande definieras därför i den lagen i enlighet med vad som tidigare angetts i telelagen (6 kap. 19 § tredje stycket lagen [2003:389] om elektronisk kommunikation).

Reglerna om hemlig teleavlyssning och teleövervakning anknyter, som framgår av avsnitt 4.1, till begreppet telemeddelande (27 kap. 18 och 19 §§ rättegångsbalken). Föremålet för hemlig teleavlyssning och hemlig teleövervakning är ett telemeddelande. Även straffbestämmelsen om brytande av post- eller telehemlighet (4 kap. 8 § brottsbalken) utgår från detta begrepp.

Som BRU har angett har definitionen av begreppet telemeddelande i lagen om elektronisk kommunikation bevarats som en övergångslösning i avvaktan på dess förslag. Med tanke på att begreppet härrör från den upphävda telelagen och inte fyller någon egen funktion i lagen om elektronisk kommunikation, bör en ny terminologi i rättegångsbalken övervägas. Frågan är då vilket begrepp som i stället kan användas för att bestämma vad som bör vara föremål för hemlig teleavlyssning eller teleövervakning.

I lagen om elektronisk kommunikation används även begreppet elektroniskt meddelande. Det definieras 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 (6 kap. 1 §). I förarbetena nämns betal-TV-tjänster som exempel på sändningstjänster som omfattas av begreppet elektroniskt meddelande (prop. 2002/03:110 s. 389).

BRU har kommit fram till att det inte är möjligt att i rättegångsbalken byta ut begreppet telemeddelande mot elektroniskt meddelande. Ingen remissinstans har invänt mot detta. Även regeringen delar BRU:s bedömning. Begreppet elektroniskt meddelande bör därmed inte användas i bestämmelserna om hemlig övervakning av elektronisk kommunikation och hemlig avlyssning av elektronisk kommunikation för att avgränsa vilka meddelanden som får avlyssnas eller övervakas. BRU har föreslagit det teknikneutrala begreppet meddelande. Visserligen kan det begreppet, som *Kriminalvårdsstyrelsen* har framhållit, framstå som väl neutralt. Ett meddelande avser enligt allmänt språkbruk information som överbringas i ett sammanhang, oavsett på vilket sätt detta sker. De meddelanden som avses bör enligt regeringens bedömning också avgränsas genom angivande av att de ska överföras eller ha överförts i ett elektroniskt kommunikationsnät (se vidare avsnitt 5.3). Ändringen medför därmed inte att tvångsmedlen ges en större räckvidd än tidigare i fråga om vilka meddelanden som får avlyssnas eller övervakas. Mot denna bakgrund ansluter regeringen sig till BRU:s förslag och föreslår att begreppet telemeddelande i rättegångsbalken byts ut mot meddelande som överförs eller har överförts i ett elektroniskt kommunikationsnät. Definitionen i 6 kap. 19 § tredje stycket lagen om elektronisk kommunikation fyller därmed ingen funktion och bör upphävas. Begreppet telemeddelande bör ersättas på motsvarande sätt även i brottsbalken, lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen (2000:562) om internationell rättslig hjälp i brottmål

I offentlighets- och sekretesslagens bestämmelser om sekretess hos en myndighet som driver televerksamhet (se närmare avsnitt 6.1) bör dock, i likhet med motsvarande bestämmelser om tystnadsplikt i lagen om elektronisk kommunikation, begreppet elektroniskt meddelande användas.

5.3 Telenät ersätts med elektroniskt kommunikationsnät

Regeringens förslag: Begreppet telenät ska ersättas med elektroniskt kommunikationsnät. Innebörden ska vara densamma som i lagen om elektronisk kommunikation.

BRU:s förslag: Överensstämmer i sak med regeringens förslag. BRU har dock föreslagit att nät som enbart är avsett för utsändning till allmänheten av program i ljudradio eller television uttryckligen ska undantas från tillämpningsområdet.

Remissinstanserna: Ingen av remissinstanserna har haft några invändningar mot förslaget.

Skälen för regeringens förslag: Enligt rättegångsbalken 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 (27 kap. 20 § andra stycket).

I den upphävda telelagen (1993:597) definierades begreppet telenät som en anläggning som är avsedd för förmedling av telemeddelanden (1 §). Vidare användes begreppet allmänt tillgängligt telenät i flera av telelagens bestämmelser utan att detta definierades i lagen. I förarbetena till telelagen angavs att ett kännetecken på att ett telenät är allmänt tillgängligt bör vara att det står öppet för en vid krets av användare att ansluta sig till nätet (prop. 1992/93:200 s. 91 f.).

I lagen om elektronisk kommunikation (2003:389) definieras tre nät, elektroniskt kommunikationsnät, allmänt telefonnät och allmänt kommunikationsnät (1 kap. 7 §). Med elektroniskt kommunikationsnät avses 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 elektromagnetiska överföringsmedier oberoende av vilken information som överförs. Allmänt telefonnät definieras 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. Med allmänt kommunikationsnät avses ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster. Elektroniskt kommunikationsnät är alltså det överordnade begreppet, medan allmänt telefonnät och allmänt kommunikationsnät utgör två underkategorier av elektroniska kommunikationsnät.

Som framgår ovan har begreppet telenät sitt ursprung i den upphävda telelagen. Som BRU har anfört är det om möjligt lämpligt att i rättegångsbalken ansluta till någon av de termer som används i lagen om elektronisk kommunikation. Härigenom skulle en större enhetlighet i

lagstiftningen uppnås. Frågan är då om något av de begrepp som används för att definiera nät i lagen om elektronisk kommunikation kan användas i rättegångsbalken.

BRU har kommit fram till att begreppen allmänt telefonnät och allmänt kommunikationsnät inte passar i rättegångsbalken. En användning av ”allmänt telefonnät” har ansetts kunna innebära en inskränkning i tvångsmedlens tillämpningsområde eftersom begreppet tar sikte på samtal. Begreppet allmänt kommunikationsnät har inte heller ansetts lämpligt att använda i rättegångsbalken eftersom det 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. En användning av sistnämnda begrepp skulle, enligt BRU, kunna medföra att tjänster som tillhandahålls på Internet faller utanför tillämpningsområdet eftersom de inte alltid tillhandahålls kommersiellt (jfr prop. 2002/03:110 s. 95). Remissinstanserna har inte invänt mot BRU:s bedömning i denna del.

BRU har i stället föreslagit att begreppet elektroniskt kommunikationsnät används i rättegångsbalken. Utöver de nät som omfattas av begreppet telenät, omfattas även nät som används för utsändning av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen. I den aktuella bestämmelsen i yttrandefrihetsgrundlagen anges, förutom ljudradio, television och vissa andra överföringar av ljud, bild eller text som sker med hjälp av elektromagnetiska vågor. Sistnämnda överföringar innefattar enligt förarbetena till yttrandefrihetsgrundlagen bl.a. överföringar av information till allmänheten via telefax. För att hindra att tvångsmedlen kommer att omfatta nät som enbart används för utsändning till allmänheten av program i ljudradio och television har BRU föreslagit att ett undantag för nät av dessa slag tas in i rättegångsbalken.

Remissinstanserna har inte haft något att invända mot att begreppet elektroniskt kommunikationsnät används i rättegångsbalken. Regeringen finner BRU:s förslag ändamålsenligt och föreslår därför att ”elektroniskt kommunikationsnät” ersätter ”telenät” i rättegångsbalken. I lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott finns ett likalydande undantag i fråga om hemlig teleavlyssning och hemlig teleövervakning för telenät av mindre betydelse från kommunikationssynpunkt. Även i den lagen och i och offentlighets- och sekretesslagen (2009:400) bör motsvarande ändring göras.

Som BRU har föreslagit ska definitionen av begreppet följa av lagen om elektronisk kommunikation. BRU har föreslagit att en uttrycklig hänvisning görs till definitionen i den lagen. Någon motsvarande hänvisning i rättegångsbalken till t.ex. definitionen av teleadress har inte ansetts behövlig. Regeringen anser inte att det heller nu finns behov av en sådan hänvisning. Det finns inte heller behov av ett uttryckligt undantag för nät som enbart är avsett för utsändning till allmänheten av program i ljudradio eller television. En sådan utsändning är allmänt tillgänglig och är därför inte aktuell för hemlig teleavlyssning eller hemlig teleövervakning. Tillämpningsområdet kommer därför i praktiken inte att ändras.

Som anges ovan bör de meddelanden som omfattas av tvångsmedlen avgränsas genom angivande av i vilken typ av nät meddelandet får

avlyssnas eller övervakas (avsnitt 5.2). Även i detta fall bör begreppet elektroniskt kommunikationsnät väljas. Samma avgränsning bör införas i fråga om vilka meddelanden som omfattas av brottet brytande av telehemlighet i brottsbalken.

5.4 Teleadress ersätts med adress

Regeringens förslag: Begreppet teleadress ska ersättas med adress. Det tydliggörs också att hemlig avlyssning och hemlig övervakning även ska kunna avse en viss elektronisk kommunikationsutrustning.

BRU:s förslag: BRU har föreslagit att begreppet teleadress utmönstras ur lagtexten och att bestämmelserna om hemlig avlyssning eller övervakning i stället ska anknyta till begreppet tekniskt hjälpmedel.

Remissinstanserna: De flesta remissinstanserna har inte haft några invändningar mot BRU:s förslag. *Sveriges advokatsamfund* har framhållit att oklarheterna med begreppet teleadress kan åtgärdas genom att byta ut detta mot ”adress”. *Kriminalvårdsstyrelsen, Tullverket* och *Stockholms Handelskammare* har ställt sig tveksamma till att införa begreppet tekniskt hjälpmedel i nu aktuellt sammanhang.

Skälen för regeringens förslag: Hemlig teleavlyssning och hemlig teleövervakning knyts som nämns i avsnitt 4.1 till ”ett telefonnummer, en kod eller annan teleadress” (27 kap. 18 och 19 §§ rättegångsbalken). Vidare får avlyssning eller övervakning endast avse en teleadress med viss anknytning till den misstänkte (27 kap. 20 § rättegångsbalken). På så sätt preciseras vad som kan vara föremål för hemlig avlyssning eller övervakning. I ett beslut att tillåta hemlig teleavlyssning eller teleövervakning ska det anges bl.a. vilken teleadress beslutet avser (27 kap. 21 § rättegångsbalken).

Begreppet teleadress är inte definierat i rättegångsbalken. Det infördes år 1996 och ersatte termen teleanläggning. ”Teleadress” användes tidigare även i den upphävda telelagen (1993:597) (50 §).

Enligt BRU har åklagare och polis påtalat vissa oklarheter när det gäller begreppet teleadress (SOU 2005:38 s. 166). En typ av uppgift 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. Från myndighetshåll har till BRU framförts att domstolarnas bedömning av frågan om IMEI-numret ska anses vara en teleadress varierar över landet. Mot bakgrund av att det kan finnas behov av att anknyta rätten till avlyssning till en viss utrustning, t.ex. en mobiltelefon, och att det inte står helt klart att dagens reglering ger utrymme för detta har BRU föreslagit att begreppet teleadress ska tas bort ur rättegångsbalken och att rätten till hemlig teleavlyssning eller hemlig teleövervakning i stället ska anknyta till begreppet tekniskt hjälpmedel.

Regeringen delar BRU:s bedömning att ”teleadress” bör ersättas i de lagar som reglerar hemlig teleavlyssning och hemlig teleövervakning. Termen tekniskt hjälpmedel används emellertid redan i rättegångsbalken.

Den tar då sikte på de tekniska hjälpmedel som krävs för att genomföra hemlig avlyssning eller övervakning, t.ex. avlyssningsapparatur (27 kap. 18, 19 och 25 §§). Som *Tullverket* anfört framstår det som mindre lämpligt att använda samma begrepp för att beskriva den utrustning som är föremål för t.ex. avlyssning som de hjälpmedel som behövs för att genomföra avlyssningen. För att göra lagstiftningen mer teknikneutral och enhetlig föreslår regeringen, i enlighet med *Sveriges advokatsamfunds* remissyttrande, att ”teleadress” byts ut mot ”adress”. Någon saklig ändring är inte avsedd. I begreppet adress ingår, liksom i begreppet teleadress, olika typer av nummer, t.ex. telefonnummer och andra identifikationsnummer och adresser, t.ex. e-postadresser. För att tydliggöra vilka adresser som avses bör i lagtexten anges att fråga är om telefonnummer eller annan adress. Begreppet kod bör inte användas i detta sammanhang eftersom det snarast leder tankarna till lösenord eller liknande. Regeringen anser också att det bör tydliggöras att ett beslut om hemlig teleavlyssning eller hemlig teleövervakning kan avse en viss elektronisk kommunikationsutrustning (t.ex. en mobiltelefon med visst identifikationsnummer).

5.5 Hemlig teleavlyssning och hemlig teleövervakning ges nya benämningar

Regeringens förslag: I fortsättningen ska hemlig teleavlyssning benämnas hemlig avlyssning av elektronisk kommunikation och hemlig teleövervakning benämnas hemlig övervakning av elektronisk kommunikation.

BRU:s förslag: BRU har föreslagit att ”hemlig teleavlyssning” och ”hemlig teleövervakning” ska utmönstras ur lagtexten.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt BRU:s förslag eller inte haft några invändningar mot det. Några remissinstanser, bl.a. *Ekobrottsmyndigheten* och *Kriminalvårdsstyrelsen,* har ställt sig tveksamma till förslaget. *Tullverket* har framfört att de begrepp som används även fortsättningsvis bör namnges och definieras i lagtext.

Skälen för regeringens förslag

Nya benämningar införs

I det föregående föreslås att vissa begrepp i rättegångsbalken som innehåller prefixet tele (telemeddelande, telenät och teleadress) ska ersättas med andra begrepp. Det är därför inte ändamålsenligt att fortsättningsvis benämna tvångsmedlen hemlig teleavlyssning och hemlig teleövervakning.

BRU har föreslagit att den aktuella lagtexten utformas utan några särskilda benämningar på tvångsmedlen. BRU har menat att det är tillräckligt att innebörden och förutsättningarna för åtgärderna beskrivs i rättegångsbalken och att man i andra författningar som hänvisar till de aktuella tvångsmedlen använder begreppen avlyssning och övervakning.

Regeringen anser dock, liksom *Tullverket,* att det av tydlighetsskäl är lämpligt att även fortsättningsvis namnge de nu aktuella tvångsmedlen i lagtexten. Detta överensstämmer med utformningen av t.ex. bestämmelserna om hemlig kameraövervakning (27 kap. 20 a § rättegångsbalken) och bestämmelsen om hemlig rumsavlyssning (1 § lagen [2007:978] om hemlig rumsavlyssning) samt underlättar hänvisning till dessa regler i annan lagstiftning.

Regeringen delar *Kriminalvårdsstyrelsens* tveksamhet till att använda enbart begreppen avlyssning och övervakning. Språkligt sett är termerna mycket vida. Dessutom förekommer ”övervakning” i rättegångsbalken i ett helt annat sammanhang, nämligen i bestämmelserna om häktning och anhållande (se t.ex. 24 kap. 2 §). Avlyssning kan numera också ske genom bestämmelserna om hemlig rumsavlyssning. Något mer preciserat begrepp bör därför användas.

I lagen (2003:389) om elektronisk kommunikation används begreppet elektronisk kommunikation. Det är inte definierat i den lagen men avser enligt förarbetena överföring av signaler via tråd, via radio, på optisk väg eller via andra elektromagnetiska överföringsmedier. Elektronisk kommunikation omfattar telefoni och datakommunikation men till skillnad från den upphävda telelagen även utsändningar till allmänheten av program i ljudradio och tv (prop. 2002/03:110 s. 111 f.). Begreppet passar väl för att språkligt sett beskriva det slag av kommunikation där hemlig avlyssning och övervakning kan bli aktuell, även om det inte exakt avgränsar de meddelanden som kan bli föremål för nu aktuella tvångsmedel. Lagen bör därför tala om ”avlyssning av elektronisk kommunikation” och ”övervakning av elektronisk kommunikation”.

Vidare framstår det, vilket bl.a. *Ekobrottsmyndigheten* har framhållit, som ändamålsenligt att behålla begreppet ”hemlig” i de aktuella bestämmelserna. ”Hemlig” tydliggör att det är fråga om tvångsmedel som genomförs utan att den som avlyssnas eller övervakas känner till det.

Mot den angivna bakgrunden föreslår regeringen att ”hemlig teleavlyssning” i rättegångsbalken ersätts med ”hemlig avlyssning av elektronisk kommunikation” och att ”hemlig teleövervakning” ersätts med ”hemlig övervakning av elektronisk kommunikation”.

Följdändringar

Att benämningarna ändras i rättegångsbalken medför att följdändringar behöver göras i offentlighets- och sekretesslagen (2009:400), lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m., lagen (1991:572) om särskild utlänningskontroll, lagen [2003:389] om elektronisk kommunikation, lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott.

Även i lagen (2000:562) om internationell rättslig hjälp i brottmål bör motsvarande följdändringar göras. De nya begreppen bör även användas för de former av rättslig hjälp som saknar motsvarighet i helt svenska förundersökningar, dvs. tekniskt bistånd med hemlig teleavlyssning eller

hemlig teleövervakning. En förändrad terminologi som återspeglar de begrepp som används för nationella förfaranden är fullt förenlig med internationella överenskommelser och praxis.

6 En tydligare och mer rättssäker reglering

6.1 Regleringens övergripande struktur

Regeringens förslag: Bestämmelserna i lagen om elektronisk kommunikation om skyldighet för operatörer att vid misstanke om vissa brott lämna ut uppgifter som angår ett särskilt elektroniskt meddelande till de brottsbekämpande myndigheterna ska upphävas. Även de särskilda bestämmelser i offentlighets- och sekretesslagen som gäller utlämnande av sekretessbelagda uppgifter som angår särskilda telemeddelanden ska upphävas. I förundersökningar ska uppgifter som angår särskilda elektroniska meddelanden kunna inhämtas från operatörerna enbart efter beslut om hemlig övervakning av elektronisk kommunikation. I underrättelseverksamhet ska befogenheten att inhämta sådana uppgifter regleras i en ny lag om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Polismetodutredningens förslag: Överensstämmer med regeringens. Polismetodutredningen har dock inte lämnat något förslag angående regleringen i offentlighets- och sekretesslagen.

Remissinstanserna: *Riksdagens ombudsmän (JO), Göta hovrätt, Stockholms tingsrätt, Malmö tingsrätt, Åklagarmyndigheten, Ekobrottsmyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Datainspektionen, Tullverket, Kustbevakningen, Juridiska fakultetsnämnden vid Stockholms universitet, Svenska Antipiratbyrån* och *Stockholms Handelskammare* har uttryckligen tillstyrkt förslaget. *Hovrätten för Västra Sverige* och *Sundsvalls tingsrätt* har föreslagit en annan placering av bestämmelserna om inhämtning av vissa uppgifter om elektronisk kommunikation i underrättelseskedet.

Sveriges advokatsamfund och *Svenska Journalistförbundet* har motsatt sig förslaget i dess nuvarande utformning. *Svenska Journalistförbundet* har anfört att utredningen inte har lyckats visa att de föreslagna ändringarna uppfyller de krav som följer av principerna om ändamål, behov och proportionalitet. Även *Post- och telestyrelsen* har uppgett att man saknar en avvägning mellan integritet och effektivitet i flera av förslagen.

IT & Telekomföretagen, Telia Sonera AB, Telenor Sverige AB, Hi3GAccess AB, Juridiska fakultesnämnden vid Stockholms universitet och *Stockholms handelskammare* har framfört att ytterligare utredning behövs för att bedöma den totala integritetspåverkan av samtlig tvångsmedelslagstiftning. IT- och Telekomföretagen, Telia Sonera AB, Telenor Sverige AB, Hi3G Access AB och *Svenska Antipiratbyrån* har

vidare framfört synpunkter på förslagens betydelse för slutanvändarnas tilltro till elektronisk kommunikation.

BRU:s förslag: BRU:s förslag att bestämmelserna om utlämnande i den då gällande sekretesslagen (1980:100) ska upphävas överensstämmer med regeringens.

Remissinstanserna: Av de remissinstanser som har yttrat sig särskilt i denna del har ingen motsatt sig förslaget.

Skälen för regeringens förslag

Behovet av en mer rättssäker och ändamålsenlig reglering

De brottsutredande myndigheterna kan enligt nuvarande regler få tillgång till historiska uppgifter om telemeddelanden både enligt rättegångsbalkens regler om hemlig teleövervakning och genom utelämnande direkt från operatörerna enligt lagen om elektronisk kommunikation (27 kap. 19 § rättegångsbalken och 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation). Det är samma slags uppgifter som avses i de båda regelverken. Det kan vara fråga om uppgifter om meddelandets ursprung, destination, färdväg, datum, tid, storlek eller varaktighet eller typ av tjänst.

Förutsättningarna för att kunna utnyttja de båda regelverken skiljer sig åt. Ett utlämnande enligt lagen om elektronisk kommunikation kräver att det är fråga om misstanke om brott med lägsta föreskrivna straff fängelse i två år, vilket ska jämföras med kravet på minst sex månaders fängelse vid hemlig teleövervakning enligt rättegångsbalken. I detta hänseende är alltså kravet i lagen om elektronisk kommunikation strängare än irättegångsbalken. Lagen om elektronisk kommunikation saknar däremot motsvarigheter till rättegångsbalkens övriga krav. Lagen om elektronisk kommunikation ställer alltså inte upp krav på att det ska finnas en skäligen misstänkt person för brottet, att åtgärden ska bedömas vara av synnerlig vikt för utredningen, att åtgärden enbart får avse vissa teleadresser och telenät, att åtgärden kräver tillstånd av domstol, att enskild ska underrättas och att Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn.

Den nu beskrivna regleringen i lagen om elektronisk kommunikation framstår inte som ändamålsenligt utformad och den uppfyller inte heller i tillräcklig grad de krav på rättssäkerhet och integritetsskydd som måste ställas på sådana integritetskänsliga åtgärder. Regeringen föreslår därför att de aktuella bestämmelserna i lagen om elektronisk kommunikation upphävs. Regeringen återkommer i det följande till frågor om utlämnande av abonnemangsuppgifter och utlämnande av uppgifter som inte har samband med brott (avsnitt 7).

Offentlighets- och sekretesslagen innehåller bestämmelser om sekretess hos myndigheter som bedriver televerksamhet. Bestämmelserna torde ha begränsad betydelse sedan myndigheten Televerket upphörde. Eftersom det enligt uppgift finns vissa kommuner som tillhandahåller IP-telefoni kan dock bestämmelserna komma att aktualiseras. Offentlighets- och sekretesslagen innehåller regler som gör det möjligt för de brottsutredande myndigheterna att få uppgifter direkt från en myndighet som bedriver televerksamhet (10 kap. 23 §, se närmare avsnitt 4.2). Detta

är en slags dubbelreglering i förhållande till såväl rättegångsbalken som lagen om elektronisk kommunikation. Reglerna i offentlighets- och sekretesslagen tar sikte på uppgifter både i historisk tid och i realtid. Förutsättningarna för utlämnande överensstämmer till stora delar med reglerna i lagen om elektronisk kommunikation. En skillnad jämfört med regleringen i lagen om elektronisk kommunikation är att ett utlämnande av uppgifter enligt offentlighets- och sekretesslagen inte förutsätter en begäran från den brottsbekämpande myndigheten. Utlämnandet kan alltså ske på initiativ av den myndighet som bedriver televerksamheten.

Som BRU har föreslagit bör bestämmelserna i offentlighets- och sekretesslagen om undantag i sekretessen på samma sätt som motsvarande bestämmelser om utlämnande i lagen om elektronisk kommunikation upphävas. Bestämmelserna bör ersättas med en reglering som innebär en tydlig förstärkning av rättssäkerhets- och integritetsskyddet. Några remissinstanser som i och för sig välkomnar syftet att tillskapa en mer rättssäker ordning, har framfört mer övergripande kritik mot utredningens förslag. *Svenska Journalistförbundet* och *Post- och telestyrelsen* anser bl.a. att utredningen brister i redovisningen av avvägningen mellan brottsbekämpningsintressen och integritetsskyddsintressen. Andra remissinstanser, bl.a. *Åklagarmyndigheten* och *Rikspolisstyrelsen,* anser att inhämtningsmöjligheterna i vissa avseenden begränsas i alltför stor utsträckning. *Sveriges Advokatsamfund* har motsatt sig förslaget, men samtidigt anfört att det i vissa avseenden innebär en klar förbättring från rättssäkerhetssynpunkt jämfört med gällande rätt.

Det krävs ingående överväganden för att finna en rimlig balans mellan intresset av att effektivt kunna bekämpa brott och integritetsskyddsintresset. Bland annat *IT & Telekomföretagen, Juridiska fakultetsnämnden vid Stockholms universitet* och *Stockholms handelskammare* har framfört att beredningsunderlaget behöver kompletteras. Det är emellertid inte första gången frågan om att samla reglerna om utlämnande av uppgifter om elektronisk kommunikation till brottsbekämpande myndigheter i ett regelverk behandlas i lagstiftningssammanhang. I samband med att möjligheten att begära ut historiska uppgifter om telemeddelanden enligt rättegångsbalken infördes, diskuterades behovet av att ha kvar telelagens och sekretesslagens regler på området. I lagrådsremissen Hemlig avlyssning m.m. den 6 april 2000 (Ju1998/1450) föreslogs att de aktuella bestämmelserna i telelagen och sekretesslagen om skyldighet för operatörerna att i vissa fall lämna ut uppgifter till brottsutredande myndigheter skulle upphävas (lagrådsremissen s. 77). I den efterföljande propositionen togs förslagen emellertid inte med. Det uttalades då att frågan om att avskaffa möjligheten för brottsutredande myndigheter att inhämta uppgifter om telemeddelanden direkt från teleoperatörerna skulle bli föremål för ytterligare överväganden (prop. 2002/03:74 s. 12 och 40). Mot den bakgrunden gav regeringen Beredningen för rättsväsendets utveckling i uppdrag att bl.a. göra en översyn av det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation (dir. 2003:15). Uppdraget till BRU och därefter uppdraget till Polismetodutredningen har lett fram till de förslag som nu behandlas.

Regeringen anser därför att det inte finns behov av ytterligare beredningsunderlag.

Förslagen medför en ökad rättssäkerhet för den enskilde genom att inhämtningen omfattas av tydliga regler i fråga om bl.a. de syften för vilka inhämtning får ske, vem som får besluta om inhämtning och tillsyn över inhämtningen. Regeringen delar inte den av bl.a. IT- och Telekomföretagen framförda farhågan att förslagen kan komma att påverka slutanvändarnas tilltro till elektronisk kommunikation negativt. Som *Svenska Antipiratbyrån* har framfört bör den ökade rättssäkerheten i stället bidra till att öka detta förtroende.

Olika regler för inhämtning i förundersökningar och underrättelseverksamhet

Som Polismetodutredningen har redovisat ser de principer som styr och de målsättningar som gäller för underrättelseverksamhet respektive förundersökning olika ut (SOU 2009:1 s. 108 f.).

Under förundersökningen är syftet att utreda ett redan begånget brott och bl.a. i ett utredningsskede utröna vem eller vilka som skäligen kan misstänkas för brottet. Inhämtningen av uppgifter under en förundersökning sker riktat mot personer som misstänks vara delaktiga i brottet. Detta innebär, som utredningen har konstaterat, att partsintresset bör vara styrande för vilka principer som ska ligga till grund för regelsystemet. Det innebär också att integritetsaspekten under förundersökningen främst tar sikte på den övervakade personen som potentiell part. De principer som styr inhämtningen bör därför så långt det är möjligt anknyta till de rättssäkerhetsprinciper som gäller för den som är skäligen misstänkt. Inhämtning av uppgifter om elektronisk kommunikation i en förundersökning bör därför alltid ske inom ramen för ett tillstånd till hemlig övervakning av elektronisk kommunikation. Därigenom kommer inhämtningen att omfattas av rättegångsbalkens bestämmelser om tillstånd av domstol till hemlig övervakning, underrättelse till enskild och tillsyn av Säkerhets- och integritetsskyddsnämnden. Detta är från rättssäkerhetssynpunkt av stort värde.

I underrättelseverksamheten däremot är utgångspunkten, ofta utifrån en mer övergripande ansats, att studera och kartlägga en befarad brottslig verksamhet för att förebygga eller förhindra brott. Inhämtning av uppgifter om elektronisk kommunikation utgör naturligtvis även i detta skede ett intrång i den enskildes integritet. Å andra sidan är partsintresset inte lika framträdande som under en förundersökning. Det finns inte skäl att behandla den som berörs av ett beslut om inhämtning som en potentiell part, utan som en enskild som i och för sig blir föremål för integritetskänsliga åtgärder. Därtill kommer att det framåtblickande perspektivet i underrättelseverksamheten inte gör domstolsprövning lika naturlig som vid en tillbakablickande bedömning när ett brott redan har begåtts och där prövningen kan knytas till en historisk händelse. I stället får insyn och kontroll samt tillsyn utövad av ett fristående organ större betydelse än i en förundersökning. En informationsinhämtning i underrättelseverksamheten ställer därför höga krav på en systematisk och

kontinuerlig efterhandskontroll och tillsyn av verksamhetens lagenlighet, enhetlighet och lämplighet. Regeringen delar mot denna bakgrund utredningens uppfattning att underrättelseverksamheten bör regleras i särskild ordning.

Frågan blir då var den reglering som avser inhämtning i de brottsbekämpande myndigheternas underrättelseverksamhet bör placeras. I rättegångsbalken regleras endast sådan inhämtning som sker inom ramen för en förundersökning. Det saknas anledning att som *Sundsvalls tingsrätt* har föreslagit frångå denna ordning genom att där införa bestämmelser som rör underrättelseverksamhet. Lagen om elektronisk kommunikation är en huvudsakligen näringsrättslig lagstiftning som syftar till att enskilda och myndigheter ska få tillgång till säker och effektiv elektronisk kommunikation och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster samt deras pris och kvalitet (1 kap. 1 § lagen om elektronisk kommunikation). Att som *Hovrätten för Västra Sverige* har föreslagit införa bestämmelserna i ett särskilt kapitel i den lagen framstår därför inte som ändamålsenligt. Bestämmelser om inhämtning av övervakningsuppgifter i underrättelseverksamhet finns också i lagen (1991:572) om särskild utlänningskontroll och i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Som utredningen funnit kan det emellertid inte anses ändamålsenligt att införa nu aktuella bestämmelser i någon av dessa lagar. Regeringen delar utredningens bedömning att det i stället är mest lämpligt att befogenheterna att inhämta uppgifter från operatörerna regleras särskilt. Regeringen föreslår därför att bestämmelsen tas in i en ny lag om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

6.2 Inhämtning av uppgifter om elektronisk kommunikation i förundersökningar

6.2.1 Tillgång till övervakningsuppgifter vid hemlig avlyssning

Regeringens förslag: Ett tillstånd till hemlig avlyssning av elektronisk kommunikation ska även ge rätt att inhämta övervakningsuppgifter och att hindra meddelanden från att komma fram.

BRU:s förslag: Överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans har motsatt sig förslaget.

Skälen för regeringens förslag: Som framgår ovan innebär hemlig avlyssning av elektronisk kommunikation att innehållet i ett meddelande blir tillgängligt medan hemlig övervakning av elektronisk kommunikation ger andra uppgifter om meddelandet, t.ex. uppgifter om uppringt eller uppringande nummer, start- och sluttid, antalet ringsignaler, IMEI-nummer (se närmare avsnitt 5.4) och lokalisering. Hemlig övervakning av elektronisk kommunikation kan även innebära att ett meddelande hindras från att komma fram.

När det gäller den teknik som används i sammanhanget har BRU angett att den bygger på internationell standard som vid hemlig teleavlyssning också medger tillgång till vissa teleövervakningsuppgifter

även om det i och för sig är möjligt att separera de två typerna av information.

BRU har anfört att det i de allra flesta fall är nödvändigt för de brottsutredande myndigheterna att få tillgång till övervakningsuppgifter även vid hemlig avlyssning. Ansökan om tillstånd till båda tvångsmedlen görs därför normalt samtidigt. Mot denna bakgrund har BRU föreslagit att tillstånd till hemlig avlyssning även ska innefatta tillstånd att inhämta övervakningsuppgifter och att hindra meddelanden från att komma fram.

Som *Åklagarmyndigheten* framhållit har BRU:s förslag klara effektivitetsvinster. Om det finns tillräckliga skäl för hemlig avlyssning, finns det så gott som alltid skäl för hemlig övervakning. Av regeringens skrivelse till riksdagen Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2008, framgår att vid samtliga tillstånd till hemlig teleavlyssning under 2008 meddelades samtidigt beslut om tillstånd till hemlig teleövervakning. Av den senaste redovisningen som Åklagarmyndigheten och Rikspolisstyrelsen har lämnat till regeringen framgår att det förhöll sig på samma sätt med användningen av dessa tvångsmedel under år 2009 (Ju2010/5064/Å). Förutom att detta förhållandet visar att BRU:s förslag skulle leda till effektivitetsvinster leder det till slutsatsen att ett inhämtande av övervakningsuppgifter när det finns skäl för den betydligt mer integritetskränkande åtgärden hemlig avlyssning bör anses rimlig från integritetssynpunkt. Regeringen föreslår därför att ett tillstånd till hemlig avlyssning av elektronisk kommunikation ska ge rätt att inhämta olika slag av övervakningsuppgifter och att hindra meddelanden från att komma fram.

6.2.2 Tillstånd till hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för ett brott

Regeringens förslag: Hemlig övervakning av elektronisk kommunikation ska i vissa fall få användas utan krav på koppling till en skäligen misstänkt person. En förutsättning är att förundersökningen rör brott för vilket det inte är föreskrivet lindrigare straff än fängelse två år, försök, förberedelse eller stämpling till sådant brott, om sådan gärning är belagd med straff, eller annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år. I fråga om uppgifter som rör ett särskilt meddelande ska inhämtningen endast få avse historiska uppgifter. Syftet med övervakningen måste vara att utreda vem som skäligen kan misstänkas för brottet. Tillstånd till åtgärden ska ges av domstol.

Polismetodutredningens förslag: Överensstämmer delvis med regeringens. Polismetodutredningen har dock föreslagit att syftet med åtgärden, förutom att fastställa vem som skäligen kan misstänkas för brottet, ska kunna vara att utröna annan omständighet av väsentlig betydelse för utredningen. Utredningen har vidare föreslagit att frågor om hemlig teleövervakning i nu aktuella fall vid sidan av domstol även ska få prövas av undersökningsledaren eller åklagaren om åtgärden inte kan

antas bli av stor omfattning eller av särskilt ingripande slag. Enligt förslaget ska, om den hemliga övervakningen avser en viss adress, den som innehar adressen kunna begära rättens prövning av beslutet.

Remissinstanserna: *Ekobrottsmyndigheten* och *Åklagarmyndigheten* har tillstyrkt att inhämtning ska få ske i fråga om brott av föreslagen svårhetsgrad. *Rikspolisstyrelsen* har framfört att samma straffröskel bör gälla som för beslut om hemlig teleövervakning i förundersökningar i övrigt. *Sundsvalls tingsrätt* anser det vara tveksamt att knyta bestämmelsen till straffvärde innan det finns en skäligen misstänkt.

Åklagarmyndigheten, Rikspolisstyrelsen och *Ekobrottsmyndigheten* har framfört att domstol endast undantagsvis bör fatta beslut om hemlig teleövervakning innan det finns en skäligen misstänkt. *JO*, *Sveriges Advokatsamfund* och *Datainspektionen* har invänt att domstolsprövning bör vara huvudregeln inom en förundersökning även innan det finns en skäligen misstänkt.

Post- och Telestyrelsen och *Sveriges Advokatsamfund* har framfört att frågan om offentliga ombuds närvaro vid beslut om hemlig teleövervakning behöver utredas. Enligt Post- och Telestyrelsen bör offentliga ombud ha en roll vid inhämtning av uppgifter om elektronisk kommunikation såväl i underrättelseskedet som i en förundersökning.

Sundsvalls tingsrätt har vidare haft synpunkter bl.a. på möjligheten till överklagande och på vilka tingsrätter som bör handlägga denna typ av ärenden.

Skälen för regeringens förslag

En möjlighet att besluta om hemlig övervakning utan skälig misstanke

Rättegångsbalkens regler om hemlig teleövervakning innebär bl.a. att tvångsmedlet får användas endast om någon är skäligen misstänkt för brott (27 kap. 20 § första stycket). Något krav på att det finns en skäligen misstänkt person gäller dock inte för att de brottsutredande myndigheterna med stöd av reglerna i lagen (2003:389) om elektronisk kommunikation från operatörerna ska få ta del av uppgifter som angår särskilda elektroniska meddelanden (6 kap. 22 § första stycket 3 i den lagen).

Regeringen föreslår i avsnitt 6.1 att de aktuella bestämmelserna om skyldighet för operatörer att lämna ut uppgifter till brottsbekämpande myndigheter ska upphävas. De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation i en förundersökning ska uteslutande regleras i rättegångsbalken enligt bestämmelserna om hemlig avlyssning respektive hemlig övervakning av elektronisk kommunikation. Mot denna bakgrund finns det skäl att överväga om det även i fortsättningen ska krävas att det finns en skäligen misstänkt person för att hemlig övervakning ska få ske.

Redan år 2000 föreslogs i lagrådsremissen Hemlig avlyssning m.m. att bestämmelserna om operatörers skyldighet att i vissa fall lämna ut uppgifter om ett särskilt telemeddelande till brottsutredande myndigheter skulle upphävas (s. 77). Samtidigt föreslogs att hemlig teleövervakning utan någon skäligen misstänkt person skulle tillåtas i vissa fall. Förslaget ledde emellertid inte till lagstiftning.

Även BRU har föreslagit en sådan reglering med motiveringen att det finns ett mycket stort behov av övervakningsuppgifter i ett tidigt utredningsskede, däribland uppgifter om positionen hos mobiltelefoner. Sådana uppgifter är enligt BRU ofta av stor vikt för att utredningar rörande grövre brott ska kunna föras framåt (SOU 2005:38 s. 194). Polisen kan bearbeta och analysera övervakningsuppgifterna och jämföra dem med andra uppgifter, t.ex. från vittnen, och på så sätt försöka utröna vilken eller vilka personer som kan misstänkas för brottet i fråga. I vissa fall kan det också vara möjligt att efter en analys av övervakningsuppgifterna komma fram till var flera gärningsmän sammanträffade, vilka flyktvägar som användes, m.m. Kartläggningen av flyktvägar kan i vissa fall leda till att de misstänktas kontakter med varandra blir utredda, att gömställen upptäcks och stulet gods påträffas, m.m. Polismetodutredningen har också framhållit att en sådan möjlighet är nödvändig för att kunna upprätthålla en effektiv brottsbekämpning (SOU 2009:1 s 114).

Tillgången till uppgifter om elektronisk kommunikation i ett tidigt skede i en brottsutredning är ofta av central betydelse för att effektivt kunna klara upp allvarliga brott. Det är många gånger avgörande att snabbt kunna utröna vem som är skäligen misstänkt för att andra åtgärder ska kunna vidtas mot denne i syfte att föra utredningen framåt. Vid sådan inhämtning är det av naturliga skäl inte möjligt att koppla åtgärden till en skäligen misstänkt person. Regeringen anser därför att de brottsutredande myndigheterna även i framtiden måste kunna få tillgång till uppgifter om elektronisk kommunikation i förundersökningar, även innan det finns en skäligen misstänkt gärningsman. Frågan är då hur bestämmelserna bör utformas för att motsvara de behov som finns och samtidigt vara godtagbara från integritetssynpunkt. Det finns inte anledning att göra undantag från rättegångsbalkens krav på att åtgärden ska vara av synnerlig vikt för utredningen (27 kap. 20 §). Nedan övervägs vilka ytterligare förutsättningar som ska gälla för inhämtandet.

Proportionalitetsprincipen

Som framgår av avsnitt 4.1 gäller proportionalitetsprincipen vid beslut om och användning av tvångsmedel. Den brukar i korthet beskrivas så att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med den. Principen har, när det gäller hemlig teleövervakning, uttryckts i 27 kap. 1 § RB och kommer att gälla även för situationer där åtgärden vidtas i syfte att utreda vem som skäligen kan misstänkas för brottet i fråga.

Vilka uppgifter ska omfattas av inhämtningen?

Enligt utredningen bör inhämtning vara möjlig i fråga om historiska uppgifter som rör ett särskilt meddelande. Ingen remissinstans har invänt mot den bedömningen. Det motsvarar den inhämtning som enligt nuvarande ordning sker med stöd av bestämmelserna i lagen om elektronisk kommunikation. Regeringen gör i denna del ingen annan

bedömning än utredningen. (Lokaliseringsuppgifter som inte har koppling till ett särskilt meddelande behandlas i avsnitt 6.4.)

Brottens svårhetsgrad

Enligt 27 kap. 19 och 20 §§ rättegångsbalken får hemlig teleövervakning användas när förundersökningen avser ett brott för vilket det inte är förskrivet lindrigare straff än sex månaders fängelse eller dataintrång, barnpornografibrott som inte är ringa, narkotikabrott eller narkotikasmuggling eller försök, förberedelse eller stämpling till sådant brott om gärningen är belagd med straff. För att de brottsbekämpande myndigheterna ska få inhämta motsvarande uppgifter enligt 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation krävs däremot att det finns misstanke om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Detta innebär bl.a. att inga försöks-, förberedelse- eller stämplingsbrott omfattas av bestämmelsen. Det betyder t.ex. att ett grovt rån som misslyckas i den meningen att gärningsmännen inte får med sig något av värde, inte omfattas av den senare regleringen. Detsamma gäller t.ex. fall av oprovocerat gatuvåld som är så allvarligt att det bedöms som försök till mord. Både BRU och Polismetodutredningen har pekat på behovet för de brottsbekämpande myndigheterna att i framtiden få tillgång till övervakningsuppgifter vid fler brott när det saknas en skäligen misstänkt person.

Som *Rikspolisstyrelsen* har anfört är det rimligt att förvänta sig att de brottsbekämpande myndigheternas möjligheter att klara upp brott skulle öka om inhämtning vore möjlig för samma brott som vid hemlig övervakning av elektronisk kommunikation i övrigt. Inhämtningen sker dock i ett mycket tidigt skede i brottsutredningen och riktas mot någon som inte är skäligen misstänkt för brott. Regeringen anser därför, när det gäller brottets svårhetsgrad, att kraven bör vara högre än för hemlig övervakning av elektronisk kommunikation i andra fall. Det synsättet överensstämmer också med gällande rätt. Som Polismetodutredningen anfört är det rimligt att tillåta hemlig övervakning vid brott som ger möjlighet att använda det klart mer integritetskänsliga tvångsmedlet hemlig avlyssning av elektronisk kommunikation mot en skäligen misstänkt person. Detta innebär en viss utvidgning i förhållande till den nuvarande regleringen i 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation. Även brott vars straffvärde överstiger fängelse i två år omfattas liksom försök, förberedelse och stämpling till brott med minimistraff om fängelse två år. Det kan t.ex. röra sig om rån av allvarligt slag som ändå inte kan kvalificeras som grovt. Det finns ett stort behov i brottsbekämpningen av tillgång till uppgifter om dessa typer av brott. Intresset av att skydda enskildas integritet bör inte hindra en sådan reglering, särskilt som brottslighetens svårhetsgrad vid hemlig övervakning av elektronisk kommunikation i dessa fall kommer att bli densamma som för hemlig avlyssning av elektronisk kommunikation. Det kan naturligtvis, som *Sundsvalls tingsrätt* har framfört, vara svårt att bedöma straffvärdet i ett så tidigt skede, bl.a. eftersom det då inte är möjligt att ta hänsyn till subjektiva omständigheter knutna till gärningsmannen. Regeringen anser dock att dessa svårigheter inte ska

överdrivas. Motsvarande synpunkt framfördes i samband med att en straffvärdeventil infördes för beslut om hemlig avlyssning. Regeringen anförde då (prop. 2002/03:74 s. 32 f.) att det inte torde föreligga någon avgörande skillnad mellan att på ett tidigt stadium bedöma om ett brott ska rubriceras på sådant sätt att en minimistraffregel är uppfylld och att göra en bedömning av detta brotts straffvärde. Att utredningen i vissa fall kan vara mindre robust ska räknas den misstänkte till godo, dvs. att en marginal till förmån för den misstänkte måste vägas in. Det finns enligt regeringen inte skäl att i det här sammanhanget göra någon annan bedömning.

Vilket syfte ska åtgärden ha och vilka övriga krav ska ställas på den?

Polismetodutredningens förslag innebär att hemlig övervakning som inte riktas mot en skäligen misstänkt person ska syfta till att fastställa vem som är skäligen misstänkt eller att utröna annan omständighet av väsentlig betydelse för utredningen. Regeringen delar utredningens bedömning att en begränsning bör införas i fråga om för vilka syften inhämtning ska vara möjlig. För den uppfattningen talar också Europakonventionens krav på klarhet och förutsebarhet i fråga om regler om intrång i skyddet för privatliv och korrespondens.

Att begränsa bestämmelsens syfte till att avse endast skedet i en förundersökning innan det finns en skäligen misstänkt person är som Polismetodutredningen har framfört inte lämpligt eftersom det då inte skulle vara möjligt att använda bestämmelsen för att kunna utreda om det finns ytterligare misstänkta för brottet. En annan möjlighet, som Polismetodutredningen har berört, är att begränsa inhämtningen till sådana fall där syftet är att fastställa vem som skäligen kan misstänkas för ett brott. En sådan begränsning finns t.ex. i fråga om hemlig kameraövervakning när det saknas en skäligen misstänkt person. Enligt förarbetena till den bestämmelsen innebär rekvisitet att övervakningen i princip ska vara avsedd att leda till att gärningsmannen kan påträffas på bar gärning (prop. 2002/03:74 s. 40 f.). Som Polismetodutredningen har konstaterat skulle även en sådan ordning innebära en alltför omfattande begränsning i fråga om när inhämtning får ske. Det bör även fortsättningsvis vara möjligt att inhämta uppgifter om elektronisk kommunikation i en förundersökning, trots att övervakningen inte kan förväntas få som direkt effekt att det kan fastställas vem som skäligen är misstänkt för brottet på det sätt som förutsätts enligt ovan nämnda bestämmelser om hemlig kameraövervakning. Åtgärden bör t.ex. kunna ta sikte på att utröna var en brottsplats är belägen om den omständigheten är av avgörande betydelse för att utreda vem som skäligen kan misstänkas för brottet. Regeringen anser dock inte att detta bör komma till uttryck på det sätt som utredningen föreslagit, dvs. att inhämtning ska kunna ske i syfte att utröna en omständighet av väsentlig betydelse för utredningen. En sådan reglering skulle i praktiken innebära en utvidgning av möjligheten att besluta om hemlig övervakning av elektronisk kommunikation mot en skäligen misstänkt person, något som inte är avsett. Mot den angivna bakgrunden anser regeringen att syftet med åtgärden bör vara att *utreda* vem som skäligen kan misstänkas för brottet.

Vem ska ge tillstånd till åtgärden?

Utredningen har föreslagit att undersökningsledare eller åklagare vid sidan av domstol ska få ge tillstånd till hemlig övervakning av elektronisk kommunikation i syfte att fastställa vem som skäligen kan misstänkas för brottet om åtgärden inte kan antas bli av stor omfattning eller särskilt ingripande slag. Om tillståndet avser en särskild teleadress ska den som innehar den teleadress som tillståndet avser enligt förslaget kunna begära rättens prövning av tillståndet.

Ett av skälen för att upphäva de aktuella reglerna i lagen om elektronisk kommunikation och samla reglerna om de brottsutredande myndigheternas tillgång till elektronisk kommunikation i en förundersökning till rättegångsbalken är att få ett mer rättssäkert och enhetligt system. Detta talar för att ha samma beslutsordning för alla beslut om tillstånd till hemlig övervakning av elektronisk kommunikation. Flera remissinstanser har sett behov av förtydliganden av i vilka fall beslut ska kunna fattas av åklagare/förundersökningsledare och i vilka fall beslut ska fattas av domstol. Både *JO* och *Datainspektionen* har invänt mot utredningens bedömning att en basstationstömning inte kan anses vara en åtgärd av stor omfattning eller särskilt ingripande slag och framfört att domstol bör fatta beslut i dessa frågor. *Åklagarmyndigheten* har framfört att det bör förtydligas att domstolsbeslut ska krävas endast i utpräglade undantagssituationer. Att remissinstanserna har haft olika uppfattning om vilka åtgärder som ska anses vara av stor omfattning eller särskilt ingripande slag tyder på en risk för att det skulle leda till praktiska tillämpningssvårigheter att införa en särskild beslutanderätt för vissa fall innan det finns en skäligen misstänkt person. En sådan ordning skulle också göra systemet mindre överskådligt.

Som bl.a. *Sundsvalls tingsrätt* har påpekat framstår vidare den föreslagna möjligheten till överprövning i praktiken som alltför begränsad. Den som övervakningen avser ska normalt sett inte ha kännedom om åtgärden och har därför inte möjlighet att begära rättens prövning. Regeringen anser därför att rättssäkerhetsskäl talar för att domstolsprövning bör ske även i dessa fall. Flera av de brottsbekämpande myndigheterna har framhållit att beslut ibland kan behöva fattas mycket skyndsamt. Det utgör dock inte skäl att avstå från en ordning med en slutlig domstolsprövning. En sådan skyndsamhet kan i stället åstadkommas genom att åklagare ges rätt att fatta interimistiska beslut om hemlig övervakning av elektronisk kommunikation. Frågan om en sådan ordning bör införas behandlas i avsnitt 6.2.3.

Sundsvalls tingsrätt har påtalat att det bör övervägas att lägga beslutanderätten på en eller flera större domstolar eftersom den domare som beslutat om hemliga tvångsmedel inte bör handlägga det efterkommande brottmålet vilket kan leda till svårigheter för mindre domstolar. Regeringen anser det dock inte vara lämpligt att på detta område överväga en annan reglering än den som gäller för hemliga tvångsmedel i övrigt.

Offentliga ombud

Polismetodutredningen har angett att frågan om offentliga ombuds medverkan vid hemlig övervakning av elektronisk kommunikation bör avgöras i hela dess vidd, dvs. för samtliga fall där hemlig övervakning av elektronisk kommunikation kan beslutas enligt rättegångsbalken och att det ligger utanför utredningens uppdrag att överväga en sådan ordning. *Sveriges Advokatsamfund* har anfört att denna fråga är grundläggande för rättssäkerheten och inte kan lämnas outredd. Även *Post- och telestyrelsen* har framfört synpunkten att frågan bör utredas och att offentliga ombud bör bevaka enskildas integritetsintressen vid de beslut som fattas.

När bestämmelserna om offentliga ombud infördes ansågs behovet av sådana ombud vara mindre vid hemlig övervakning än vid hemlig teleavlyssning och reglerna kom inte att omfatta sådan övervakning (se prop. 2002/03:74 s. 22 f.). Sedan dess har integritetsskyddet vid hemlig teleövervakning stärkts genom införandet av bestämmelserna om underrättelse till enskild vid hemlig tvångsmedelsanvändning och inrättandet av Säkerhets- och integritetsskyddsnämnden som tillsynsmyndighet på området. *Post- och telestyrelsen* har som skäl för sin uppfattning framfört att offentliga ombud behövs för att balansera de brottsbekämpande myndigheternas utökade möjligheter att inhämta uppgifter om elektronisk kommunikation med de begränsade möjligheter till domstolsprövning som utredningens förslag innebär. Regeringens förslag innebär emellertid att det ställs högre krav på tillståndsgivningen än enligt nuvarande ordning och att kontrollfunktionerna för tillståndsgivningen stärks. Mot den angivna bakgrunden anser regeringen att förslaget om en utökad möjlighet att besluta om hemlig övervakning av elektronisk kommunikation enligt rättegångsbalken kan genomföras trots att frågan om offentliga ombuds medverkan vid sådan tillståndsprövning inte har utretts i detta sammanhang.

6.2.3 En möjlighet för åklagare att i brådskande fall fatta interimistiska beslut

Regeringens förslag: Kan det befaras att inhämtande av rättens tillstånd till hemlig övervakning av elektronisk kommunikation skulle medföra fördröjning eller annan olägenhet av väsentlig betydelse får tillstånd till åtgärden ges av åklagaren. Ett sådant beslut ska genast anmälas hos rätten, som skyndsamt ska pröva om det finns skäl för åtgärden. Har åtgärden upphört att gälla ska rätten pröva om det har funnits skäl för den. Finner rätten att det har saknats skäl för åtgärden får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av övervakningen.

Förslaget om interimistisk beslutanderätt för åklagare medför följdändringar i rättegångsbalken och i lagen (2000:562) om internationell rättslig hjälp i brottmål.

Polismetodutredningens förslag: Överensstämmer delvis med regeringens förslag. Utredningen har dock föreslagit att någon

domstolsprövning inte ska ske om åtgärden har upphört att gälla innan rätten har prövat ärendet. I stället ska åklagaren enligt förslaget anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden.

Remissinstanserna: *Göta hovrätt, Malmö tingsrätt, Sundsvalls tingsrätt, Åklagarmyndigheten, Rikspolisstyrelsen* och *Tullverket* har tillstyrkt förslaget. *Åklagarmyndigheten, Ekobrottsmyndigheten* och *Rikspolisstyrelsen* har särskilt betonat betydelsen av att snabbt få tillgång till uppgifterna. Flera myndigheter har framfört att möjligheten för åklagare att fatta interimistiska beslut är av stor vikt.

JO har uttalat att man bör överväga åtgärder angående domstolarnas beredskap om en domstolsprövning inte anses tillgodose kraven på snabba ställningstaganden.

Sveriges advokatsamfund har framfört att det är svårt att se något avgörande skäl till att åklagaren ska ges möjlighet att fatta interimistiska beslut. Samfundet har vidare angett att det inte är tillfredsställande att uppgifter som inhämtats genom ett beslut om tvångsmedel som undanröjs eller skulle ha undanröjts av domstol kan användas i den fortsatta förundersökningen. *Rikspolisstyrelsen* har efterlyst ett klargörande i fråga om vad som ska ske med uppgifter som har inhämtats om rätten upphäver ett beslut som har fattats av undersökningsledare eller åklagare.

Rikspolisstyrelsen har också framhållit att det i de aktuella författningarna tydligt bör framgå att en begäran till en teleoperatör om uppgifter från en brottsbekämpande myndighet ska handläggas skyndsamt. *IT & Telekomföretagen, HiG3 Access AB, Telenor Sverige AB och TeliaSonera AB* har framfört att behovet av ”minutoperativa beslut” skulle kunna innebära krav på att operatörerna tillhandahåller 24-timmarsservice, vilket skulle medföra väsentligt ökade kostnader, särskilt för mindre operatörer.

Skälen för regeringens förslag

Gällande rätt

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

Enligt rättegångsbalkens nuvarande regler ska ett beslut att tillåta hemlig avlyssning eller övervakning alltid fattas av domstol (27 kap. 21 §). Som framgår av det föregående kan övervakningsuppgifter avseende förfluten tid erhållas även direkt från operatörerna med stöd av

reglerna i lagen om elektronisk kommunikation (6 kap. 22 § första stycket 3).

I lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott finns i 4 § ett undantag från regeln om domstolsbeslut. Där anges att tillstånd till hemlig teleövervakning i de fall som omfattas av lagen får ges av åklagaren om det kan befaras att inhämtande av rättens tillstånd till hemlig teleövervakning skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen. Det anges också att åklagaren genast ska göra anmälan om åtgärden hos rätten, som skyndsamt ska pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden ska den upphäva beslutet. Skulle däremot åtgärden ha upphört att gälla innan rätten har prövat ärendet, ska åklagaren anmäla ärendet till Säkerhets- och integritetsskyddsnämnden (6 §).

Åklagare får möjlighet att intermistiskt ge tillstånd till hemlig övervakning av elektronisk kommunikation

Mot bakgrund av att regeringen föreslår att den nuvarande möjligheten för brottsbekämpande myndigheter att snabbt få tillgång till historiska uppgifter som rör ett elektroniskt meddelande genom lagen om elektronisk kommunikation tas bort (avsnitt 6.1) aktualiseras frågan om det finns anledning att införa en rätt för åklagare att ge interimistiskt tillstånd till hemlig övervakning av elektronisk kommunikation.

Frågan om en interimistisk beslutanderätt har diskuterats i tidigare lagstiftningsärenden. I förarbetena till ändringar i reglerna om hemliga tvångsmedel år 1989 uttalades att någon befogenhet för åklagare att fatta interimistiska beslut om teleavlyssning och teleövervakning inte borde införas, om inte tvingande praktiska behov talade för det. Sådana behov ansågs då inte föreligga (prop. 1988/89:124 s. 51 f.). Buggningsutredningen föreslog år 1998 att en möjlighet för åklagare att fatta interimistiska beslut om hemlig teleövervakning, hemlig teleavlyssning och hemlig kameraövervakning skulle införas (SOU 1998:46 s. 414 f.). Remissutfallet var blandat. I propositionen 2002/03:74 Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering gjordes bedömningen att det inte borde införas någon möjlighet för åklagare att enligt rättegångsbalken fatta interimistiska beslut om hemliga tvångsmedel. Det angavs att det inte hade framkommit så starka skäl som krävs för att i rättegångsbalken införa ett system där integritetskänsliga hemliga tvångsmedel får verkställas utan rättens tillstånd (s. 42 f.). Den dåvarande regeringen angav att man hade för avsikt att noga följa utvecklingen och vid behov pröva frågan på nytt. BRU föreslog att en möjlighet för åklagare att ge interimistiskt tillstånd till hemlig teleövervakning skulle införas i rättegångsbalken och motiverade det främst med behovet av snabba avgöranden (SOU 2005:38 s. 200 f.).

Flera remissinstanser har betonat behovet av ett snabbt förfarande när frågor om användning av hemliga tvångsmedel enligt rättegångsbalkens regler aktualiseras. Snabbheten i förfarandet är ofta en avgörande faktor för ett lyckat utredningsresultat. Det gäller särskilt som de personer som är delaktiga i grov brottslighet många gånger aktivt vidtar åtgärder i syfte

att försvåra myndigheternas brottsbekämpande insatser, t.ex. genom att med regelbundenhet byta mobiltelefoner eller kontantkort. Domstolarna har i och för sig möjlighet att ta om hand brådskande frågor om tvångsmedel, men någon beredskap för omedelbara beslut dygnet runt finns inte. Det är inte heller rimligt att bygga upp en sådan organisation för att tillstånd ska kunna ges mycket snabbt under dygnets alla timmar. Regeringen delar därför uppfattningen att det är nödvändigt för en effektiv brottsbekämpning att tillstånd till hemlig övervakning av elektronisk kommunikation kan ges snabbare än vad som är möjligt vid en exklusiv domstolsprövning. För att åstadkomma detta anser regeringen att åklagaren bör ges möjlighet att interimistiskt tillåta hemlig övervakning av elektronisk kommunikation. Åklagaren måste som förundersökningsledare vara väl insatt i ärendet och bör på ett objektivt och effektivt sätt snabbt kunna ta ställning till en tvångsmedelsfråga av detta brådskande slag.

Att de brottsbekämpande myndigheterna snabbt ska kunna få tillgång till uppgifterna förutsätter naturligtvis också att utlämnandet från operatörerna kan ske utan dröjsmål. En sådan ordning krävs dessutom i fråga om de uppgifter som omfattas av lagringsskyldigheten i EU:s direktiv om lagring av trafikuppgifter. Den särskilda anpassningsskyldighet som föreslagits i propositionen Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG (prop. 2010/11:46) för uppgifter som har lagrats med stöd av direktivet innehåller således ett krav på att dessa uppgifter ska lämnas ut utan dröjsmål.

Obligatorisk domstolsprövning av interimistiska beslut

Ett beslut av åklagaren bör som utredningen har föreslagit genast anmälas hos rätten. I fråga om tillstånd till inhämtning avseende historiska uppgifter upphör åtgärden när de uppgifter som begärts utlämnade har lämnats ut. Om rätten då inte redan har prövat frågan kommer det enligt utredningens förslag inte att ske någon domstolsprövning, utan beslutet ska i stället anmälas till Säkerhets- och integritetsskyddsnämnden. En sådan ordning gäller för interimistiska beslut enligt 2008 års tvångsmedelslag. Med hänsyn till vad som anförs ovan om vikten av ett snabbt förfarande, är det sannolikt att utredningens förslag i praktiken i många fall skulle innebära en slutlig beslutanderätt för åklagare. En sådan effekt kan enligt regeringen starkt ifrågasättas. Regeringen delar därmed inte utredningens uppfattning att regleringen i 2008 års tvångsmedelslag bör tjäna som förebild för en reglering i nu aktuellt avseende.

Regeringen föreslår i stället att det av integritets- och rättssäkerhetsskäl införs en obligatorisk domstolsprövning av interimistiska beslut. Det innebär att rätten ska pröva åtgärden också i de fall den har upphört. En sådan reglering gäller i Danmark och Norge (71 kap. 783 § lov om rettens pleje och 16 a kap. 216 d § lov om rettegangsmåten i straffesaker). En reglering av det slaget gör att domstolspraxis kan utvecklas i fråga om de närmare förutsättningarna för interimistiska tillstånd till hemlig övervakning av elektronisk kommunikation och att

tillståndsgivningen alltid kommer att prövas av en från de brottsbekämpande myndigheterna fristående instans. Härigenom ges goda förutsättningar för enhetlighet och hög kvalitet i åklagarnas beslutsfattande. När åtgärden har upphört ska rättens prövning ske med utgångspunkt i förhållandena vid tidpunkten för åklagarens beslut.

Användandet av uppgifter som inhämtats genom ett interimistiskt beslut

Rikspolisstyrelsen har efterlyst ett förtydligande av vad som ska ske med uppgifter som har inhämtats om rätten upphäver beslutet. *Sveriges Advokatsamfund* har framfört att det inte är tillfredsställande från rättssäkerhetssynpunkt att uppgifter som framkommit vid ett beslut om tvångsmedel som undanröjs av domstol kan användas i den fortsatta förundersökningen. Regeringen konstaterar att själva inhämtningen av uppgifter innebär ett intrång i den enskildes privatliv som kan uppfattas som integritetskränkande. Att använda uppgifterna i en brottsutredning mot en person kan sägas innebära att integritetsintrånget tillåts fortsätta. Lämpligheten av att fritt kunna använda uppgifter som framkommit vid ett interimistiskt beslut som upphävts av domstol kan därför ifrågasättas. Ett generellt förbud mot sådan användning skulle dock föra för långt. Användning som är till fördel för en misstänkt person måste alltid tillåtas. Uppgifterna bör dock inte få användas i en brottsutredning till nackdel för någon som har omfattats av inhämtningen. Det bör dock framhållas att rättens beslut att upphäva åklagarens interimistiska beslut om hemlig övervakning av elektronisk kommunikation inte hindrar att rätten eller åklagaren om förhållandena ändras fattar ett nytt beslut om övervakning avseende samma historiska uppgifter.

Behov av följdändringar

En följd av regeringens förslag är att bestämmelsen i 27 kap. 25 § första stycket rättegångsbalken, som anger att tekniska hjälpmedel får användas vid verkställigheten av domstols beslut om hemlig avlyssning eller övervakning, bör justeras så att den omfattar även åklagares interimistiska beslut om hemlig övervakning av elektronisk kommunikation.

Förslaget ger också anledning att ifrågasätta om det fortsättningsvis finns behov av en bestämmelse om interimistisk beslutanderätt för åklagare i fråga om hemlig övervakning av elektronisk kommunikation i 2008 års tvångsmedelslag (4 §). Eftersom lagen är tidsbegränsad och under utvärdering, avstår regeringen dock från att i detta sammanhang föreslå några ändringar i den lagen. Även enligt lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. har åklagaren en möjlighet att fatta interimistiska beslut om hemlig övervakning av elektronisk kommunikation.

Lagen (2000:562) om internationell rättslig hjälp i brottmål innehåller regler om åklagares och domstolars samarbete över gränserna i brottsutredningar och brottmålsrättegångar (se närmare avsnitt 4.2). Reglerna knyter an till vad som gäller för att motsvarande åtgärder ska få

vidtas i en svensk förundersökning eller rättegång. Åtgärderna vidtas således under samma förutsättningar som i en svensk förundersökning enligt rättegångsbalken (prop. 1999/2000:61 s. 97). Mot denna bakgrund anser regeringen att de nu föreslagna reglerna som ger åklagare möjlighet att fatta interimistiska beslut i vissa fall bör gälla även enligt den lagen. Uppgifterna bör dock inte få lämnas över till den ansökande staten innan rätten har fattat ett beslut om hemlig övervakning av elektronisk kommunikation. Vad gäller tillstånd i Sverige till gränsöverskridande hemlig övervakning finns det dock inte behov av en möjlighet för åklagaren att fatta interimistiska beslut.

6.3 Inhämtning av uppgifter i underrättelseverksamhet

6.3.1 När ska inhämtning få ske?

Regeringens förslag: I underrättelseverksamhet ska övervakningsuppgifter om elektronisk kommunikation få hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år.

Inhämtning ska också under samma förutsättningar enligt en bestämmelse som ska tidsbegränsas till utgången av år 2012 få ske beträffande brottslig verksamhet som innefattar

1. sabotage enligt 13 kap. 4 § brottsbalken,
2. kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,
4. spionerі, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet, grovt brott, enligt 19 kap. 5 eller 8 eller 10 § tredje stycket brottsbalken, och
5. grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.

Inhämtning får beslutas och genomföras endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Polismetodutredningens förslag: Överensstämmer delvis med regeringens. Enligt utredningen ska inhämtning kunna ske i en undersökning om det finns särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka viss brottslig verksamhet. Utredningens förslag omfattar även brottslig verksamhet som innefattar olovlig kårverksamhet, brott mot medborgerlig frihet, obehörig befattning med hemlig uppgift, olovlig underrättelseverksamhet och företagsspionerі enligt 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller

av någon som har agerat för en främmande makts räkning. Utredningens förslag omfattar däremot inte grovt brott enligt 6 § lagen om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet (som trätt i kraft den 1 december 2010). Utredningen har inte beträffande någon bestämmelse föreslagit en tidsbegränsad giltighet.

Remissinstanserna: *Göta hovrätt* och *Säkerhetspolisen* har tillstyrkt förslaget. Säkerhetspolisen har särskilt framhållit att det är nödvändigt att de i brottskatalogen angivna brotten mot rikets säkerhet omfattas av regleringen. *Juridiska fakultetsnämnden vid Stockholms universitet* har avstyrkt att inhämtning ska vara möjlig i fråga om olovlig kårverksamhet eftersom det enligt nämnden kan komma att stå i strid med förbudet mot åsiktsregistrering i 2 kap. 3 § regeringsformen.

Ekobrottsmyndigheten, Åklagarmyndigheten och *Skatteverket* har framfört att det bör införas en straffvärdeventil även för underrättelseverksamheten för att inte en stor del av den grova organiserade brottsligheten ska falla utanför regleringen. Även *Kustbevakningen, Rikspolisstyrelsen* och *Tullverket* har framfört synpunkten att två års straffminimum är ett för högt ställt krav. *Rikspolisstyrelsen* har föreslagit att inhämtning ska få ske om straffminimum uppgår till fängelse sex månader eller mer.

Datainspektionen har anfört att den föreslagna lagen innehåller ändamålsenliga regleringar till skydd för den personliga integriteten och innebär en klar förbättring i jämförelse med dagens bestämmelser utan att effektiviteten i underrättelseverksamheten försämras.

Skälen för regeringens förslag

Underrättelseverksamhet

De brottsbekämpande myndigheternas underrättelseverksamhet är i huvudsak inriktad på att avslöja om en viss, inte närmare specificerad allvarlig brottslighet har ägt rum, pågår eller kan antas komma att begås. Arbetet består främst i att samla in, bearbeta och analysera information.

Inhämtning av underrättelseinformation sker på flera olika sätt. I stor utsträckning sker det genom öppna källor, men en inte obetydlig del av inhämtningen sker genom informatörer eller andra hemliga källor. En viktig del i underrättelsetjänsten utgörs av s.k. inre spaning, dvs. sökande efter information som redan finns tillgänglig inom respektive polismyndighet. I detta arbete ingår bl.a. sökning i register. Information inhämtas också genom samarbete med andra myndigheter och företag. Även internationellt samarbete spelar en stor roll. Det gäller såväl organiserat samarbete i multilaterala eller bilaterala former som mera informellt sådant samarbete.

Inom den öppna polisen bedrivs arbetet enligt polisens underrättelsemodell (PUM). Detta är en modell för ledning och styrning av planlagd operativ polisverksamhet där beslut om inriktning, prioritering och genomförande baseras på underrättelser och annan relevant kunskap. Enligt modellen ska underrättelseverksamhet bedrivas på lokal, regional och central nivå. Polisens underrättelsemodell kan beskrivas på följande sätt. Kriminalunderrättelsetjänsten samlar in

information, både på egen hand och genom att ta emot information som samlas in av andra enheter inom polisen. Informationen bearbetas och analyseras och leder fram till underrättelser. Underrättelserna delges den operativa ledningen som med underrättelserna som underlag fattar beslut om prioriteringar och adekvata brottsförebyggande aktiviteter. Kriminalunderrättelsetjänsten avgör vilken underrättelseinformation som ska delges den personal inom polisen som bedriver brottsbekämpande verksamhet.

Den aktuella modellen bygger således på ett flöde av information. Alla anställda inom polisen har ett ansvar för att inhämta information. Om en polisman gör iakttagelser som bedöms ha samband med misstänkt brottslig verksamhet ska informationen samlas in, dokumenteras och vidarebefordras till kriminalunderrättelsetjänsten. Informationsinhämtningen ska koncentreras till prioriterade områden. Kriminalunderrättelsetjänsten ansvarar för att annan personal inom polisen ständigt hålls informerad om inom vilka områden uppgifter främst efterfrågas, dvs. vilka de prioriterade underrättelsebehoven är. Polismän i yttre tjänst ska känna till vilka företeelser eller personer som det är särskilt viktigt att vara uppmärksam på. Den information som delges polismän i yttre tjänst kan vara av mer generellt slag eller avse vissa utpekade personer, t.ex. några som misstänks för delaktighet i viss brottslig verksamhet. Merparten av underrättelseinformationen stannar inom kriminalunderrättelsetjänsten. Det är i huvudsak slutsatserna av analys och bearbetning som förmedlas till andra delar av polisen.

Enligt 2 och 3 §§ förordningen (2002:1050) med instruktion för Säkerhetspolisen ska Säkerhetspolisen leda och bedriva polisverksamhet för att förebygga och avslöja brott mot rikets säkerhet, bekämpa terrorism samt fullgöra de uppgifter som Rikspolisstyrelsen har att utföra enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Med säkerhetsskydd avses enligt säkerhetsskyddslagen skydd mot bl.a. spioneri liksom mot terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott. Säkerhetspolisen har enligt förordningen också i uppdrag att leda och bedriva det bevaknings- och säkerhetsarbete som avser den centrala statsledningen eller som har samband med statsbesök och liknande händelser. Säkerhetspolisen tillämpar i princip samma modell som den övriga polisen för att styra underrättelsearbetet. Modellen innebär i korthet att ett väl definierat underrättelsebehov leder till en beställning av uppgifter. Beställningen resulterar i att olika inhämtningsåtgärder vidtas. De inhämtade uppgifterna bearbetas och analyseras varefter resultatet rapporteras till beställaren. Resultatet ligger sedan till grund för beslut om fortsatta åtgärder.

Även i Tullverket bedrivs underrättelseverksamhet genom insamling, inhämtning, bearbetning och analys av uppgifter. Syftet är att förhindra eller upptäcka brottslig verksamhet. Resultatet av underrättelseverksamhet, de slutsatser eller produkter som tas fram, delges beslutsfattare på olika nivåer och ingår som beslutsunderlag dels vid beslut om inriktning och prioriteringar av Tullverkets brottsbekämpande verksamhet (strategisk underrättelse), dels vid beslut om direkt operativa åtgärder (operativ underrättelse).

Som nämns i avsnitt 4.4 bedrivs underrättelseverksamhet även vid vissa andra myndigheter. Dessa myndigheter samlar också in, bearbetar och analyserar uppgifter inom ramen för sin underrättelseverksamhet.

Vilka uppgifter ska kunna hämtas in?

Det ovan beskrivna behovet av att i underrättelseverksamheten kunna hämta in information innefattar uppgifter om elektronisk kommunikation. I fråga om vilka uppgifter som ska kunna hämtas in anser regeringen, liksom utredningen, att samma bedömning bör göras som i fråga om inhämtning i en förundersökning innan det finns en skäligen misstänkt. Det innebär att historiska uppgifter om meddelanden får inhämtas. Dessutom får, i fråga om lokaliseringsuppgifter, uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller uppgifter om i vilket avgränsat geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits inhämtas (jfr. avsnitt 6.2.2 och 6.4). Regeringen anser till skillnad från utredningen att det inte finns behov av att i lagtext ange att det geografiska område som avses ska vara avgränsat eftersom det ändå följer av att inhämtningen ska avse ett visst geografiskt område.

När ska inhämtning få ske?

Att inhämtningen av uppgifter kan ske förhållandevis brett och förutsättningslöst är nödvändigt för att underrättelsearbetet ska kunna bedrivas effektivt. En alltför strikt reglering riskerar att hindra inhämtningen på ett icke önskvärt sätt. Samtidigt innebär en inhämtning av övervakningsuppgifter normalt sett ett visst intrång i den övervakades personliga integritet. Det måste därför finnas en klar reglering som är tillräckligt förutsebar och som möjliggör en effektiv fortlöpande tillsyn och granskning i efterhand.

Ett krav på att inhämtningen, i likhet med vad som gäller enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (1 §), ska kunna kopplas till *en viss person* skulle göra inhämtningen smalare och därmed kunna minska integritetsintrånget. Regeringen delar *Datainspektionens* uppfattning att en sådan begränsning ändå inte bör införas eftersom den avsevärt skulle minska möjligheterna att nå framgång i underrättelsearbetet. Den reglering som nu föreslås skiljer sig i väsentliga avseenden från lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Den senare lagen omfattar även det betydligt mer integritetskränkande tvångsmedlet hemlig avlyssning av elektronisk kommunikation och har kommit att tillämpas i sådana situationer där en förundersökning har varit mycket nära förestående. Lagen har dessutom kritiserats för att inte i tillräckligt hög grad uppfylla de brottsbekämpande myndigheternas behov (SOU 2009:70 s. 168 f.). Regeringen har nyligen beslutat att lagen ska ses över (dir. 2010:62).

Enligt utredningens förslag ska i ett beslut om inhämtning anges den teleadress eller det avgränsade geografiska område inhämtningen avser. Regeringen delar utredningens uppfattning att ett beslut om inhämtning ska ange vad beslutet avser. Beslutet ska därmed innehålla en upplysning

om vilken brottslig verksamhet som avses. Med den nya terminologi som föreslås i avsnitt 5 bör i beslutet dessutom anges det telefonnummer eller annan adress eller den elektroniska kommunikationsutrustning som inhämtningen avser.

Enligt utredningens förslag ska det finnas ett krav på att uppgifterna kan antas ha en påtaglig betydelse för den undersökning inom vars ramar inhämtningen ska ske. Utredningen föreslår att det ska uttryckas så att det ska finnas särskild anledning att anta att uppgifterna kan bidra till att förebygga, förhindra eller upptäcka viss brottslig verksamhet.

Att inhämtningen ska ske i en undersökning avses innefatta olika former av ”ärenden” i underrättelseverksamheten, t.ex. särskild undersökning i kriminalunderrättelseverksamheten, underrättelseprojekt, aktionsgrupp eller insats (SOU 2009:1 s. 126). Regeringen delar *JO:*s tveksamhet till att begreppet undersökning i förslaget i praktiken innebär någon precisering av inom vilken ram inhämtning får ske. Begreppet undersökning kan vidare leda tankarna till en förundersökning eller förutredning. Begreppet bör därför inte användas i den aktuella lagtexten. Den ram utifrån vilken inhämtningen får ske ska i stället framgå genom övriga rekvisit för inhämtningen och genom att beslutet ska preciseras på det sätt som framgår ovan. En annan sak är att beslutet om inhämtning naturligen bör läggas upp som ett särskilt inhämtningsärende vari skälen för beslutet framgår. Ärendet bör avslutas när inhämtningen har skett. Härigenom möjliggörs en effektivare löpande tillsyn över inhämtningen (se vidare avsnitt 6.3.2 och 8.2).

Som utredningen har föreslagit bör begreppen förebygga, förhindra eller upptäcka viss brottslig verksamhet i likhet med regleringen i 7 § lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och 2 kap. 5 § i den nya polisdatalagen (2010:361) användas för att avgränsa underrättelseverksamheten.

Att såsom i en förundersökning koppla ett beviskrav till ett specifikt brott är som utredningen har funnit inte lämpligt. I stället bör, på samma sätt som i den gällande polisdatalagen, den nya polisdatalagen och lagen om åtgärder för att förhindra vissa särskilt allvarliga brott, en koppling ske till viss *brottslig verksamhet*. Vilken brottslig verksamhet som bör omfattas utvecklas närmare nedan.

Regeringen delar utredningens uppfattning att det bör ställas krav på uppgifternas förväntade betydelse för det syfte i vilket de inhämtas. Enligt regeringens uppfattning är det dock inte tillräckligt att, som utredningen har föreslagit, uppgifterna ska förväntas *bidra till* att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som avses. En förutsättning för att inhämtning ska få ske bör i stället vara att det på goda grunder kan bedömas att åtgärden skulle ha stor betydelse för att uppnå det syfte i vilket åtgärden genomförs. För att en sådan bedömning ska kunna göras krävs rimligen att andra uppgifter, t.ex. källinformation, ger vid handen att viss brottslighet kan förebyggas, förhindras eller upptäckas genom åtgärden. I detta ligger också ett krav på uppgifternas förväntade betydelse för att uppnå det syfte i vilket de inhämtats. Regeringen föreslår att detta bör uttryckas så att uppgifter får inhämtas om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka den brottsliga verksamheten.

Brottens svårhetsgrad

Enligt nuvarande bestämmelse i lagen (2003:389) om elektronisk kommunikation (6 kap. 22 § första stycket 3) har de brottsbekämpande myndigheterna möjlighet att inhämta andra uppgifter än innehållsuppgifter om elektronisk kommunikation, om misstankarna rör brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Även om en sänkt tröskel naturligtvis som flera remissinstanser påpekat skulle ge de brottsbekämpande myndigheterna förbättrade förutsättningar i sin underrättelseverksamhet har det inte framkommit att behovet är så stort att det överväger de nackdelar en sådan utökad inhämtningsmöjlighet skulle innebära från integritetssynpunkt. I stället är det med hänsyn till den breda informations- och kunskapsinsamlingen och det framåtblickande perspektivet i underrättelseverksamheten, som Polismetodutredningen särskilt framhållit, av integritetsskäl lämpligt att som utgångspunkt behålla en lika hög tröskel som tidigare. Det förhållandet att uppgifter i underrättelseskedet om brottslig verksamhet innefattande vissa brott normalt sett har mindre konkretion än uppgifter om specifika brott i en förundersökning talar också för att möjligheten att inhämta uppgifter om elektronisk kommunikation i underrättelseskedet normalt bör vara mer begränsad jämfört med i en förundersökning. Med hänsyn härtill och till att lagen i många fall kommer att tillämpas innan det finns någon anknytning till ett specifikt brott eller en konstaterad brottsmisstanke anser regeringen, till skillnad från bl.a. *Åklagarmyndigheten*, att det inte är lämpligt att införa en straffvärdeventil. När det finns en misstanke om ett konkret brott kan inhämtning i stället komma att ske inom ramen för en förundersökning innan det finns en skäligen misstänkt person. För sådan inhämtning föreslås en straffvärdeventil. Eftersom det är fråga om underrättelseverksamhet finns det inte heller behov av att i detta sammanhang föra in osjälvständiga brottsformer (försöks-, förberedelse- och stämplingsbrott).

Med hänsyn till den valda begränsningen av för vilken brottslig verksamhet inhämtning ska vara möjlig, kommer regelverket att vara tillämpligt för polisen (både den öppna polisen och Säkerhetspolisen) och Tullverket. Detta bör uttryckligen anges i den föreslagna nya lagen.

Särskilt om vissa samhällsfarliga brott

Polismetodutredningen har föreslagit att det ska införas en möjlighet att inhämta uppgifter om elektronisk kommunikation i underrättelseskedet i fråga om vissa brott som trots att de inte har ett straffminimum som uppgår till två års fängelse får anses vara särskilt allvarliga för rikets säkerhet. 2008 års tvångsmedelslag innehåller en uppräkning av brott av detta slag. Lagen innehåller särskilda regler för tvångsmedelsanvändningen i fråga om utredning av dessa brott. Polismetodutredningen har föreslagit att inhämtning av övervakningsuppgifter i underrättelseverksamhet ska få ske avseende de brott som omfattas av den lagen.

Säkerhetsunderrättelseverksamheten vid Säkerhetspolisen skiljer sig från den övriga polisverksamheten bl.a. på så sätt att Säkerhetspolisens

uppdrag främst är inriktat på att förhindra brott och i mindre utsträckning på att utreda brott som redan har begåtts. För att kunna förhindra särskilt samhällsfarlig brottslighet har Säkerhetspolisen därför i vissa fall, som utredningen har konstaterat, ett särskilt behov av tillgång till övervakningsuppgifter i ett tidigt skede även då den brottsliga verksamheten inte innefattar brott med ett minimistraff om två års fängelse. Ingen remissinstans har invänt mot den bedömningen.

Frågan är då vid vilka brott en sådan inhämtning ska vara möjlig. Som framgår ovan har utredningen föreslagit att inhämtning ska kunna ske vid brottslig verksamhet som innefattar något av de brott som kan föranleda hemlig teleövervakning enligt 2008 års tvångsmedelslag. Även i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott finns en brottskatalog som upptar vissa brott vid vilka hemlig teleövervakning under särskilda förutsättningar är möjlig, trots att förutsättningarna för inhämtning enligt rättegångsbalken inte är uppfyllda. Vid en jämförelse mellan de båda lagarna kan det konstateras att det för vissa av de brott för vilka hemlig teleövervakning kan beslutas i en förundersökning enligt 2008 års lag inte finns någon motsvarande möjlighet i underrättelseskedet enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Detta gäller bl.a. olovlig kårverksamhet. Båda dessa lagar är som tidigare sagts tidsbegränsade till utgången av år 2012 och föremål för utvärdering (dir. 2010:62). Möjligheten att enligt den nu föreslagna lagen inhämta uppgifter i fråga om den aktuella brottsligheten bör mot den bakgrunden tills vidare begränsas till att avse de brott som omfattas av båda dessa lagar och ges samma giltighetstid som dem.

Sedan utredningen lämnat sitt betänkande har lagen om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet trätt i kraft. Grovt brott enligt 6 § den lagen omfattas numera av regleringen i såväl 2008 års tvångsmedelslag som lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Även det brottet bör enligt regeringen omfattas av den reglering som nu föreslås.

Frågan om Säkerhetspolisens fortsatta tillgång till övervakningsuppgifter för tiden efter utgången av år 2012 bör övervägas i det sammanhang som en framtida reglering av hemliga tvångsmedel för särskilt allvarlig eller samhällsfarlig brottslighet övervägs. Det kan också finnas ett behov av att tillåta hemlig övervakning av elektronisk kommunikation för dessa brott i en förundersökning innan det finns en skäligen misstänkt person även när straffvärdet inte uppgår till fängelse två år. Frågan om en sådan särreglering omfattas emellertid inte av utredningens förslag. Även den frågan bör ses över i nämnda sammanhang.

Proportionalitet

Som framgår av avsnitt 4.1 gäller proportionalitetsprincipen för samtliga tvångsmedel. Principen brukar i korthet beskrivas så att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden. Principen finns uttryckt i bl.a. 24 kap. 1 §, 25 kap. 1 §, 26 kap. 1 §, 27 kap. 1 § och 28 kap. 3 a §

rättegångsbalken samt i 3 § lagen om hemlig rumsavlyssning och 5 § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.

Regeringen föreslår att det uttryckligen anges i den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet anges att proportionalitetsprincipen ska tillämpas. Inhämtning ska få beslutas och genomföras endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

6.3.2 Vem ska fatta beslut?

Regeringens förslag: Beslut om inhämtning av övervakningsuppgifter om elektronisk kommunikation i underrättelseverksamhet fattas av en polismyndighet eller av Tullverket. Myndighetschefen får delegera rätten att fatta beslut till annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Ett beslut om inhämtning ska inte vara överklagbart. Säkerhets- och integritetsskyddsnämnden ska dock underrättas om varje beslut.

Polismetodutredningens förslag: Överensstämmer i huvudsak med regeringens förslag. Enligt utredningens bedömning ska delegation endast få ske till annan person på ledningsnivå. Utredningen har inte föreslagit någon skyldighet att underrätta Säkerhets- och integritetsskyddsnämnden om fattade beslut.

Remissinstanserna: *Ekobrottsmyndigheten, Åklagarmyndigheten* och *Säkerhetspolisen* har tillstyrkt att beslutanderätten ligger kvar på de brottsbekämpande myndigheterna. *Sveriges Advokatsamfund* har framfört att samfundet delar utredningens bedömning att det är svårförenligt med åklagares och domstolars roll att besluta om sådana åtgärder. *JO* har ansett att det bör övervägas att införa särskilda beslutsnämnder för beslut om tvångsmedel i underrättelseverksamhet. *Post- och Telestyrelsen* har framfört att domstol även i dessa fall bör besluta om inhämtningen eller att besluten ska kunna överklagas.

Rikspolisstyrelsen och Säkerhetspolisen har framhållit att möjligheterna till delegation är alltför begränsade.

Skälen för regeringens förslag: Enligt nuvarande bestämmelse i 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation, ska operatören vid misstanke om vissa brott på begäran av den brottsbekämpande myndigheten lämna ut uppgifter om elektronisk kommunikation. Beslut om inhämtning av uppgifter fattas enligt nuvarande ordning av polismyndighet respektive Tullverket. Det är inte närmare reglerat på vilken nivå inom myndigheten som besluten ska fattas.

Regeringen gör i avsnitt 6.2.3 bedömningen att rätten att inhämta uppgifter om elektronisk kommunikation *i förundersökningar* alltid ska prövas av domstol. Att allmän domstol fattar beslut om hemliga tvångsmedel under en förundersökning är lämpligt och väl förenligt med det tvåpartsförfarande och de möjligheter till rättslig prövning som gäller

där. Frågan blir då om allmän domstol, som *Post- och Telestyrelsen* har förordat, också bör fatta beslut om inhämtning i *underrättelseverksamhet*. Som redovisas i avsnitt 6.1 ovan gör sig andra intressen gällande i underrättelseverksamhet än under en förundersökning. Integritetsaspekten präglas i underrättelseskedet mer av ett medborgarperspektiv än av ett sådant tvåpartsförfarande som särskilt lämpar sig för rättslig prövning i allmän domstol. Det får också, såsom bl.a. *JO* och *Sveriges Advokatsamfund* har framfört, anses vara principiellt tveksamt att de allmänna domstolarna på förhand rättsligt prövar olika åtgärder som vidtas inom ramen för underrättelseverksamhet. Kännetecknande för den verksamheten är att den är operativ, kunskapssökande och undersökande men inte primärt inriktad mot någon viss inträffad gärning eller någon viss misstänkt person. För det fall allmän domstol generellt skulle rättsligt pröva olika åtgärder som vidtas i underrättelseverksamheten och därmed i många fall skulle ge tillstånd till olika operativa spaningsåtgärder, kan det finnas risk för att domstolens roll som oberoende prövningsinstans i brottsmålsförfarandet ifrågasätts, i varje fall när åtgärderna senare leder fram till förundersökning och åtal. En sådan roll skulle för domstolen också vara delvis främmande i det svenska rättssystemet. Enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott är det visserligen domstol som ger tillstånd till inhämtningen efter ansökan av åklagare (6 §). Det rör sig dock i det fallet om en tidsbegränsad lag som enligt uppgift har kommit att tillämpas när en förundersökning är förestående, dvs. i praktiken inom ramen för vad som brukar benämnas förutredning (SOU 2009:70 s. 172). Den nu föreslagna regleringen är avsedd att ha ett vidare tillämpningsområde. Det kan dessutom ifrågasättas om domstolarna skulle kunna tillgodose behovet av snabba beslut utanför kontorstid. Att införa en ordning med dygnetruntberedskap för de allmänna domstolarna för att pröva frågor om inhämtande av uppgifter i underrättelseverksamhet framstår inte som ändamålsenligt. Mot den angivna bakgrunden anser regeringen att allmänna domstolar inte bör ges beslutanderätten för inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Frågan uppkommer då om beslutanderätten bör läggas hos åklagare. Som Polismetodutredningen har anfört så deltar åklagarna som regel inte i polisens eller tullens underrättelseverksamhet (SOU 2009:1 s. 130). I stället sker åklagarinträde först i samband med att förundersökning rörande ett brott har inletts och någon är skäligen misstänkt för brottet. Som *Åklagarmyndigheten* har framhållit ska det krävas starka skäl för att åklagare ska tilldelas en roll i polisens allmänna underrättelsearbete. Beslutanderätten bör därför enligt regeringen inte heller läggas hos åklagare.

Är det då, vilket *JO* har ansett bör övervägas, lämpligt att inrätta särskilda beslutsnämnder för beslut om inhämtning av övervakningsuppgifter i underrättelseverksamhet? Frågan diskuterades i propositionen Åtgärder för att förhindra vissa särskilt allvarliga brott (prop. 2005/06:177 s. 64 f.). Regeringen bedömde i det sammanhanget att ett system med en särskild nämnd har nackdelar, bl.a. genom att det skulle kunna uppstå svårigheter att med kort varsel samla nämnden för

föredragning och beslut. Regeringen menade att övervägande skäl talade mot ett införande av en nämnd som fattar beslut i dessa frågor. Det finns inte skäl att nu göra en annan bedömning.

Som nämns tidigare fattas beslut om inhämtning av uppgifter enligt nuvarande ordning av polisen respektive tullen. Med de förtydliganden av förutsättningarna för inhämtning som har föreslagits i det föregående och förslaget i avsnitt 6.3.3 att det krävs ett beslut om hemlig övervakning av elektronisk kommunikation för att uppgifterna ska få användas i en förundersökning, delar regeringen utredningens uppfattning att de brottsbekämpande myndigheterna även fortsättningsvis ska få besluta om inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. Med hänsyn till de överväganden som bör göras innan ett beslut om inhämtning fattas, bör beslutanderätten dock inte tillkomma varje tjänsteman vid de aktuella myndigheterna. Tvärtom finns det skäl att precisera vem som får fatta besluten och tillskapa en ordning som innebär att beslutet om inhämtning fattas av någon som inte handlägger det aktuella ärendet i övrigt.

Polismetodutredningen har föreslagit att beslutanderätten ska tillkomma myndighetschefen och bedömt att denne ska ha möjlighet att delegera beslutanderätten till andra personer på ledningsnivå. Regeringen delar bedömningen att det bör vara myndighetschefen som ger tillstånd till inhämtningen. *Säkerhetspolisen* och *Rikspolisstyrelsen* har kritiserat begränsningen i delegationsmöjlighet. Regeringen delar uppfattningen att förslaget att delegation endast ska kunna ske till annan person på ledningsnivå inte är tillräckligt anpassad till framförallt polisens organisation. Delegation bör i stället kunna ske till annan tjänsteman vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Detta bör framgå av lagtexten.

Det är först vid inledandet av en förundersökning som ett partsintresse gör sig gällande med sådan styrka att det finns skäl att möjliggöra en rättslig prövning av beslut om inhämtande av uppgifter. De skäl som anförs ovan mot att domstol eller åklagare ges en roll i det allmänna underrättelsearbetet talar också mot att införa en generell möjlighet till överprövning. Regeringen delar utredningens bedömning att en sådan möjlighet inte bör införas.

Inhämtningen kommer att omfattas av Säkerhets- och integritetsskyddsnämndens tillsyn. Regeringen återkommer till denna fråga i avsnitt 8.2. För att möjliggöra att tillsynen blir så effektiv som möjligt föreslår regeringen att de brottsbekämpande myndigheterna fortlöpande ska underrätta Säkerhets- och integritetsskyddsnämnden om fattade beslut.

6.3.3 I vilken omfattning ska uppgifterna få användas?

Regeringens förslag: Om det vid de brottsbekämpande myndigheternas inhämtning av elektronisk kommunikation i underrättelseverksamhet har framkommit uppgifter av betydelse för utredningen av ett brott, ska uppgifterna få användas i en förundersökning endast efter tillstånd till hemlig övervakning av elektronisk kommunikation. Inhämtade uppgifter ska få användas för att förhindra även andra brott än de brott som omfattas av beslutet om inhämtning.

Polismetodutredningens förslag överensstämmer med regeringens förslag.

Remissinstanserna: Ingen remissinstans har motsatt sig förslaget.

Datainspektionen har tillstyrkt att uppgifter som har inhämtats i underrättelseverksamheten endast ska få användas för att utreda brott om dessa omfattas av ett beslut om hemlig teleövervakning. Även *Malmö tingsrätt* har ansett att en sådan ordning är motiverad av integritets- och rättssäkerhetsskäl. Tingsrätten har emellertid anfört att det framstår som oklart hur inhämtade uppgifter ska hanteras i praktiken och i vilket skede beslut om hemlig teleövervakning ska fattas samt att det bör övervägas att införa en bestämmelse avseende överskottsinformation. *Rikspolisstyrelsen* har invänt att förslaget innebär en alltför stor begränsning i fråga om för vilka brott informationen kan användas i en brottsutredning.

Säkerhetspolisen har tillstyrkt att det inte ska finnas några begränsningar för att använda inhämtad information för att förhindra brott.

Skälen för regeringens förslag

Gällande rätt

Vid användning av hemliga tvångsmedel kan det komma fram uppgifter som inte har något som helst samband med det brott som legat till grund för tvångsmedelsbeslutet. Uppgifterna kan i stället vara av betydelse för utredningen av ett annat begånget brott eller för att förhindra nya brott. De kan röra den person som förundersökningen gäller eller andra personer som är ovidkommande i det sammanhanget. Det kan också vara fråga om uppgifter som inte har samband med något brott men som är av betydelse i ett annat sammanhang, exempelvis för sociala myndigheter. All sådan information brukar benämnas överskottsinformation.

En första reglering av de brottsbekämpande myndigheternas användning av överskottsinformation infördes den 1 juli 2005. Regleringen omfattar användning av sådan information som framkommer vid användning av hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning för brottsutredande och brottsförebyggande ändamål. Regleringen innebär att

överskottsinformation om ett annat brott än det som ligger till grund för beslutet om det hemliga tvångsmedlet normalt får användas för att utreda det brottet. Beträffande överskottsinformation om mindre allvarliga brott gäller dock en viss begränsning. En förundersökning om ett sådant mindre allvarligt brott får inledas på grund av överskottsinformation endast om fängelse i ett år eller däröver är föreskrivet för brottet och det kan antas att brottet inte föranleder böter eller det finns särskilda skäl. Uppgifter om förestående brott får emellertid alltid användas för att förhindra brott (27 kap. 23 a § rättegångsbalken).

Även i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott regleras användandet av uppgifter om annan förestående brottslig verksamhet än den som omfattas av tillståndet till tvångsmedelsanvändningen. Sådana uppgifter får användas för att förhindra brott. Om det har kommit fram uppgifter om begångna brott, får uppgifterna användas för att utreda brottet endast om det är fråga om brott som hade kunnat föranleda tvångsmedelsanvändning enligt den lagen (12 §). Med att uppgifterna får användas för att utreda brott avses enligt den aktuella bestämmelsen både att de får ligga till grund för ett beslut att inleda en förundersökning och att de får användas i en redan pågående förundersökning (prop. 2005/06:177 s. 92).

Användning av uppgifter i brottsutredningssyfte

Polismetodutredningen har föreslagit en begränsning i möjligheterna för de brottsbekämpande myndigheterna att använda uppgifter om elektronisk kommunikation som har framkommit vid inhämtning i underrättelseskedet för att utreda brott. Uppgifterna ska enligt utredningens förslag endast få användas i en förundersökning om tillstånd ges till hemlig övervakning av elektronisk kommunikation.

Regeringen delar uppfattningen att rättssäkerhetsskäl talar för att införa en sådan begränsning, även om det som *Rikspolisstyrelsen* har invänt innebär en inte obetydlig begränsning i fråga om för vilka brott informationen kan användas i en brottsutredning. På det sättet säkerställs nämligen att samma prövning görs av om uppgifterna ska kunna ligga till grund för ett beslut om åtal oberoende av om de har inhämtats i underrättelseverksamhet eller i en förundersökning. Därigenom beaktas också skillnaden i integritetshänseende mellan underrättelseskedet och en brottsutredning (se närmare avsnitt 6.1).

Utredningen har inte närmare utvecklat i vilken utsträckning uppgifter som har inhämtats i underrättelseskedet enligt den nya lagen ska få ligga till grund för att *inleda* en förundersökning. Regeringen konstaterar i avsnitt 6.3.2 att starka skäl talar mot att ge domstolar en roll i underrättelseverksamheten utöver den begränsade roll de har enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det framstår därför inte som lämpligt att nu föreslå någon mer generell möjlighet till domstolsprövning innan en förundersökning har inletts.

En tänkbar ordning är att de aktuella uppgifterna aldrig skulle få ligga till grund för att inleda en förundersökning. Det kan dock förekomma att uppgifter av detta slag är av avgörande betydelse för att kunna inleda en förundersökning, dvs. att rekvisitet att det finns anledning att anta att ett

brott som hör under allmänt åtal har begåtts endast är uppfyllt om uppgifterna beaktas. Att en förundersökning i de fallen inte skulle få inledas ter sig betänkligt ur brottsutredningsperspektiv. Som framgår av det föregående ska de brottsbekämpande myndigheternas underrättelseverksamhet på olika sätt bistå myndigheternas brottsutredningsverksamhet. Resultaten från underrättelseverksamheten ska delges utredningsverksamheten när det finns operativa skäl till det. Det framstår enligt regeringen som en orimlig konsekvens att uppgifter som har inhämtats i syfte att upptäcka sådan allvarlig brottslig verksamhet som anges i lagen inte skulle kunna ligga till grund för ett beslut om att inleda en förundersökning om ett sådant brott. Vid inledandet av en förundersökning blir de rättssäkerhetsgarantier som framgår av 23 kap. rättegångsbalken direkt tillämpliga. Att en förundersökning *ska* inledas när det kan antas att ett brott har begåtts innebär att den som ska fatta beslutet om inledande av förundersökningen, om förutsättningarna är uppfyllda, inte kan avvakta med beslutet i avvaktan på ytterligare utredning (JO 1999/2000 s. 122). Något undantag från skyldigheten att inleda en förundersökning på grund av att uppgifterna har inhämtats i underrättelseverksamheten bör enligt regeringen således inte införas för dessa fall.

Det framstår i stället som mest lämpligt att tillåta att sådana uppgifter får ligga till grund för ett beslut om att inleda en förundersökning, men att uppgifterna inte fortsatt får användas i förundersökningen utan ett beslut om tillstånd till hemlig övervakning av elektronisk kommunikation. När en förundersökning har inletts förutsätter alltså en fortsatt användning av uppgifterna (t.ex. att de läggs till grund för ett beslut om användandet av andra tvångsmedel) ett tillstånd till hemlig övervakning av elektronisk kommunikation.

Användning av uppgifter för att förhindra brott

Intresset av att förhindra brott är mycket starkt. I nuvarande reglering om användning av överskottsinformation tillåts sådan användning utan inskränkningar. Även beträffande uppgifter som framkommer vid inhämtning av uppgifter om elektronisk kommunikation i underrättelseskedet saknas det enligt regeringen skäl att begränsa möjligheten att använda uppgifterna för att förhindra brott. Ingen remissinstans har invänt mot denna bedömning.

6.3.4 Bevarande och behandling av uppteckningar av uppgifter om elektronisk kommunikation

Regeringens förslag: Uppteckningar av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska granskas snarast möjligt. Uppteckningar ska, i de delar de är av betydelse för att förebygga, förhindra eller upptäcka brottslig verksamhet som omfattas av beslutet om inhämtning eller för att förhindra brott, bevaras så länge det behövs för det syftet. De ska därefter förstöras, om behandling inte får ske i enlighet med vad som är särskilt föreskrivet i lag.

Polismetodutredningens förslag: Överensstämmer i huvudsak med regeringens förslag.

Remissinstanserna: Ingen remissinstans har motsatt sig förslaget. *Datainspektionen* har uttalat att förslaget innebär ett fullgott integritetsskydd.

Skälen för regeringens förslag: En upptagning eller uppteckning som görs vid hemlig teleavlyssning, hemlig teleövervakning (hemlig avlyssning respektive övervakning av elektronisk kommunikation enligt den terminologi som regeringen har föreslagit i avsnitt 5) eller hemlig rumsavlyssning eller en upptagning som görs vid hemlig kameraövervakning ska granskas så snart det är möjligt (27 kap. 12 och 24 §§ rättegångsbalken samt 13 § lagen (2007:978) om hemlig rumsavlyssning). Granskningen får utföras endast av rätten, förundersökningsledaren, åklagaren eller en sakkunnig. I de delar upptagningen eller uppteckningen är av betydelse från brottsutredningssynpunkt ska de bevaras till dess förundersökningen lagts ned eller avslutats eller målet har avgjorts slutligt. Har upptagningen eller uppteckningen betydelse för att förhindra brott, ska den bevaras så länge det behövs för det syftet för att därefter förstöras. Liknande bestämmelser finns i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (13 §).

Det bör även i den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet finnas bestämmelser om behandling av uppteckningar av uppgifter. Regeringen delar utredningens uppfattning att det är lämpligt att utforma regleringen med de bestämmelser som gäller vid hemlig övervakning av elektronisk kommunikation som förebild. Granskning av uppteckningar bör följaktligen ske snarast möjligt. Däremot saknas det anledning att för underrättelseverksamheten föreskriva vem som får genomföra granskningen. På motsvarande sätt som enligt regleringen i rättegångsbalken bör uppteckningarna i de delar de är av betydelse för att förhindra brott, få bevaras så länge de behövs för det syftet. Eftersom en användning av uppteckningarna i en förundersökning kommer att förutsätta ett tillstånd till hemlig övervakning av elektronisk kommunikation kommer de att omfattas av rättegångsbalkens reglering (27 kap. 24 § andra stycket). Det innebär att

de ska bevaras till förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. När uppgifterna inte längre behövs ska de förstöras.

Av 27 kap. 24 § fjärde stycket rättegångsbalken framgår att bestämmelserna om bevarande respektive förstörande av upptagningar och uppteckningar från hemlig avlyssning eller övervakning av elektronisk kommunikation inte hindrar att de brottsutredande myndigheterna behandlar uppgifter från upptagningarna eller uppteckningarna i enlighet med vad som är särskilt föreskrivet i lag. Om det har kommit fram uppgifter som får behandlas i register eller på annat sätt enligt de förutsättningar som ställs upp i exempelvis polisdatalagen eller lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet, utgör alltså regleringen inte hinder för att nämnda uppgifter behandlas enligt dessa lagar (prop. 2004/05:143 s. 53). I fråga om gallring m.m. av uppgifterna gäller då vad som föreskrivs i de särskilda lagarna. Utredningen har föreslagit att en motsvarande ordning bör gälla även för myndigheternas underrättelseverksamhet. Regeringen ansluter sig till utredningens förslag. Det innebär att uppgifter som t.ex. är av betydelse för att förhindra sådan brottslig verksamhet som avses i lagen får bevaras så länge det behövs för det syftet men att uppgifterna sedan som huvudregel ska förstöras. Om den brottsliga verksamhet som skulle förhindras trots allt genomförs behöver uppgifterna dock inte förstöras om behandling t.ex. i syfte att utreda brott är tillåten enligt annan lag.

Regeringen delar *Datainspektionens* bedömning att Polismetodutredningens förslag i denna del, även med beaktande av den försiktighet som bör iakttas i fråga om att behandla uppgifter som har inhämtats i underrättelsesyfte i de brottsutredande myndigheternas system och register, innebär ett fullgott integritetsskydd.

6.4 Tillgång till lokaliseringsuppgifter

Regeringens förslag: Ett beslut om hemlig övervakning av elektronisk kommunikation ska även kunna avse inhämtning av

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

Sådana uppgifter ska också få inhämtas enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Polismetodutredningens förslag: Överensstämmer delvis med regeringens förslag. Enligt utredningen ska inhämtning av lokaliseringsuppgifter kunna ske under samma förutsättningar som gäller för hemlig teleövervakning men inte utgöra en del av det tvångsmedlet.

Remissinstanserna: *Åklagarmyndigheten, Säkerhetspolisen, Tullverket* och *Justitiekanslern* har tillstyrkt förslaget. *Post- och Telestyrelsen* och *Svenska Journalistförbundet* har invänt att förslaget

innebär ytterligare integritetsintrång som inte tillräckligt motiverats av utredningen.

Skälen för regeringens förslag

Gällande rätt

Genom hemlig teleövervakning har de brottsbekämpande myndigheterna möjlighet att få tillgång till vissa lokaliseringsuppgifter avseende bl.a. mobiltelefoner. Det kan gälla uppgifter om vilken basstation en telefon eller annan elektronisk kommunikationsutrustning varit uppkopplad mot i samband med kommunikation. Sådana historiska uppgifter har myndigheterna möjlighet att få ut även enligt 6 kap. 22 § första stycket 3 lagen (2003:389) om elektronisk kommunikation eftersom det är fråga om uppgifter som angår särskilda elektroniska meddelanden.

En basstationstömning innebär att de brottsbekämpande myndigheterna får uppgift om samtliga de mobiltelefoner som vid en viss tidpunkt har varit uppkopplade för kommunikation (t.ex. för samtal eller SMS-meddelande) mot en viss basstation, dvs. information om vilka mobiltelefoner som har använts inom det avgränsade geografiska område som är aktuellt. Sådana uppgifter anses vara uppgifter som angår särskilda elektroniska meddelanden och kan därför lämnas ut till myndigheterna om förutsättningarna i 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation är uppfyllda. Däremot kan en basstationstömning inte ske enligt de nuvarande bestämmelserna om hemlig teleövervakning eftersom övervakningen enbart får avse uppgifter om meddelanden till eller från vissa adresser med viss koppling till en skäligen misstänkt person.

Både regleringen i 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation och bestämmelsen om hemlig teleövervakning förutsätter att lokaliseringsuppgifter, för att kunna lämnas ut, har genererats i samband med att mobiltelefonen har varit uppkopplad för kommunikation. Lokaliseringsuppgifter som finns hos operatören och som genereras av utrustningens kontakt med en basstation utan att det varit fråga om kommunikation omfattas alltså inte av de aktuella bestämmelserna. Sådana uppgifter omfattas inte heller av operatörernas tystnadsplikt enligt lagen om elektronisk kommunikation, eftersom det inte är fråga om uppgifter som angår något särskilt elektroniskt meddelande. Justitiekanslern har i ett beslut konstaterat att de möjligheter de brottsbekämpande myndigheterna har enligt andra regler (rättegångsbalkens bestämmelser om husrannsakan och beslag) inte torde vara tillräckliga för att tillgodose det legitima behov som ofta finns att komma över dessa uppgifter. Det framstår enligt Justitiekanslern som givet, trots integritetsriskerna, att polis och åklagare bör ges en sådan möjlighet (Justitiekanslerns beslut den 15 augusti 2008, dnr 6545-0621).

Inhämtning av lokaliseringsuppgifter som inte har samband med kommunikation omfattas inte av skyddet mot hemlig upptagning av telefonsamtal eller annan förtroligt meddelande i regeringsformen. Som framgår av avsnitt 4.3 anges fr.o.m. den 1 januari 2011 i regeringsformen att var och en gentemot det allmänna ska vara skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och

innebär övervakning eller kartläggning av den enskildes personliga förhållanden. En inhämtning av nu aktuellt slag sker utan samtycke och innebär övervakning av den enskildes personliga förhållanden. Vid en bedömning av vilka sådana åtgärder som kan anses utgöra ett betydande intrång ska både åtgärdens omfattning och arten av intrånget beaktas. Även åtgärdens ändamål och andra omständigheter kan ha betydelse vid bedömningen (prop. 2009/10:80 s. 250). Artikel 8 i Europakonventionen, som gäller som svensk lag, ger också ett skydd i nu aktuellt hänseende.

En möjlighet att inhämta lokaliseringsuppgifter med koppling till elektronisk kommunikationsutrustning

Såväl Buggningsutredningen (SOU 1998:46 s. 365 f. och 477 f.) som BRU har tidigare föreslagit att hemlig övervakning av elektronisk kommunikation uttryckligen ska få användas för att inhämta uppgifter om lokalisering, oavsett om kommunikationsutrustningen har använts för kommunikation eller inte. BRU konstaterade att uppgifterna många gånger är värdefulla i brottsbekämpningen, att uppgifterna kan ha mycket stor betydelse i effektivitetshänseende, att det tveklöst finns ett mycket stort behov av att få tillgång till sådana uppgifter och att det inte möter några avgörande hinder från integritetssynpunkt med en ordning där sådana uppgifter lämnas ut vid hemlig teleövervakning (SOU 2005:38 s. 202 f.). Majoriteten av de remissinstanser som uttalade sig särskilt om BRU:s förslag om de brottsbekämpande myndigheternas tillgång till lokaliseringsuppgifter tillstyrkte eller hade inte någon invändning mot förslaget. Nu har även Polismetodutredningen föreslagit att en sådan möjlighet införs.

En eller flera basstationstömningar sker ofta med avseende på platsen för ett grovt brott. För de brottsbekämpande myndigheterna är möjligheten till en sådan inledande åtgärd ofta central för att så snabbt som möjligt kunna identifiera misstänkta personer i utredningen. Regeringen delar utredningens bedömning att det är nödvändigt för effektiviteten i den brottsbekämpande verksamheten att möjligheten att genomföra basstationstömning finns kvar när bestämmelsen i 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation, enligt vad som föreslagits i avsnitt 6.1, upphävs. Det är av samma skäl viktigt att det i brottsbekämpningen ges tillgång till uppgifter avseende t.ex. mobiltelefoner som är påslagna men som inte vid det aktuella tillfället har använts för kommunikation. Regeringen bedömer liksom *Datainspektionen* att det saknar betydelse från integritetssynpunkt om en mobil kommunikationsutrustning används för kommunikation eller inte. Införandet av en möjlighet att inhämta lokaliseringsuppgifter som inte har samband med en kommunikation kan inte anses medföra någon nämnvärd ökning av integritetsintrånget för den enskilde.

Post- och Telestyrelsen och *Svenska Journalistförbundet* har anmärkt att förslagets integritetspåverkan inte har analyserats tillräckligt. En basstationstömning kan beröra ett stort antal personer. Integritetsintrånget för varje enskild individ är emellertid mycket begränsat, eftersom det normalt endast är fråga om en positionsbestämning vid ett specifikt tillfälle. En sådan inhämtning kan

enligt regeringens bedömning varken av hänsyn till uppgifternas integritetskänsliga natur eller andra omständigheter sägas innebära ett betydande ingrepp i den enskildes privata sfär och omfattas därför inte av regeringsformens skydd i dess föreslagna nya lydelse. En inhämtning som innebär att de brottsbekämpande myndigheterna får möjlighet att följa hur en mobiltelefon förflyttas kommer att beröra betydligt färre personer men innebär samtidigt ett större integritetsintrång för den person som övervakningen avser. Möjligheten att kartlägga den enskilde och hans eller hennes förhållanden ökar. Denna form av kartläggning får enligt regeringens bedömning anses omfattas av tillämpningsområdet för den nya grundlagsbestämmelsen om stärkt skydd för den personliga integriteten (se närmare ovan). Mot bakgrund av de tydliga avgränsningar som regeringen föreslår för den nya regleringen om inhämtning bl.a. i fråga om syftet med inhämtningen och betydelsen av uppgifterna, blir dock tillämpningsområdet så snävt att nyttan av att införa en sådan möjlighet för de brottsbekämpande myndigheterna måste anses överväga det ökade integritetsintrång utvidgningen medför. Inhämtningsmöjligheten medför inte heller ett hot mot den fria åsiktsbildningen.

Vilka uppgifter ska få hämtas in?

Utredningen har föreslagit att det ska vara möjligt att inhämta uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits i ett avgränsat geografiskt område (historiska uppgifter) och uppgifter om i vilket visst avgränsat geografiskt område en sådan utrustning finns eller har funnits (realtidsuppgifter och historiska uppgifter). Det finns emellertid enligt regeringens uppfattning inte behov av att i lagtext ange att inhämtningen ska avse ett *avgränsat* område eftersom den omständigheten att inhämtningen ska avse ett visst geografiskt område redan får anses innefatta ett sådant krav.

Ingen remissinstans har invänt mot den föreslagna tidsmässiga avgränsningen av möjligheten till inhämtning. Den inhämtning som kan ske enligt lagen om elektronisk kommunikation i fråga om ett särskilt elektroniskt meddelande är begränsad till historiska uppgifter. Regeringen har i det föregående föreslagit att inhämtning som har samband med en elektronisk kommunikation även fortsättningsvis ska vara möjlig enbart för historiska uppgifter såväl i underrättelseverksamheten som i en förundersökning innan det finns en skäligen misstänkt person. När det gäller inhämtning som avser var en viss elektronisk kommunikationsutrustning befinner sig delar dock regeringen utredningens bedömning att det är angeläget att inhämtningen kan ske även i realtid. På det sättet kan myndigheterna t.ex. följa en viss mobiltelefon längs en flyktväg eller lokalisera ett gömställe eller den plats där en eventuell gärningsman kan befinna sig. Tillgången till sådana historiska uppgifter kommer sannolikt också, som flera remissinstanser har påpekat, att vara begränsad.

Regeringen delar mot den angivna bakgrunden utredningens uppfattning att inhämtningsmöjligheten också innan det finns en skäligen misstänkt bör omfatta såväl historiska uppgifter som uppgifter i realtid

när det gäller lokaliseringen av viss elektronisk kommunikationsutrustning. Inhämtningen av uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits i ett visst geografiskt område bör dock endast avse historiska uppgifter.

Förutsättningar för inhämtning

Polismetodutredningen har i fråga om inhämtning i en förundersökning gjort bedömningen att uppgifterna ska benämnas lokaliseringsuppgifter och att inhämtningen av sådana uppgifter inte ska regleras som en del av tvångsmedlet hemlig övervakning av elektronisk kommunikation. Enligt förslaget ska vad som sägs om hemlig teleövervakning även gälla inhämtning i hemlighet av lokaliseringsuppgifter. Som *JO* har påpekat är den föreslagna definitionen av lokaliseringsuppgifter dock problematisk eftersom den inte är likalydande med den definition av begreppet som finns i lagen om elektronisk kommunikation. Till exempel omfattas endast historiska uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område av den föreslagna definitionen. Lämpligheten av att avgränsa definitionen på ett sådant sätt kan ifrågasättas. Det kan också riktas invändningar mot förslaget i systematiskt hänseende eftersom begreppet inte används i den föreslagna nya lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, trots att det är fråga om inhämtning av samma uppgifter.

Med hänsyn till att uppgifterna har ett sådant nära samband med andra uppgifter som kan inhämtas inom ramen för ett tillstånd till hemlig övervakning av elektronisk kommunikation delar regeringen utredningens uppfattning att samma förutsättningar bör gälla för inhämtningen. Regeringen delar också utredningens bedömning att de aktuella uppgifterna ska få inhämtas även i enlighet med de andra lagar som reglerar hemlig övervakning av elektronisk kommunikation. Regeringen anser däremot att den mest lämpliga ordningen är att inhämtningen sker inom ramen för ett tillstånd till hemlig övervakning av elektronisk kommunikation. Med den lösningen finns det inte behov av att använda begreppet lokaliseringsuppgifter i rättegångsbalken. Härigenom tydliggörs också att ändringen, vilket också har varit utredningens avsikt, får effekt för de andra lagar som reglerar hemlig övervakning av elektronisk kommunikation, t.ex. 2008 års tvångsmedelslag och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (se avsnitt 5.5 för en fullständig uppräkning av de lagar som reglerar hemlig övervakning av elektronisk kommunikation). Att hemlig övervakning av elektronisk kommunikation får ett delvis nytt innehåll får också konsekvenser för lagen (2000:562) om internationellt rättslig hjälp i brottmål genom att reglerna knyter an till vad som gäller för att motsvarande åtgärder ska få vidtas i en svensk förundersökning eller rättegång (jfr avsnitt 6.2.3).

Även i underrättelseverksamhet bör, som utredningen har föreslagit, samma förutsättningar gälla för inhämtning av lokaliseringsuppgifter

med koppling till elektronisk kommunikationsutrustning som för uppgifter om elektronisk kommunikation.

7 Inhämtning av uppgifter om abonnemang m.m.

7.1 Bakgrund

En operatör som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har tystnadsplikt för bl.a. uppgifter om abonnemang och för andra uppgifter som angår särskilda elektroniska meddelanden som operatören har fått del av eller har tillgång till (6 kap. 20 § första stycket 1 och 3 lagen (2003:389) om elektronisk kommunikation, se närmare avsnitt 4.2). Med uppgifter om abonnemang avses främst uppgifter om namn, titel, adress och abonnentnummer (prop. 1992/93:200 s. 310). Sådana uppgifter kallas ibland kataloguppgifter. Uppgifter som angår särskilda elektroniska meddelanden anses i praxis vara uppgifter 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 brukar hänföras till den sistnämnda kategorin.

Lagen om elektronisk kommunikation innehåller regler om när operatörerna trots sin tystnadsplikt är skyldiga att på begäran lämna ut uppgifter om abonnemang till polisen eller annan myndighet. Reglerna får i första hand betydelse för hemliga abonnemangsuppgifter. Beträffande öppna abonnemangsuppgifter har abonnenten redan samtyckt till att uppgifterna kan lämnas ut och myndigheterna kan söka efter uppgifterna i sedvanliga register (jfr 6 kap. 16 §). Bestämmelserna som anger när en operatör är skyldig att lämna ut uppgifter finns i 6 kap. 22 § första stycket. En skyldighet att lämna ut uppgifter om abonnemang föreligger bl.a. beträffande misstanke om brott för vilket fängelse är föreskrivet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter (punkten 2) och när en myndighet finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387), dvs. överlämnande till föräldrar eller annan vårdnadshavare av en ung person som har omhändertagits (punkten 6). Operatörerna är dessutom skyldiga att, utan att något särskilt ändamål anges, lämna ut abonnemangsuppgifter och uppgifter som angår ett särskilt elektroniskt meddelande till en regional alarmeringscentral, t.ex. SOS Alarm AB (punkten 8).

7.2 En effektiv tillgång till uppgifter om abonnemang

Regeringens förslag: Skyldigheten för operatörerna att lämna ut uppgifter om abonnemang till de brottsbekämpande myndigheterna i samband med misstanke om brott ska inte vara begränsad till brott av viss svårhet.

Polismetodutredningens förslag: Överensstämmer med regeringens förslag.

Remissinstanserna: *Göta hovrätt, Juridiska fakultetsnämnden vid Stockholms universitet, Rikspolisstyrelsen, Säkerhetspolisen* och *Justitiekanslern* har tillstyrkt förslaget. *Swedish Network Users' Society* och *Svenska Stadsnätsföreningen* har angett att de ställer sig tveksamma till att de brottsbekämpande myndigheterna ges möjlighet att inhämta uppgifter om abonnemang för bötesbrott. *Datainspektionen* har framfört att myndigheten delar utredningens bedömning att skyldigheten att lämna ut abonnemangsuppgifter även fortsättningsvis bör regleras i lagen om elektronisk kommunikation men ansett att abonnemangsuppgifter endast ska få inhämtas för brott som har fängelse i straffskalan och för vissa brott som omfattas av 5 kap. brottsbalken (ärekränkningsbrotten).

Säkerhetspolisen och *Post- och Telestyrelsen* har anmärkt att det kan uppstå osäkerhet om en uppgift är en uppgift om abonnemang eller annan särskild uppgift om ett elektronisk meddelande. Säkerhetspolisen har anfört att s.k. IMEI-uppgifter (hårdvaruidentitet för mobila telefoner) bör betraktas som abonnemangsuppgifter.

Skälen för regeringens förslag

Regleringen bör finnas kvar i lagen om elektronisk kommunikation

Som framgår av föregående avsnitt är operatörerna enligt lagen om elektronisk kommunikation skyldiga att under vissa förutsättningar lämna ut uppgifter om abonnemang till polis- och åklagarmyndighet vid misstanke om brott som bedöms föranleda annan påföljd än böter. I likhet med *Datainspektionen* delar regeringen utredningens bedömning att skyldigheten att lämna ut abonnemangsuppgifter även i fortsättningen bör regleras i lagen om elektronisk kommunikation

En uppgift om abonnemang kan avse namn, adress eller abonnentnummer (kataloguppgifter). *Säkerhetspolisen* och *Post- och Telestyrelsen* har framfört att det kan råda osäkerhet om en viss uppgift ska anses vara en uppgift om abonnemang eller inte. Post- och Telestyrelsen har anfört att det därför vore lämpligt med en annan uppdelning än den i abonnemangsuppgifter och uppgifter om särskilda elektroniska meddelanden. Uppdelningen skulle enligt Post- och Telestyrelsen lämpligen vara mer inriktad på syftet med användningen av uppgifterna. Regeringen konstaterar att det inte inom ramen för detta lagstiftningsärende är möjligt att föreslå någon ny uppdelning och att de ändringar som nu föreslås inte innebär någon ändring i fråga om vilka

uppgifter som ska anses höra till vilken kategori. Det har tidigare ifrågasatts om s.k. dynamiska IP-nummer är att anse som abonnemangsuppgifter. Ett IP-nummer är ett unikt nummer som kan användas för att identifiera en abonnent som är uppkopplad mot Internet. IP-adressen hänför sig till Internetuppkopplingen som sådan och inte till något särskilt meddelande. Numera får det anses stå klart att IP-nummer är att betrakta som en uppgift om abonnemang.

När bör utlämnande kunna ske?

Kravet på att det för utlämnande av abonnemangsuppgifter i samband med misstanke om brott ska vara fråga om ett brott som kan föranleda annan påföljd än böter har överförts från den upphävda telelagen (1993:597). Det har sedan dess skett en betydande teknisk utveckling och förändring av i vilken omfattning enskilda använder bl.a. datorer och mobiltelefoner. Under de senaste åren har exempelvis s.k. nätmobbning och andra trakasserier via Internet blivit ett allt större problem. När dessa gärningar misstänks utgöra brott har ofta de brottsutredande myndigheterna begränsade möjligheter att ingripa. Samma sak gäller vuxnas kontakter med barn i sexuella syften, grooming. Det hänger bl.a. samman med att polisen inte kan få tillgång till abonnemangsuppgifter, t.ex. uppgifter om en viss IP-adress, vid misstanke om brott som i det konkreta fallet bedöms föranleda böter. Flera remissinstanser har också betonat att det är angeläget att de brottsutredande myndigheterna kan få tillgång till abonnemangsuppgifter även vid denna typ av brott, inte minst eftersom de ofta innebär en betydande kränkning av brottsoffrens integritet. När det gäller immaterialrättsliga brott har sedan den 1 april 2009 rättighetshavare en civilrättslig möjlighet att efter domstolsprövning få ut information från en Internetoperatör om vem som har ett abonnemang (en IP-adress) (prop. 2008/09:67, bet. 2008/09:NU 11, rskr. 2008/09:176). Regleringen kan tillämpas oavsett om intrånget är på bötesnivå eller fängelsenivå. Som *Göta hovrätt* har framfört bör de brottsbekämpande myndigheterna ha minst lika stora befogenheter som privata rättighetsinnehavare att säkra tillgång till uppgifter som kan användas i brottsbekämpande syften. Detta var också något som förutsattes vid införandet av den civilrättsliga regleringen (prop. 2008/09:67 s. 140).

Det finns alltså ett starkt intresse av att införa en möjlighet för de brottsbekämpande myndigheterna att få tillgång till abonnemangsuppgifter. Samtidigt innebär utlämnandet ett visst integritetsintrång, eftersom abonnentens identitet röjs. Vid denna intresseavvägning bör beaktas att privatpersoner oftast använder s.k. dynamiska IP-adresser, dvs. adresser som byts slumpvis och oregelbundet. En uppgift om att en viss person hade en viss IP-adress vid ett visst tillfälle säger alltså i regel ingenting om vem som hade den adressen vid ett annat tillfälle (prop. 2008/09:67 s. 141). Det förtjänar också att påpekas att uppgifter som går utöver vad som kan anses som identitetsuppgifter, t.ex. vilka andra IP-nummer som innehavaren har kommunicerat med, vilka hemsidor som ett visst IP-nummer har besökt och liknande uppgifter inte omfattas av den aktuella bestämmelsen. Med

hänsyn till den tekniska utvecklingen och det sätt på vilket brottsligheten på t.ex. Internet har utvecklats på senare tid anser regeringen att de brottsbekämpande myndigheternas behov av tillgång till abonnemangsuppgifter har förändrats påtagligt. Det finns ett stort behov av sådana uppgifter både i fråga om brott som har fängelse i straffskalan men som vanligen föranleder en bötespåföljd och i fråga om sådana brott som bara har böter i straffskalan, t.ex. ärekränkningsbrotten. *Datainspektionen* har framfört att inhämtning inte ska vara tillåten för alla bötesbrott. Vid en avvägning mellan det integritetsintrång ett utlämnande av abonnemangsuppgifter innefattar å ena sidan och den stora betydelse uppgifterna ofta kan ha för polisens möjlighet att över huvud taget kunna utreda brott som begås på Internet å andra sidan, anser regeringen att skälen för att låta polisen i framtiden få en mer omfattande tillgång till abonnemangsuppgifter väger klart tyngre än enskildas motsvarande intresse av integritetsskydd.

7.3 Utlämnande av vissa uppgifter från operatörer när personer har försvunnit

Regeringens förslag: Det ska införas en skyldighet för operatörer att till polismyndighet lämna ut abonnemangsuppgifter, uppgifter som angår särskilda elektroniska meddelanden och uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits, om 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.

BRU:s förslag: Överensstämmer med regeringens förslag.

Remissinstanserna: Remissinstanserna har tillstyrkt eller inte haft något att invända mot förslaget.

Skälen för regeringens förslag: När polisen kan konstatera att en person är försvunnen är orsaken i de flesta fall inte att ett brott har begåtts eller att en olycka har inträffat. Efterforskning av försvunna personer förekommer i en mängd olika situationer och vid ett stort antal tillfällen varje år. I vissa fall fordras endast någon enkel åtgärd för att omständigheterna kring försvinnandet ska kunna klarläggas medan det i andra fall kan bli nödvändigt med omfattande insatser från myndigheter och enskilda. I många fall, särskilt när barn, äldre och personer med nedsatt mental förmåga har försvunnit, är det också nödvändigt att insatsen sker snabbt för att hindra att personerna skadas.

Det ingår i polisens uppgifter att efterforska försvunna personer. Lagen (2003:778) om skydd mot olyckor innehåller bestämmelser om bl.a. de åtgärder som stat och kommun ska vidta till skydd mot olyckor, om tjänsteplikt och om ingrepp i annans rätt. Enligt lagen avses med räddningstjänst de räddningsinsatser som staten eller kommunerna ska ansvara för vid olyckor och överhängande fara för olyckor för att förhindra och begränsa skador på människor, egendom eller miljön. Lagen gäller också vid efterforskning av försvunna 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 förordningen (2003:789) om skydd mot olyckor anges att polismyndigheterna ska svara för efterforskningen av försvunna personer i sådana fall.

Om polisen får tillgång till lokaliseringsuppgifter avseende mobiltelefoner i samband med efterforskning av försvunna personer, skulle många gånger den försvunne kunna påträffas snabbare. Dessutom skulle stora resurser kunna sparas vid polisarbetet. BRU har mot denna bakgrund föreslagit att operatörernas uppgiftsskyldighet i dessa fall ska omfatta abonnemangsuppgifter och andra uppgifter som angår särskilda elektroniska meddelanden samt lokaliseringsuppgifter avseende elektronisk kommunikationsutrustning. Ingen remissinstans har invänt mot förslaget. Regeringen delar BRU:s uppfattning av det är ändamålsenligt att polisen vid efterforskning av försvunna personer ska kunna få tillgång till abonnemangsuppgifter och uppgifter som angår ett elektroniskt meddelande, t.ex. om samtal pågår från en viss mobiltelefon, med vilket nummer samtalet utväxlas, tiden för samtalet etc., samt till uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Tillgången till lokaliseringsuppgifter avseende den försvunna personens mobiltelefon kan ibland vara helt avgörande för att hitta personen om denne inte själv kan berätta var han eller hon befinner sig. Denna möjlighet bör dock, som BRU föreslagit, endast vara tillgänglig om det kan befaras att det föreligger fara för personens liv eller allvarlig risk för dennes hälsa. Det ska således inte vara möjligt att få tillgång till de aktuella uppgifterna såvitt avser personer som frivilligt håller sig borta. När den försvunne är underårig eller en person med nedsatt mental hälsa kan man dock enligt regeringens uppfattning alltid utgå från att sådan fara eller risk föreligger.

7.4 Skyldighet att registrera abonnemangsuppgifter för kontantkort

Regeringens bedömning: Någon särskild skyldighet för operatörer att registrera uppgifter om abonnemang för kontantkort bör inte införas.

BRU:s bedömning: Överensstämmer med regeringens bedömning.

Remissinstanserna: De flesta remissinstanserna har instämt i BRU:s bedömning eller inte haft något att invända mot den. *Säkerhetspolisen* har dock ansett att en skyldighet att registrera kontantkort bör införas.

Skälen för regeringens bedömning: Det är mycket vanligt att mobiltelefoner med anonyma kontantkort förekommer vid brottslig verksamhet (jfr avsnitt 5.4). Enligt nuvarande regler kan teleadresser som avser mobiltelefoner omfattas av beslut om hemlig teleavlyssning och hemlig teleövervakning. Det förutsätter dock i det enskilda fallet att såväl teleadressen som en skäligen misstänkt person är identifierad. De brottsutredande myndigheterna har ofta problem med att identifiera själva teleadressen och knyta den, när den härrör från ett anonymt kontantkort, till en viss person.

Som BRU har anfört är det givet att de brottsutredande myndigheterna har ett påtagligt behov av att i olika sammanhang få tillgång till uppgifter om abonnemang avseende kontantkort.

Till en viss del är detta redan möjligt genom att kunden frivilligt har valt att lämna dessa uppgifter till operatören. Enligt BRU behandlar vissa operatörer uppgifterna som öppna abonnemangsuppgifter medan andra betraktar dem som hemliga. I de fall kunden har 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 (se närmare avsnitt 7.2).

För att undvika att operatörerna saknar uppgifter om innehavarna skulle en registreringsskyldighet kunna införas. De brottsutredande myndigheternas behov av att få tillgång till uppgifterna måste dock, som BRU har anfört, vägas mot andra intressen. En skyldighet att registrera den abonnent som använder ett visst kontantkort skulle innebära ett åliggande för operatörerna med kostnader som följd. En sådan skyldighet skulle också innebära en skyldighet för de personer som köper kontantkort att ge upp den anonymitet som hittills har funnits. Som BRU har påpekat är det dessutom tveksamt hur effektiv en registreringsskyldighet avseende abonnemangsuppgifter för kontantkort skulle bli för den brottsutredande verksamheten. För att säkerställa att tillförlitliga uppgifter registreras skulle kontrollmekanismer behövas för att t.ex. förhindra att köpare av kontantkort uppger felaktiga personuppgifter och att vissa köpare registrerar sig för ett stort antal kontantkort och sedan tillhandahåller dessa i kriminella kretsar. Även om sådana kontrollmekanismer införs skulle de inte kunna förhindra att anonyma kontantkort köps utomlands och utnyttjas i Sverige i brottsliga sammanhang. Regeringen bedömer att det finns stora problem förknippade med ett system för registrering av abonnemangsuppgifter till kontantkort. Mot den angivna bakgrunden bör någon skyldighet att registrera abonnemangsuppgifter inte införas.

8 Ytterligare rättssäkerhetsgarantier m.m.

8.1 Underrättelse till enskild

Regeringens förslag: Enskild som innehar ett telefonnummer eller annan adress eller viss elektronisk kommunikationsutrustning som en hemlig övervakning av elektronisk kommunikation har avsett, ska i efterhand underrättas om övervakningen även när syftet med tvångsmedlet har varit att utreda vem som skäligen kan misstänkas för ett brott. Åklagaren ska ansvara för att underrättelse sker. Underrättelseskyldigheten ska inte gälla när integritetsintrånget för den enskilde kan antas vara ringa.

Regeringens bedömning: Någon underrättelseskyldighet i de brottsbekämpande myndigheternas underrättelseverksamhet bör inte införas. Det bör heller inte införas någon underrättelseskyldighet vid inhämtning av uppgifter om abonnemang.

Polismetodutredningens förslag och bedömning: Överensstämmer i sak med regeringens.

Remissinstanserna: Av de remissinstanser som har yttrat sig särskilt i denna del har *Åklagarmyndigheten* och *Datainspektionen* tillstyrkt förslaget och bedömningen. *Post- och telestyrelsen* har framhållit att det bör finnas en skyldighet att underrätta enskild vid inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet och efterlyst en tydligare redovisning av i vilken mån utredningens förslag i praktiken kommer att leda till att enskilda underrättas.

Skälen för regeringens förslag och bedömning

Underrättelseskyldighet i fråga om inhämtning som har skett i en förundersökning

Enligt gällande rätt omfattar underrättelseskyldigheten vid hemlig teleövervakning den som är eller har varit misstänkt för brott och innehavaren av den teleadress som den hemliga övervakningen har avsett (27 kap. 31 § rättegångsbalken). Detta innebär att i de fall åtgärden enligt 20 § första stycket 2 rättegångsbalken har avsett en teleadress som det finns synnerlig anledning att anta att en skäligen misstänkt person har kontaktat eller kommer att kontakta, innehavaren av den teleadressen ska underrättas. Underrättelseskyldigheten omfattar emellertid endast personer som är eller har varit innehavare av den övervakade adressen. Det innebär att för utredningen ovidkommande personer som har varit i kontakt med den övervakade adressen *inte* ska underrättas. Regeringen uttalade i samband med att bestämmelserna infördes att en underrättelseskyldighet beträffande sådana ovidkommande personer skulle skapa betydande praktiska problem och dessutom typiskt sett medföra att integritetskränkningen för den enskilde skulle kunna öka (prop. 2006/07:133 s. 39 f.).

Polismetodutredningen har framfört uppfattningen att det inte är motiverat att lämna en underrättelse till alla de personer som innehar ett telefonnummer eller annan adress eller viss elektronisk kommunikationsutrustning som omfattas av en s.k. basstationstömning (ett beslut om inhämtning av uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område) eftersom integritetsintrånget för den enskilde kan bedömas vara så ringa att det inte motiverar någon underrättelse. Regeringen delar utredningens uppfattning. Beträffande sådana för brottsutredningen ovidkommande personer skulle en underrättelseskyldighet typiskt sett innebära att integritetsintrånget ökar. Åtskilliga av dessa kommer inte heller att kunna identifieras, i varje fall inte utan att stora utredningsresurser läggs ned på identifieringen. Eftersom en basstationstömning inte kan sägas *avse* en teleadress i den mening som avses i 31 § behövs dock inget undantag för den situationen. De terminologiska förändringar som föreslagits i avsnitt 5.4 föranleder enligt regeringen ingen annan bedömning.

Utredningen har bedömt att det även finns andra situationer där en underrättelseskyldighet inte är motiverad. Ett sådant exempel är den bearbetning som sker i skedet efter en basstationstömning.

Myndigheterna kan då hämta in uppgifter beträffande de elektroniska kommunikationsutrustningar som befann sig på platsen i syfte att sortera ut de uppgifter som kan vara intressanta för den fortsatta utredningen. Regeringen delar bedömningen att någon underrättelseskyldighet inte är motiverad i de fall det har rört sig om en enstaka inhämtning av uppgifter i ett tidigt skede av brottsutredningen och åtgärden inte har lett till några ytterligare åtgärder mot personen i fråga. Som utredningen har föreslagit bör ett undantag för sådana situationer tas in i lagtexten. Undantaget bör dock endast omfatta fall av hemlig övervakning innan det finns en skäligen misstänkt person.

Utredningen har föreslagit att någon underrättelse inte heller ska lämnas i de fall det inte har fastställts vem som innehar den teleadress som tillståndet har avsett, t.ex. när åtgärden har avsett ett anonymt kontantkort. Regeringen konstaterar att det redan enligt nuvarande ordning torde förekomma att det inte har fastställts vem som innehar den adress som övervakningen har avsett när det har varit fråga om en teleadress som innehas av någon annan än den skäligen misstänkte. Det är då inte möjligt att lämna någon underrättelse. Att så inte ska ske får anses gälla utan ett uttryckligt undantag i lag.

Enligt gällande rätt ansvarar åklagare för att underrättelse om hemlig teleövervakning sker (14 b § förundersökningskungörelsen [1947:948]). Enligt utredningens förslag ska den åklagare, polisman eller tulltjänsteman som var förundersökningsledare när förundersökningen avslutades vara ansvarig för underrättelsen. Detta förslag ska ses mot bakgrund av att utredningen föreslagit att förundersökningsledare ska få fatta beslut om hemlig teleövervakning i syfte att fastställa vem som är skäligen misstänkt. Med hänsyn till att regeringen inte har föreslagit någon sådan möjlighet för förundersökningsledare (avsnitt 6.2.3) finns inte heller skäl att i detta avseende ändra nuvarande ordning.

Ingen underrättelseskyldighet i fråga om inhämtning som har skett i underrättelseverksamhet

Utredningen har bedömt att det inte bör införas någon skyldighet att underrätta enskild vid inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. *Post- och Telestyrelsen* har invänt mot den bedömningen. Utredningen har som skäl för sin uppfattning anfört att en sådan underrättelseskyldighet med hänsyn till verksamhetens framåtblickande perspektiv och övergripande natur riskerar att motverka huvudsyftet med underrättelseverksamheten. En underrättelseskyldighet skulle därför behöva förses med en rad undantag. Vidare skulle det i många fall kunna ta lång tid innan en underrättelse kunde lämnas och den eventuella identifiering och granskning av kommunikationen som måste föregå en underrättelse skulle kunna innebära en ytterligare integritetskränkning för dessa personer. I många fall torde det inte heller vara möjligt eller i vart fall förenat med betydande svårighet att identifiera den person som varit föremål för övervakningen. Det förtjänar därutöver att påpekas att en användning av uppgifterna i en förundersökning förutsätter tillstånd till hemlig övervakning av elektronisk kommunikation (se närmare avsnitt 6.3.3). I

de fall där uppgifterna innebär en påtaglig integritetspåverkan för en enskild blir därmed bestämmelserna om underrättelseskyldighet i 27 kap. 31–33 §§ rättegångsbalken tillämpliga. Europadomstolen har angett att såvitt avser hemlig övervakning ett objektivt övervakningssystem kan vara tillräckligt så länge som de åtgärder som riktas mot enskilda förblir hemliga och att det är först när åtgärderna har blivit kända som egentliga rättsmedel måste bli tillgängliga för den enskilde (Rotaru mot Rumänien, dom 2000-05-04).

Den tillsyn som Säkerhets- och integritetsskyddsnämnden kommer att utöva (se närmare avsnitt 8.2) tillsammans med möjligheten för enskild att begära en kontroll av om han eller hon har utsatts för inhämtning enligt den nya lagen om inhämtning av uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet och om denna i så fall har skett i enlighet med lag, innebär enligt regeringens uppfattning att Europakonventionens krav på tillgång till ett effektivt rättsmedel är uppfyllt. Mot den angivna bakgrunden och då integritetsintrånget måste anses som måttligt i de fall som inte kommer att omfattas av underrättelseskyldigheten enligt rättegångsbalken, delar regeringen utredningens bedömning att det inte bör införas någon skyldighet att underrätta enskild vid inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet.

Ingen underrättelseskyldighet i fråga om inhämtning av uppgifter om abonnemang

Som anges i avsnitt 7.2 bedömer regeringen att regleringen av de brottsbekämpande myndigheternas möjlighet att få uppgifter om abonnemang i samband med misstanke om brott även fortsättningsvis ska regleras i lagen om elektronisk kommunikation. Inhämtning av sådana uppgifter innebär inte ett så betydande integritetsintrång att de bör medföra något krav på underrättelseskyldighet. Regeringen delar utredningens bedömning att det inte finns skäl att införa en underrättelseskyldighet avseende inhämtande av abonnemangsuppgifter.

8.2 Säkerhets- och integritetsskyddsnämnden ska utöva tillsyn

Regeringens bedömning: Säkerhets- och integritetsskyddsnämnden ska utöva löpande tillsyn över inhämtningen av övervakningsuppgifter avseende elektronisk kommunikation m.m. i de brottsbekämpande myndigheternas underrättelseverksamhet.

Nämnden ska även vara skyldig att på begäran av en enskild person kontrollera om han eller hon har utsatts för inhämtning av sådana uppgifter i de brottsbekämpande myndigheternas underrättelseverksamhet och om inhämtningen och därmed sammanhängande verksamhet har skett i enlighet med lag eller annan författning.

Polismetodutredningens förslag och bedömning: Överensstämmer i allt väsentligt med regeringens. Utredningen har föreslagit att Säkerhets- och integritetsskyddsnämndens kapacitet ska förstärkas med ett eller flera granskningsombud som hos myndigheterna ska kontrollera hur befogenheterna att inhämta uppgifter har beslutats och använts.

Remissinstanserna: *Åklagarmyndigheten* har tillstyrkt förslaget. *JO, Sveriges advokatsamfund* och *Hovrätten för Västra Sverige* har framfört att det föreslagna antalet granskningsombud är för litet. *Säkerhets- och integritetsskyddsnämnden* har tillstyrkt att den tillförs denna tillsynsuppgift men har anfört att en ordning med särskilda granskningsombud är främmande för svensk rätt och att det är mer lämpligt att nämndens kansli förstärks för att möjliggöra tillsyn även på detta område. Nämnden har också anfört att det bör klargöras att nämndens nya tillsyn inte ska gälla retroaktivt i fråga om inhämtning av uppgifter enligt lagen (2003:389) om elektronisk kommunikation.

Säkerhetspolisen har framhållit att det är tveksamt om en och samma myndighet ska tilldelas uppgiften att utöva hela tillsynen/kontrollen över Säkerhetspolisen.

Skälen för regeringens bedömning

Gällande rätt

Säkerhets- och integritetsskyddsnämnden påbörjade sin verksamhet den 1 januari 2008. Verksamheten regleras i lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Nämnden ska bestå av högst tio ledamöter som utses av regeringen för en tid av högst fyra år. Ordföranden och vice ordföranden ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet.

Nämnden ska, såvitt här är av intresse, utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och därmed sammanhängande verksamhet samt Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen (1998:622). Tillsynen ska särskilt syfta till att säkerställa att verksamheten bedrivs i enlighet med lag eller annan författning. Tillsynen ska fr.o.m. den 1 mars 2012 även omfatta polisens behandling av personuppgifter enligt de föreslagna nya lagarna om polisens allmänna spaningsregister och polisdatalagen (prop. 2009/10:85).

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

inspektioner och andra undersökningar. I uppdraget ingår att uttala sig om konstaterade förhållanden och om behovet av förändringar i verksamheten. Nämnden ska vidare verka för att brister i lag eller annan författning avhjälps.

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

Nämnden har rätt att få de uppgifter och det biträde som nämnden begär, dels av de myndigheter som omfattas av tillsynen, dels av de domstolar och myndigheter som inte omfattas av denna. Nämndens beslut får inte överklagas.

Av 22 § förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden följer vidare att nämnden om den i sin verksamhet uppmärksammar förhållanden som kan utgöra brott, ska anmäla det till Åklagarmyndigheten eller annan behörig myndighet. Om nämnden uppmärksammar felaktigheter som kan medföra skadeståndsansvar för staten ska nämnden anmäla det till Justitiekanslern och finner den omständigheter som Datainspektionen bör uppmärksammas på ska nämnden anmäla det dit.

En ny tillsynsuppgift

Som framgår ovan är det av grundläggande betydelse att även de brottsbekämpande myndigheternas inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamheten omfattas av en effektiv och kontinuerlig tillsyn av en fristående myndighet. Mot bakgrund av de författningsreglerade uppgifter som Säkerhets- och integritetsskyddsnämnden har enligt beskrivningen ovan är det enligt regeringen ändamålsenligt och lämpligt att, såsom utredningen har föreslagit, nämndens verksamhet utökas till att avse även den nu föreslagna inhämtningen av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Regeringen delar inte den tveksamhet som *Säkerhetspolisen* har framfört i fråga om att nämnden tilldelas denna uppgift, utan anser att det tvärtom är följdriktigt att nämnden som redan utövar tillsyn över Säkerhetspolisens användning av hemliga tvångsmedel också tilldelas motsvarande tillsynsuppgifter över inhämtningen enligt den nya lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Utredningen har inte föreslagit någon ändring i lagen om tillsyn över viss brottsbekämpande verksamhet i fråga om omfattningen av nämndens tillsyn. *Säkerhets- och integritetsskyddsnämnden* har uppgett sig dela bedömningen att tillsynen över den inhämtning som kommer att ske enligt den nya lagen faller under nämndens tillsyn utan någon lagändring, genom att nämnden ska utöva tillsyn över användning av hemliga tvångsmedel (1 §). Varken i lagen om tillsyn över viss brottsbekämpande verksamhet eller i förarbetena till den definieras vad som avses med hemliga tvångsmedel. Avsikten är att tillsynen även ska omfatta fall då

användningen av metoderna sker otillåtet och att tillsynen även ska kunna omfatta eventuella nya tvångsmedel som införs (prop. 2006/07:133 s. 80). Regeringen delar bedömningen att den inhämtning som enligt förslaget ska kunna äga rum i underrättelseskedet och som har väsentliga likheter med den inhämtning som kan ske i en förundersökning inom ramen för ett tillstånd till hemlig övervakning av elektronisk kommunikation utgör ett hemligt tvångsmedel. Både utredningen och nämnden har dock påpekat att den inhämtning som sker enligt bestämmelserna i lagen om elektronisk kommunikation inte har ansetts omfattas av nämndens tillsyn. Att regeringen nu föreslår en ny reglering i fråga om inhämtning av uppgifter om elektronisk kommunikation i underrättelseskedet innebär ingen förändring av nämndens tillsynsansvar i fråga om inhämtning av uppgifter enligt lagen om elektronisk kommunikation.

En ordning med särskilda granskningsombud införs inte

Enligt utredningens förslag ska särskilda granskningsombud utses av nämnden för att utöva den nya tillsynsfunktionen. Ett granskningsombud ska vara eller ha varit ordinarie domare eller ha annan motsvarande juridisk erfarenhet. Enligt förslaget ska det vara nämnden som ska ta slutlig ställning till ett tillsynsärende och uttala sig om konstaterade förhållanden och eventuellt behov av förändringar i myndighetens underrättelseverksamhet. Vid den tillsyn över användningen av hemliga tvångsmedel som Säkerhets- och integritetsskyddsnämnden utövar enligt gällande rätt bistås nämnden av ett kansli. Utredningen har inte närmare utvecklat hur de föreslagna ombuden närmare skulle utöva granskningen eller vilka fördelar detta skulle medföra jämfört med om det sker en förstärkning av nämndens kansli. *Säkerhets- och integritetsskyddsnämnden* har framfört att det skulle vara mer lämpligt att kansliet förstärks. Regeringen anser mot denna bakgrund att det inte finns ett tillräckligt underlag för att överväga införandet av en ordning med särskilda granskningsombud för den utvidgade tillsynsuppgiften. Säkerhets- och integritetsskyddsnämnden har sedan januari 2008 bedrivit en fristående tillsynsverksamhet avseende bl.a. de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och därmed sammanhängande verksamhet. Vid myndigheten sker dessutom en kontinuerlig utveckling av arbetsformer och arbetsmetoder för att den på ett effektivt sätt och med hög kvalitet ska kunna fullgöra sina uppgifter. Med hänsyn till detta anser regeringen att det är en lämplig och ändamålsenlig lösning att, som Säkerhets- och integritetsskyddsnämnden själv förespråkat, förstärka nämndens kansli för de nya tillsynsuppgifterna. På så sätt säkerställs en effektiv resursanvändning som snabbt kan koncentreras till de områden som bedöms som mest angelägna. Det är som flera remissinstanser har påpekat av stor betydelse att tillsynen sker löpande. För att möjliggöra en sådan löpande granskning föreslår regeringen i avsnitt 6.3.2 att nämnden alltid ska underrättas om ett beslut om inhämtning av uppgifter om elektronisk kommunikation m.m. i underrättelseverksamhet.

8.3 Regeringens redovisning till riksdagen

Regeringens bedömning: Regeringens årliga skrivelse till riksdagen om användningen av vissa hemliga tvångsmedel i brottsutredningar bör även innehålla en redovisning av inhämtningen av uppgifter om elektronisk kommunikation i underrättelseverksamhet. Säkerhetspolisens inhämtning av uppgifter bör dock inte redovisas.

Polismetodutredningens bedömning: Överensstämmer med regeringens.

Remissinstanserna: Remissinstanserna har inte yttrat sig särskilt i denna del.

Skälen för regeringens bedömning: En parlamentarisk kontroll av tillämpningen av reglerna om bl.a. hemlig teleövervakning utövas av riksdagen bl.a. på grundval av en årlig skrivelse från regeringen. Regeringen har gett Åklagarmyndigheten och Rikspolisstyrelsen i uppdrag att årligen till regeringen lämna en gemensam redovisning för användningen av tvångsmedlen under föregående år. I den senaste skrivelsen, som avser användningen under år 2008 (skr. 2009/10:66), framgår att antalet fall av hemlig teleövervakning uppgick till 1 455 stycken. I skrivelsen redovisas vilka brott som besluten avsett, den genomsnittliga övervakningstiden och antalet fall där tvångsmedlet haft betydelse för förundersökningen. De fall av hemlig teleövervakning som avser Säkerhetspolisens ärenden redovisas i särskild ordning och inte i den skrivelse som lämnas till riksdagen eftersom Säkerhetspolisens uppgifter omfattas av sekretess enligt 15 kap. 2 § och 18 kap. 2 § offentlighets- och sekretesslagen (2009:400). Tillämpningen av lagen om särskild utlänningskontroll (1991:572), som också innefattar användningen av hemliga tvångsmedel, redovisas också i en skrivelse till riksdagen

Någon motsvarande redovisning till riksdagen av de fall där brottsbekämpande myndigheter har beslutat att inhämta uppgifter om elektronisk kommunikation med stöd av 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation har inte gjorts.

Enligt artikel 10 i EG:s direktiv (2006/24/EG) om lagring av trafikuppgifter ska det föras statistik över antalet verkställda beslut om hemlig teleövervakning och utlämnanden motsvarande dem i 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation samt vilka typer av brott som ärendena har avsett, hur lång tid som har förlöpt från det att respektive trafikuppgift lagrades till dess att den brottsbekämpande myndigheten begärde tillgång till uppgiften, antalet ärenden där myndigheternas begäran om att få tillgång till trafikuppgifter inte har kunnat tillgodoses av operatörerna och vilka typer av brott ärendena har avsett (SOU 2007:76 s. 281 f.). I propositionen Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG (prop. 2010/11:46) lämnas förslag hur direktivet ska införlivas i svensk rätt. Som framgår förutsätter direktivet att en redovisning av inhämtningen sker i fråga om uppgifter som har lagrats enligt direktivet.

Regeringen delar utredningens bedömning att det i den årliga skrivelsen till riksdagen om användningen av vissa hemliga tvångsmedel också bör redovisas inhämtning av uppgifter om elektronisk kommunikation och lokaliseringsuppgifter med koppling till elektroniska kommunikationsutrustningar i underrättelseverksamhet. I likhet med vad som gäller i fråga om övriga hemliga tvångsmedel bör uppgifter som rör Säkerhetspolisens inhämtning inte redovisas i skrivelsen.

8.4 Sekretess och tystnadsplikt

Regeringens förslag: Det ska införas en särskild tystnadsplikt för operatörer när det gäller brottsbekämpande myndigheters inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. Tystnadsplikten ska även omfatta uppgifter som hänför sig till inhämtning av uppgift om abonnemang.

Uppgifter om de brottsbekämpande myndigheternas inhämtning av övervakningsuppgifter om elektronisk kommunikation och elektroniska kommunikationsutrustningar i underrättelseverksamhet ska undantas från rätten att meddela och offentliggöra uppgifter.

Polismetodutredningens förslag: Överensstämmer i sak med regeringens. Utredningens författningsförslag utgår dock från sekretesslagen (1980:100).

Remissinstanserna: Endast *Säkerhetspolisen* har yttrat sig särskilt i denna del och har tillstyrkt förslaget.

Skälen för regeringens förslag

Sekretess med hänsyn till intresset av att förebygga eller beivra brott

I offentlighets- och sekretesslagen (2009:400) finns bestämmelser som syftar till att begränsa spridningen av information som innehas av de brottsbekämpande myndigheterna. Hos myndigheterna gäller sekretess bl.a. med hänsyn till intresset av att förebygga eller beivra brott och till skydd för enskilds personliga och ekonomiska förhållanden.

Enligt 18 kap. 1 § första stycket offentlighets- och sekretesslagen gäller sekretess för bl.a. uppgift som hänför sig till förundersökning i brottmål eller angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott. Sekretessen gäller om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Bestämmelsen gäller uppgifter som hänför sig till viss verksamhet. Det innebär att sekretessen för uppgifterna upprätthålls oavsett hos vilken myndighet de finns.

Av 18 kap. 2 § första stycket offentlighets- och sekretesslagen framgår att sekretess även gäller för uppgift som hänför sig till sådan underrättelseverksamhet som avses i 3 § polisdatalagen, dvs. polisverksamhet som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas och som inte utgör förundersökning enligt 23 kap.

rättegångsbalken. Av bestämmelsen framgår vidare att sekretess gäller för uppgift som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terrorism. Sekretess gäller om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Sekretess gäller under samma förutsättningar uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar samt sådan verksamhet som avses i 7 § 1 lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Sekretesskyddet för uppgifter som hänför sig till förundersökning och underrättelseverksamhet får genom dessa bestämmelser anses vara adekvat utformat.

Sekretess till skydd för enskilds personliga och ekonomiska förhållanden

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

Sekretessen enligt 35 kap. 1 § offentlighets- och sekretesslagen hindrar inte att uppgifter lämnas till enskild i vissa särskilt angivna fall, t.ex. enligt vad som föreskrivs i säkerhetsskyddslagen, lagen (1998:621) om misstankeregister och polisdatalagen. I 35 kap. 6–7 §§ offentlighets- och sekretesslagen finns bestämmelser om att sekretessen enligt 35 kap. 1 § första stycket offentlighets- och sekretesslagen i vissa fall inte gäller. Så är fallet för flertalet uppgifter som lämnas till domstol med anledning av åtal. När det gäller operatörers tystnadsplikt för bl.a. uppgifter om elektronisk kommunikation hänvisas till avsnitt 6.1.

Även sekretessen till förmån för enskildas personliga och ekonomiska förhållanden får anses adekvat utformat med avseende på uppgifter som hänför sig till förundersökning och underrättelseverksamhet.

En särskild tystnadsplikt för operatörer med avseende på inhämtning av abonnemangsuppgifter i brottsutredningssyfte införs

I bl.a. personuppgiftslagen (1998:204) och lagen om elektronisk kommunikation finns vissa allmänna bestämmelser om hur operatörer får behandla olika typer av uppgifter. Därutöver finns i 6 kap. 21 § lagen om elektronisk kommunikation en särskild straffsanktionerad tystnadsplikt för operatörerna när det gäller uppgifter som hänför sig till angelägenhet som avser användning av bl.a. hemlig övervakning av elektronisk kommunikation. Bestämmelsen innebär bl.a. att operatören inte får informera en abonnent om att denne är föremål för vissa

tvångsmedelsåtgärder. På liknande sätt finns i den immaterialrättsliga lagstiftningen bestämmelser som innebär att en operatör inte får underrätta en abonnent om ett s.k. informationsföreläggande förrän det har gått viss tid (se t.ex. 53 f § andra stycket lagen [1960:729] om upphovsrätt till litterära och konstnärliga verk).

Regeringen instämmer i utredningens förslag att bestämmelsen i 6 kap. 21 § lagen om elektronisk kommunikation ska kompletteras så att regleringen även omfattar uppgifter som hänför sig till inhämtning av övervakningsuppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Regleringen föreslås dessutom omfatta myndigheternas inhämtning av uppgift om abonnemang i syfte att utreda brott. Även i de fallen kan det finnas ett starkt intresse av att den som uppgiften avser inte får kännedom om inhämtningen och därigenom ges möjlighet att undanröja eventuell bevisning.

Rätten att meddela och offentliggöra uppgifter

Med rätten att meddela och offentliggöra uppgifter avses de rättigheter som följer av 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen. Enligt 1 kap. 1 § andra stycket tryckfrihetsförordningen står det varje svensk medborgare fritt att, med iakttagande av bestämmelserna i tryckfrihetsförordningen, i tryckt skrift yttra sina tankar och åsikter, offentliggöra allmänna handlingar samt meddela uppgifter och underrättelser i vilket ämne som helst. På motsvarande sätt har varje svensk medborgare enligt 1 kap. 1 § yttrandefrihetsgrundlagen rätt att i radio eller TV eller annat medium som omfattas av yttrandefrihetsgrundlagen offentligen uttrycka tankar, åsikter och känslor och i övrigt lämna uppgifter i vilket ämne som helst. Enligt 1 kap. 1 § tredje stycket tryckfrihetsförordningen och 1 kap. 2 § yttrandefrihetsgrundlagen står det vidare envar fritt att lämna uppgifter i vilket ämne som helst till de personkategorier och organ som anges i de sistnämnda bestämmelserna för publicering i de medier som de båda grundlagarna omfattar (den s.k. meddelarfriheten). Rätten att meddela och offentliggöra uppgifter är således ett vidare begrepp än meddelarfrihet och innefattar, förutom rätten att lämna uppgifter till någon annan för publicering eller på något annat sätt medverka till någon annans publicering, också rätten att själv, som ansvarig enligt grundlagarnas bestämmelser om ensamansvar, offentliggöra uppgifter.

Sekretess innebär såväl handlingssekretess som tystnadsplikt (3 kap. 1 § offentlighets- och sekretesslagen). Den rätt att meddela och offentliggöra uppgifter som följer av tryckfrihetsförordningen och yttrandefrihetsgrundlagen har som huvudregel företräde framför tystnadsplikten. Rätten att meddela och offentliggöra uppgifter har dock aldrig företräde framför handlingssekretessen (7 kap. 3 § första stycket 2 och 5 § 1 tryckfrihetsförordningen samt 5 kap. 1 § första stycket och 3 § första stycket 2 yttrandefrihetsgrundlagen). Det kan således vara tillåtet att t.ex. muntligen lämna en sekretessbelagd uppgift till en journalist eller att själv publicera uppgiften, men det är aldrig tillåtet att med stöd av rätten att meddela och offentliggöra uppgifter lämna den allmänna

handling av vilken den sekretessbelagda uppgiften framgår till t.ex. en journalist eller att själv publicera denna handling.

I ett antal fall har dock även bestämmelser om tystnadsplikt företräde. I dessa fall är således rätten att meddela och offentliggöra uppgifter helt inskränkt. Av 18 kap. 19 § offentlighets- och sekretesslagen framgår att uppgifter som omfattas av sekretess enligt 18 kap. 1–3 §§ offentlighets- och sekretesslagen och som avser användning av bl.a. hemlig teleövervakning är undantagna från rätten att meddela och offentliggöra uppgifter. Detsamma gäller enligt 44 kap. 4 § för uppgifter som omfattas av sekretess hos operatörerna enligt 6 kap. 20 § lagen om elektronisk kommunikation och som avser annan uppgift som angår ett särskilt elektroniskt meddelande, dvs. uppgifter som omfattas av regleringen i 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation. Inte heller uppgifter som omfattas av sekretess hos operatörerna enligt 6 kap. 21 § lagen om elektronisk kommunikation och som avser uppgift om bl.a. hemlig teleövervakning omfattas av rätten att meddela och offentliggöra uppgifter.

En inhämtning av övervakningsuppgifter om elektronisk kommunikation och elektroniska kommunikationsutrustningar i de brottsbekämpande myndigheternas underrättelseverksamhet kan i detta avseende jämställas med användningen av hemliga tvångsmedel i förundersökning. Regeringen föreslår därför att det även för sådana uppgifter införs undantag från rätten att meddela och offentliggöra uppgifter. Det gäller oavsett om tystnadsplikten följer av 18 kap. 1 § offentlighets- och sekretesslagen eller 6 kap. 21 § lagen om elektronisk kommunikation.

9 Ikraftträdande m.m.

Regeringens förslag: Lagändringarna ska träda i kraft den 1 juli 2011. Bestämmelsen i 4 § lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska gälla till och med den 31 december 2012.

Skälen för regeringens förslag: Lagförslagen bör träda i kraft så snart som möjligt. De bör därför träda i kraft den 1 juli 2011. Regeringen har i avsnitt 6.3.1 föreslagit att 4 § lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska gälla till och med den 31 december 2012.

När det gäller processrättslig lagstiftning är utgångspunkten att nya regler ska tillämpas genast efter ikraftträdandet. Det innebär att nya regler ska tillämpas på varje processuell företeelse som inträffar efter det att regleringen har trätt i kraft. Det medför att de brottsbekämpande myndigheterna och domstolarna ska tillämpa de nya bestämmelserna även i förundersökningar som har inletts innan de föreslagna bestämmelserna träder i kraft. Det finns inte behov av några övergångsbestämmelser.

10 Förslagens konsekvenser

Regeringens bedömning: Förslaget att ersätta de bestämmelser i lagen om elektronisk kommunikation som reglerar de brottsbekämpande myndigheternas tillgång till elektronisk kommunikation med en tydligare och mera rättssäker reglering medför vissa ökade kostnader. Dessa ska finansieras inom befintliga anslag på utgiftsområde 4 Rättsväsendet.

Polismetodutredningens bedömning: Överensstämmer i huvudsak med regeringens.

Remissinstanserna: Flera remissinstanser har framfört att förslagen för deras del kommer att medföra högre kostnader eller att de ekonomiska konsekvenserna behöver analyseras ytterligare.

Skälen för regeringens bedömning

Ekonomiska konsekvenser

Förslagen i denna remiss ger de rättsliga förutsättningarna för inhämtning av uppgifter om elektronisk kommunikation i underrättelseskedet och under förundersökning. De brottsutredande myndigheternas tillgång till uppgifter om elektronisk kommunikation m.m. ska enligt förslaget regleras dels i rättegångsbalken, dels i en ny lag om inhämtning av övervakningsuppgifter om elektronisk kommunikation m.m. i de brottsbekämpande myndigheternas underrättelseverksamhet. Bestämmelserna i lagen om elektronisk kommunikation, som innebär att de brottsutredande myndigheterna utan domstols eller åklagares prövning kan få del av övervakningsuppgifter avseende förfluten tid, föreslås upphävas.

Jämfört med den nuvarande regleringen i lagen om elektronisk kommunikation innebär förslagen att de brottsbekämpande myndigheterna ges viss utökad möjlighet att inhämta uppgifter. Uppgifter om elektronisk kommunikation ska enligt regeringens förslag till skillnad från vad som nu gäller kunna hämtas in i förundersökningar där det inte finns någon skäligen misstänkt även i fall där brottet inte har ett straffminimum på fängelse i två år, men där det på grund av omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år. Det införs också en möjlighet att inhämta lokaliseringsuppgifter som inte har samband med kommunikation. Detta talar för att det kan komma att ske en ökning av antalet inhämtade uppgifter. Förslagen innebär emellertid också att inhämtningen omgärdas av en snävare reglering i fråga om bl.a. för vilka syften inhämtningen får ske och vem som får besluta om inhämtning. Detta kan förväntas leda till en viss återhållsamhet i tillämpningen. Sammantaget bedömer regeringen till skillnad från utredningen att förslagen inte kan förväntas medföra någon ökning av antalet inhämtningar från operatörerna. Förslagen förväntas därför inte heller medföra några ökade kostnader för dem. Förslagen kan däremot för rättsväsendet förväntas medföra att kostnaden för varje inhämtning ökar, bl.a. genom kravet på domstolsprövning vid

inhämtning i en förundersökning och den utökade skyldigheten att underrätta enskild.

Det saknas statistik över hur många inhämtningar som görs enligt lagen om elektronisk kommunikation. BRU har uppskattat antalet inhämtningar till ca 4 000 per år. Trafikuppgiftsutredningen redovisade beräkningar från polisen som visade att antalet var ca 8 000 under år 2006 (SOU 2007:76 s. 225). Polisen har därefter gjort beräkningar över antalet inhämtningar under år 2007 och uppskattat dem till ca 9 500 (SOU 2009:1 s. 94). Det finns ingen uppgift om hur många av dessa inhämtningar som sker inom ramen för en förundersökning och hur många som sker i underrättelseskedet.

I propositionen Lagring av trafikuppgifter för brottsbekämpning – genomförande av direktiv 2006/24/EG, (prop. 2010/11:46), görs bedömningen att det förslaget kan förväntas innebära att de brottsbekämpande myndigheterna kommer att begära ut trafikuppgifter i något utökad utsträckning i förhållande till vad som nu gäller.

Polismetodutredningen har bedömt att dess förslag, med den utvidgning av framförallt underrättelseskyldigheten till enskild som förslaget innebär, skulle medföra ytterligare kostnader för de brottsbekämpande myndigheterna.

Polismetodutredningen uppskattar den sammanlagda kostnadsökningen för polisens del till 5 miljoner kr motsvarande 10-12 personer. Till skillnad från utredningens förslag innebär regeringens förslag dock inte att polisen åläggs någon underrättelseskyldighet till enskild. Regeringens förslag innebär till skillnad från utredningens förslag, inte heller någon rätt för förundersökningsledare att ge tillstånd till hemlig övervakning av elektronisk kommunikation. En viss kostnadsökning kan ändå uppkomma för polisen i form av ökade kostnader för administration genom att besluten om inhämtning i underrättelseskedet föreslås fattas av chefen för myndigheten och att det införs en skyldighet att underrätta Säkerhets- och integritetsskyddsnämnden om besluten. Enligt regeringens bedömning kan denna kostnadsökning dock beräknas bli betydligt lägre än vad utredningen har antagit. Regeringen anser att de marginellt ökade kostnader som kan förutses ska hanteras inom polisens befintliga anslag. Regeringen delar utredningens bedömning att förslagen för Tullverkets del inte bör medföra några ökade kostnader.

För Åklagarmyndigheten och Ekobrottsmyndigheten har utredningen bedömt kostnadsökningen till 5 miljoner kr, motsvarande fem åklagare. *Åklagarmyndigheten* och *Ekobrottsmyndigheten* har invänt mot denna bedömning. Enligt Åklagarmyndigheten kan förslagen förväntas medföra kostnader motsvarande tio åklagare för myndigheterna. Ekobrottsmyndigheten har framfört att kostnadsökningen för deras del kan beräknas till tre åklagare och fem poliser. Den kostnadsökning som förslagen medför för åklagarmyndigheterna består framförallt i den förmodade ökningen av antalet fall där domstol ska ge tillstånd till hemlig övervakning av elektronisk kommunikation och kostnaderna för den föreslagna möjligheten att fatta interimistiska beslut. Regeringens förslag innebär att fler ärenden ska prövas av domstol än vad Polismetodutredningen har föreslagit. Å andra sidan kommer förslaget att ett tillstånd till hemlig avlyssning av elektronisk kommunikation också ska ge tillgång till övervakningsuppgifter att medföra ett mindre antal

beslut om hemlig övervakning av elektronisk kommunikation. Ökningen kan trots det ändå förväntas bli mer betydande än den uppskattning som Polismetodutredningen har gjort om 500 ärenden per år. Som anförs ovan har inhämtning enligt lagen om elektronisk kommunikation uppskattats till 8 000-9 500 per år under åren 2006 och 2007. Merparten av inhämtningarna torde ske i underrättelseskedet eller i ett tidigt stadium av en brottsutredning. Ökningen av antalet ansökningar om tillstånd till hemlig övervakning av elektronisk kommunikation kan försiktigtvis uppskattas till motsvarande knappt hälften av det totala antalet inhämtningar enligt lagen om elektronisk kommunikation, dvs. ca 4 000 ärenden årligen. Den genomsnittliga kostnaden för ett ärende om hemlig övervakning av elektronisk kommunikation kan enligt uppgift från Åklagarmyndigheten uppskattas till 1 340 kr. Kostnadsökningen för Åklagarmyndigheten och Ekobrottsmyndigheten kan därmed uppskattas till ca 5 miljoner kr. Regeringen bedömer att denna ökning kan hanteras inom befintliga anslag.

För domstolarnas del leder förslaget till att fler ärenden om hemlig övervakning av elektronisk kommunikation behöver prövas. *Domstolsverket* har instämt i utredningens bedömning att kostnaden per ärende kan uppskattas till 1 000 kr. Regeringen gör ingen annan bedömning. Med den uppskattade ökningen av antalet tillstånd till hemlig övervakning av elektronisk kommunikation (knappt 4 000 fall), blir den sammanlagda kostnaden för domstolarna knappt 4 000 000 kr vilken enligt regeringens bedömning kan hanteras inom befintligt anslag.

Regeringen föreslår också en förstärkning av Säkerhets- och integritetsskyddsnämndens tillsyn av Säkerhetspolisens, den öppna polisens och Tullverkets underrättelseverksamhet. Utredningen gör bedömningen att deras förslag, med två eller flera särskilda av nämnden utsedda granskningsombud motsvarande två årsarbetskrafter, skulle medföra en årlig kostnadsökning för Säkerhets- och integritetsskyddsnämnden uppgående till 3 miljoner kr. *Säkerhets- och integritetsskyddsnämnden* har själva uppskattat kostnaden för att förstärka kansliet till 4,5 miljoner kr per år, motsvarande tre årsarbetskrafter, resor, lokaler, säkerhetsskydd, m.m. Regeringens förslag innebär att nämndens arbetsbelastning ökar jämfört med förslaget eftersom nämnden kommer att underrättas om samtliga beslut om inhämtning i underrättelseverksamhet. Regeringens förslag att granskningen ska utföras av nämndens kansli kommer dock sannolikt att innebära en lägre kostnad än införandet av särskilda granskningsombud. Regeringen bedömer sammantaget att kostnadsökningen för Säkerhets- och integritetsskyddsnämnden kommer att uppgå till ungefär den som utredningen har uppskattat. Regeringen bedömer i nuläget att detta kan hanteras inom befintliga anslagsramar.

Övriga konsekvenser

Förslagen bedöms inte påverka kostnader eller intäkter för kommuner, landsting, företag eller andra enskilda. Inte heller bedöms förslagen ha någon betydelse för den kommunala självstyrelsen, sysselsättningen, den offentliga servicen i olika delar av landet eller små företags

arbetsförutsättningar, konkurrensförmåga, eller villkor i övrigt i förhållande till större företag. Den nya regleringen bedöms inte heller ha någon påverkan på jämställdheten mellan män och kvinnor, möjligheterna att nå de integrationspolitiska målen eller miljön.

11 Författningskommentar

11.1 Förslaget till lag (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

1 § Denna lag innehåller bestämmelser om befogenhet för polismyndighet och Tullverket att i underrättelseverksamhet i hemlighet hämta in uppgifter om elektronisk kommunikation eller om lokaliseringen av elektronisk kommunikationsutrustning från den som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

I paragrafen anges lagens tillämpningsområde. Övervägandena finns i avsnitten 6.1 och 6.3.1.

Lagen ger polismyndighet (såväl den öppna polisen som Säkerhetspolisen) och Tullverket befogenhet att i underrättelseverksamhet i hemlighet hämta in uppgifter om elektronisk kommunikation och lokaliseringsuppgifter avseende elektroniska kommunikations-utrustningar från den som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Vilka typer av uppgifter som får hämtas in framgår av 2 §. Bestämmelsen bryter den tystnadsplikt för operatörer som framgår av 6 kap. 20–21 §§ lagen om elektronisk kommunikation. De brottsbekämpande myndigheternas möjlighet att med egna tekniska hjälpmedel hämta in uppgifter om elektronisk kommunikation omfattas inte av lagen. Begreppen elektroniskt kommunikationsnät och elektronisk kommunikationstjänst har samma innebörd som enligt lagen om elektronisk kommunikation. Angående begreppet elektronisk kommunikationsutrustning, se närmare kommentaren till 27 kap. 19 § rättegångsbalken.

2 § Inhämtning får avse uppgifter om

1. meddelanden som i ett elektroniskt kommunikationsnät har överförts till eller från ett telefonnummer eller annan adress,
2. vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller
3. i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

Paragrafen preciserar vilka typer av uppgifter som får inhämtas enligt lagen. Övervägandena finns i avsnitten 6.3.1 och 6.4.

Inhämtningen får avse samma typ av uppgifter som föreslås kunna hämtas in inom ramen för ett tillstånd till hemlig övervakning av elektronisk kommunikation enligt 27 kap. 20 § andra stycket rättegångsbalken, se närmare kommentaren till den bestämmelsen.

3 § Uppgifter får hämtas in om omständigheterna är sådana att

1. åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, och
2. skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Paragrafen innehåller förutsättningarna för att de uppgifter som anges i 2 § ska få hämtas in. Övervägandena finns i avsnitt 6.3.1.

Genom rekvisitet ”brottslig verksamhet” i *första punkten* framgår att regleringen inte ställer upp något krav på att det ska finnas en misstanke om ett specifikt brott. Det föreligger därför en principiell skillnad i förhållande till tillämpningsområdet för straffprocessuella tvångsmedel enligt rättegångsbalken. Uppgifterna får alltså hämtas in om någon del av den brottsliga verksamhet, som t.ex. en viss gruppering antas vara delaktig i, innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Detta motsvarar de brott i fråga om vilka inhämtning tidigare var möjlig enligt 6 kap. 22 § första stycket 3 lagen om elektronisk kommunikation. Begreppen förebygga, förhindra och upptäcka brottslig verksamhet används t.ex. i 7 § lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet och 2 kap. 7 § polisdatalagen (2010:361). I förarbetena till dessa bestämmelser anges att vad som framförallt avses är arbete med att insamla, bearbeta och analysera information för att förebygga, förhindra eller upptäcka brottslig verksamhet när det ännu inte finns konkreta misstankar om att ett visst brott har begåtts (prop. 2004/05:164 s. 115 f. och 2009/10:85 s. 318). I fråga om sådana gärningar som kan utgöra tryck- eller yttrandefrihetsbrott får uppgiftsinhämtningen givetvis inte inkräkta på bestämmelserna om censur och hindrande åtgärder i tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Att omständigheterna ska vara sådana att åtgärden ska vara av särskild vikt för att förebygga, förhindra eller upptäcka viss brottslig verksamhet innebär att det ska finnas andra uppgifter (t.ex. källinformation) som möjliggör en bedömning av uppgifternas förväntade betydelse för att t.ex. förebygga eller förhindra sådan brottslig verksamhet som avses i bestämmelsen. I detta ligger också ett krav på uppgifternas förväntade betydelse för det syfte i vilket de inhämtas. Kravet på särskild vikt innefattar alltså både ett kvalitetskrav på de upplysningar som åtgärden kan ge och ett krav på behovet av inhämtningen i det enskilda fallet. Bedömningen får inte bygga enbart på spekulationer eller allmänna antaganden utan måste grundas på faktiska omständigheter.

Utrymmet för att inhämta uppgifter för att *förebygga brott* kan med hänsyn till ovan nämnda krav på konkretion komma att bli begränsat. Ett exempel inom Säkerhetspolisens ansvarsområde på när sådan inhämtning ändå under vissa omständigheter kan vara tillåten är inhämtning i syfte att förebygga terroristbrott. Om det finns uppgifter om att personer som får viss träning eller utbildning utomlands kan komma att begå ett terroristbrott, kan inhämtning i syfte att kartlägga personer som deltar i eller verkar för att sådana tränings- och utbildningsaktiviteter kommer till stånd bedömas vara av särskild vikt för att förebygga brottslig verksamhet som innefattar ett terroristbrott. Däremot innebär kraven på konkretion bl.a. i fråga om vilken typ av brottslighet som ska förebyggas

att det t.ex. inte kan bli fråga om att rutinmässigt inhämta uppgifter i syfte att kartlägga personer enbart på grund av att de är kriminellt belastade eller ingår i en viss grupp eller nätverk.

I *andra punkten* anges att proportionalitetsprincipen ska tillämpas vid ett beslut om inhämtning. Principen brukar i korthet beskrivas på det sättet att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden. Myndigheten måste alltid beakta principen när den prövar om inhämtning av uppgifter ska få ske enligt denna lag. Vid inhämtningen ska bl.a. hänsyn tas till om åtgärden innebär intrång i ett rättsligt skyddat intresse, t.ex. meddelarskyddet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Innebär inhämtningen ett kringgående av förbudet för massmedier att röja sina källor eller för det allmänna att efterforska vem som är meddelare får inhämtning inte ske. Proportionalitetsprincipen får betydelse också för i vilken omfattning inhämtning ska få ske (se även 6 §) och vilka villkor som beslutet eventuellt ska förenas med. Den gäller vidare under hela verkställighetsförfarandet och ska alltså, även sedan beslut om inhämtning har fattats, beaktas av myndigheten. Integritetsintrånget under verkställigheten kan bli så stort att åtgärden att hämta in uppgifter inte längre kan anses tillåten, trots att rekvisiten i punkten 1 fortfarande är uppfyllda.

4 § Uppgifter får också, under de förutsättningar som anges i 3 § 2, hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar

1. sabotage enligt 13 kap. 4 § brottsbalken,
2. kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,
4. spionerі, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet, grovt brott, enligt 19 kap. 5, 8 eller 10 § tredje stycket brottsbalken, eller
5. grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.

Paragrafen innehåller en särskild reglering i fråga om vissa brott som ligger inom Säkerhetspolisens verksamhetsområde. Övervägandena finns i avsnitt 6.3.1.

Möjligheten till inhämtning av uppgifter utvidgas i förhållande till 3 § till att även omfatta brottslig verksamhet som innefattar vissa särskilt angivna brott som har ett minimistraff som understiger fängelse två år. De aktuella brotten återfinns såväl i lagen om åtgärder för att utreda vissa samhällsfarliga brott som i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Förutsättningarna för inhämtning överensstämmer i övrigt med vad som anges i 3 §. Genom förslaget till lag (0000:00) om ändring i lag (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas

underrättelseverksamhet tidsbegränsas bestämmelsen t.o.m. den 31 december 2012.

5 § Beslut om inhämtning av uppgifter fattas av myndigheten. Myndighetschefen får delegera rätten att fatta beslut om inhämtning till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs.

Paragrafen reglerar vilka som får besluta att inhämta uppgifter enligt denna lag. Övervägandena finns i avsnitt 6.3.2.

Av paragrafen framgår att det är den brottsbekämpande myndigheten som beslutar om inhämtning av uppgifter. Beslutanderätten ligger därmed för polisens del hos rikspolischefen, säkerhetspolischefen och länspolismästarna och för tullens del hos generaltulldirektören. Av paragrafen framgår vidare att myndighetschefen får delegera beslutanderätten. Delegation får ske till annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Avsikten är att restriktivitet ska iakttas vid delegation till anställda som operativt deltar i underrättelseverksamheten. Delegation bör kunna ske till t.ex. myndighetschefens ställföreträdare, rikskriminalchefen, biträdande rikskriminalchefen, biträdande säkerhetspolischefen, biträdande länspolismästare, länskriminalchefer, chefer för operativ verksamhet och chefer för underrättelseverksamhet.

6 § I ett beslut om inhämtning av uppgifter ska det anges vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet avser. Tiden får inte bestämmas längre än nödvändigt och får, när det gäller tid som infaller efter beslutet inte överstiga en månad från dagen för beslutet.

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

Paragrafen reglerar vad som ska ingå i ett beslut om inhämtning och när ett beslut om inhämtning ska hävas. Övervägandena finns i avsnitt 6.3.1.

Första stycket reglerar vilka uppgifter ett beslut om inhämtning av uppgifter ska innehålla och motsvarar i princip vad som gäller vid hemlig övervakning av elektronisk kommunikation enligt 27 kap. 21 § andra och tredje styckena rättegångsbalken. Att det ska anges vilken brottslig verksamhet beslutet avser innebär att det vid inhämtning som sker enligt 3 § ska anges vilket eller vilka brott som innefattas i den brottsliga verksamhet som avses och att det vid inhämtning som sker enligt 4 § ska anges vilken av punkterna 1–5 som ligger till grund för beslutet. Den tid som ska anges får inte bestämmas längre än nödvändigt. Det gäller för såväl historiska uppgifter som realtidsuppgifter. Vad avser sistnämnda uppgifter gäller den ytterligare begränsningen att tiden inte får överstiga en månad från dagen för beslutet. Vidare ska den adress, den elektroniska kommunikationsutrustning eller det geografiska område som tillståndet avser anges i beslutet. Beslutet om att inhämta uppgifter bör hanteras inom ett särskilt inhämtningsärende som avslutas när inhämtningen har skett.

I *andra stycket* föreskrivs att ett beslut om inhämtning av uppgifter omedelbart ska hävas om det inte längre finns skäl för beslutet. Detta

överensstämmer i princip med vad som gäller för hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation enligt 27 kap. 23 § rättegångsbalken. Om det under den tid som inhämtning av uppgifter får ske har kommit fram att det inte längre finns förutsättningar för beslutet, t.ex. på grund av att den brottsliga verksamhet som skulle förhindras ändå har lett till att specifika brott misstänks ha begåtts, ska den brottsbekämpande myndigheten häva beslutet. Finns det i sådant fall fortfarande tillräckliga skäl för att inhämta uppgifter kan det bli aktuellt att besluta om hemlig övervakning av elektronisk kommunikation enligt rättegångsbalkens regler.

7 § Säkerhets- och integritetsskyddsnämnden ska underrättas om ett beslut om inhämtning av uppgifter enligt denna lag. Underrättelsen ska lämnas senast en månad efter det att ärendet om inhämtning avslutades.

Paragrafen reglerar underrättelseskyldigheten till Säkerhets- och integritetsskyddsnämnden. Övervägandena finns i avsnitt 6.3.2.

Av paragrafen framgår att Säkerhets- och integritetsskyddsnämnden ska underrättas om ett beslut om tillstånd till inhämtning av uppgifter enligt lagen. Underrättelsen ska lämnas senast en månad efter det att inhämtningsärendet har avslutats, se vidare kommentaren till 6 §.

8 § Om det vid inhämtning av uppgifter enligt denna lag har kommit fram uppgifter om annan brottslig verksamhet än som omfattas av beslutet om inhämtning, får uppgifterna användas för att förhindra brott.

Paragrafen reglerar polisens och Tullverkets användning av inhämtade uppgifter för att förhindra brott. Övervägandena finns i avsnitt 6.3.3.

I paragrafen finns ingen begränsning i fråga om användningen av inhämtade uppgifter i syfte att förhindra brott.

9 § Uppgifter som har kommit fram vid inhämtning enligt denna lag får användas i en förundersökning endast efter tillstånd till hemlig övervakning av elektronisk kommunikation. Utan ett sådant tillstånd får dock inhämtade uppgifter ligga till grund för att inleda en förundersökning.

Paragrafen reglerar polisens och Tullverkets användning av inhämtade uppgifter för att utreda brott. Övervägandena finns i avsnitt 6.3.3.

Av paragrafens första mening framgår att inhämtade uppgifter får användas i en förundersökning endast om tillstånd till hemlig övervakning av elektronisk kommunikation har meddelats. Frågan om sådant tillstånd prövas enligt bestämmelserna i rättegångsbalken. Om tillstånd meddelas får åklagaren avgöra om uppgifterna ska begäras in från operatörerna på nytt eller om uppgifterna ska föras över från underrättelseverksamheten till förundersökningen. Av andra meningen följer att det inte krävs tillstånd till hemlig övervakning av elektronisk kommunikation för att uppgifterna ska få ligga till grund för att inleda en förundersökning. Efter att förundersökning har inletts får uppgifterna dock användas i förundersökningen endast om rätten har gett tillstånd till hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § rättegångsbalken. Att uppgifterna inte får användas i förundersökningen innebär i praktiken att ytterligare utredningsåtgärder får anstå till dess att

rätten har prövat frågan om tillstånd till elektronisk kommunikation, om inte andra uppgifter tillkommer som medför att det även utan övervakningsuppgifterna finns förutsättningar att bedriva förundersökningen.

10 § Uppteckningar av uppgifter ska granskas snarast möjligt.

Uppteckningar ska, i de delar de är av betydelse för att förebygga, förhindra eller upptäcka brottslig verksamhet som omfattas av beslutet om inhämtning eller att förhindra annat brott, bevaras så länge det behövs för något av dessa syften. De ska därefter förstöras.

Det som sägs i andra stycket hindrar inte att brottsbekämpande myndigheter behandlar uppgifter från uppteckningar i enlighet med vad som är särskilt föreskrivet i lag.

I paragrafen regleras polisens och Tullverkets hantering och behandling av uppteckningar av inhämtade uppgifter. Övervägandena finns i avsnitt 6.3.4.

Enligt *första stycket* ska en uppteckning av uppgifter, på samma sätt som vid hemlig övervakning av elektronisk kommunikation, granskas snarast möjligt (jfr 27 kap. 24 § rättegångsbalken). Det är den brottsbekämpande myndigheten som utför granskningen.

Av *andra stycket* framgår att uppteckningar som är av betydelse för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som omfattas av beslutet om inhämtning, eller för att förhindra brott, bevaras så länge det behövs för något av dessa syften. De ska därefter förstöras. Om uppgifterna använts i en förundersökning blir regleringen om bevarande av uppgifter i 27 kap. 24 § andra stycket rättegångsbalken tillämplig på uppgifterna (jfr 9 §). När uppteckningarna inte längre ska bevaras, ska de förstöras. Med det avses att uppgifterna ska utplånas, inte enbart att uppgifterna görs oåtkomliga för den operativa verksamheten.

Tredje stycket innehåller ett undantag från vad som föreskrivs om förstörande av uppteckningar enligt andra stycket. Om uppgifterna inte längre ska bevaras enligt andra stycket, t.ex. på grund av att den brottsliga verksamhet som skulle förhindras trots allt har inneburit att brott har genomförts, innebär tredje stycket att uppgifterna ändå kan behandlas t.ex. i syfte att utreda brott, om sådan användning är tillåten enligt annan lag. De lagar som främst kan komma i fråga är polisdatalagen och lagen om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet. I fråga om gallring m.m. av uppgifterna gäller då vad som föreskrivs i de lagarna.

11.2 Förslaget till lag (0000:00) om ändring i lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Härigenom föreskrivs att 4 § lag (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska upphöra att gälla vid utgången av december 2012.

Lagen innebär att möjligheten att inhämta uppgifter enligt 4 § lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet vid brottslig verksamhet som innefattar vissa brott som ligger under Säkerhetspolisens verksamhetsområde tidsbegränsas till den 1 januari 2013. Övervägandena finns i avsnitt 6.3.1.

11.3 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 i ett elektroniskt kommunikationsnät,* döms för *brytande av post- eller telehemlighet* till böter eller fängelse i högst två år.

Paragrafen behandlar brottet brytande av post- eller telehemlighet. Övervägandena finns i avsnitten 5.2 och 5.3.

Begreppet telemeddelande har ersatts med meddelande som förmedlas i ett elektroniskt kommunikationsnät (se vidare kommentaren till 27 kap. 18 § rättegångsbalken). Med elektroniskt kommunikationsnät avses detsamma som i lagen (2003:389) om elektronisk kommunikation. Ändringen är inte avsedd att innebära någon förändring i fråga om omfattningen av det straffrättsliga ansvaret.

11.4 Förslaget till lag om ändring i rättegångsbalken

27 kap. Om beslag, hemlig avlyssning av elektronisk kommunikation m.m.

18 § Hemlig *avlyssning av elektronisk kommunikation* innebär att *meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts* till eller från ett telefonnummer eller annan *adress,* i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.

Hemlig *avlyssning av elektronisk kommunikation* får användas vid förundersökning *som avser*

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 till hemlig avlyssning av elektronisk kommunikation ger också rätt att vidta sådana åtgärder som anges i 19 §.

I paragrafen anges vad tvångsmedlet hemlig avlyssning av elektronisk kommunikation (nuvarande hemlig teleavlyssning) innebär och en uppräkning av vid vilka brott tvångsmedlet får användas. Övervägandena finns i avsnitten 5 och 6.2.1.

I *första stycket* har begreppet hemlig teleavlyssning ersatts av det nya begreppet hemlig avlyssning av elektronisk kommunikation och begreppet telemeddelande med meddelande som överförs eller har

överförts i ett elektroniskt kommunikationsnät. Vad som avses med ett sådant nät framgår av 1 kap. 7 § lagen om elektronisk kommunikation. Elektroniskt kommunikationsnät är ett vidare begrepp än telenät (som tidigare använts i t.ex. 20 §) då det även avser nät som är avsett för utsändning till allmänheten av radio och television. Ändringen är dock inte avsedd att medföra någon utvidgning i fråga om tillämpningsområdet för tvångsmedlen. Vidare har begreppet teleadress bytts ut mot adress och begreppet kod har utgått. Begreppet befordra har ersatts med överföra för att bättre överensstämma med terminologin i lagen om elektronisk kommunikation.

I *andra stycket* har begreppet hemlig teleavlyssning ersatts med begreppet hemlig avlyssning av elektronisk kommunikation.

Det *tredje stycket*, som är nytt, innebär att ett tillstånd till hemlig avlyssning av elektronisk kommunikation även ger rätt att hämta in sådana övervakningsuppgifter om elektronisk kommunikation som anges i 19 § första stycket 1 och 3 och avser den adress eller kommunikationsutrustning som omfattas av tillståndet. Det innebär också att ett tillstånd till hemlig avlyssning av elektronisk kommunikation ger rätt att hindra meddelanden från att nå fram i enlighet med vad som anges i 19 § andra stycket. Bestämmelsen innebär att åklagaren inte behöver ansöka om tillstånd till båda tvångsmedlen för att få såväl uppgifter om innehållet i ett meddelande som andra uppgifter om detta. Om rätten till hemlig avlyssning upphör, faller också rätten att få ta del av övervakningsuppgifter. Om det då fortfarande finns behov av att ta del av övervakningsuppgifter, får en ansökan enligt 19 § göras.

19 § Hemlig *övervakning av elektronisk kommunikation* innebär att uppgifter i hemlighet hämtas in om

1. meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress,

2. vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller

3. i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

Genom hemlig övervakning av elektronisk kommunikation får sådana meddelanden som avses i första stycket 1 även hindras från att nå fram.

Hemlig *övervakning av elektronisk kommunikation* får användas vid förundersökning *som avser*

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

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

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

I fall som avses i 20 § andra stycket får hemlig övervakning av elektronisk kommunikation dock användas endast vid förundersökning som avser brott som kan föranleda hemlig avlyssning av elektronisk kommunikation enligt 18 § andra stycket.

I paragrafen anges vad tvångsmedlet hemlig övervakning av elektronisk kommunikation (nuvarande hemlig teleövervakning) innebär och en uppräkning av vid vilka brott tvångsmedlet får användas. Övervägandena finns i avsnitten 6.2.2 och 6.4.

I *första stycket* har begreppet telemeddelande ersatts av begreppet meddelande i ett elektroniskt kommunikationsnät, se vidare kommentaren till 18 §. Det meddelande som övervakas ska överföras eller ha överförts till eller från ett telefonnummer eller annan adress, i stället för som tidigare en teleadress. Paragrafen har också ändrats så att det blir möjligt att inhämta uppgifter om lokalisering av en viss elektronisk kommunikationsutrustning oavsett om några meddelanden har överförts till eller från utrustningen eller inte. Det rör sig framförallt om uppgifter om lokalisering av mobiltelefoner, men även annan elektronisk utrustning som kan anslutas till ett elektroniskt kommunikationsnät för kommunikation omfattas. Uppgifter kan hämtas in dels om vilka kommunikationsutrustningar som har funnits inom ett visst geografiskt område (s.k. basstationstömning), dels om inom vilket område en viss sådan utrustning finns eller har funnits. Inhämtning av lokaliseringsuppgifter får ske även om utrustningens identifikationsnummer är okänt. Som framgår av 20 § första stycket kan inhämtningen avse ett telefonnummer eller annan adress. På samma sätt ska en basstationstömning kunna ge upplysningar om telefonnumret till ett kontantkort som använts i en mobiltelefon som befunnit sig på den aktuella platsen.

Bestämmelsen att tvångsmedlet även får användas för att hindra ett meddelande från att nå fram har flyttats från första stycket till ett nytt *andra stycke.*

I *tredje stycket*, tidigare andra stycket, har begreppet hemlig teleövervakning ersatts av det nya begreppet hemlig övervakning av elektronisk kommunikation.

Vid förundersökning som avser brott som anges i 18 § andra stycket får enligt *fjärde stycket,* som är nytt, hemlig övervakning av elektronisk kommunikation användas i syfte att utreda vem som skäligen kan misstänkas för brottet.

20 § Hemlig *avlyssning av elektronisk kommunikation och* hemlig *övervakning av elektronisk kommunikation* får*, om inte annat följer av andra stycket , endast ske* om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får endast avse

1. *ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning* 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. *ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning* som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Hemlig övervakning av elektronisk kommunikation får, utöver vad som anges i första stycket, ske i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Övervakning som innebär att uppgifter hämtas in om meddelanden får dock endast avse förfluten tid.

Avlyssning eller övervakning får inte avse meddelanden som endast överförs eller har överförts 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 förutsättningarna för när hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation får användas. Övervägandena finns i avsnitten 5.4 och 6.2.2.

Hemlig teleavlyssning och hemlig teleövervakning har ersatts med de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Hemlig avlyssning och hemlig övervakning ska enligt *första stycket*, i stället för att avse en teleadress, avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning. Att ”viss elektronisk kommunikationsutrustning” lagts till tydliggör att det är möjligt att låta ett tillstånd till hemlig övervakning avse t.ex. en viss mobiltelefon med ett visst identifikationsnummer, se vidare kommentaren till 19 §. I stycket erinras också om att andra stycket innehåller avvikande regler vad gäller kravet på att det ska finnas någon som är skäligen misstänkt för brottet.

Andra stycket, som har fått ett nytt innehåll, reglerar förutsättningarna för att använda hemlig övervakning av elektronisk kommunikation för att utreda vem som skäligen kan misstänkas för brottet. I stycket anges att hemlig övervakning av elektronisk kommunikation får ske i syfte att utreda vem som skäligen kan misstänkas för brottet. Av 19 § fjärde stycket framgår att en första förutsättning är att brottsmisstanken gäller brott som är av den svårhetsgrad som gäller för användning av hemlig avlyssning av elektronisk kommunikation, dvs. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, försök, förberedelse eller stämpling till sådant brott eller annat brott som med hänsyn till omständigheterna kan antas ha ett straffvärde som överstiger fängelse i två år. Syftet med inhämtningen ska vara att kunna identifiera en skäligen misstänkt gärningsman. Att syftet ska vara att utreda vem som skäligen kan misstänkas för brottet utesluter dock inte att åtgärden primärt kan ta sikte på att utröna var t.ex. en brottsplats är belägen, om den upplysningen är av avgörande betydelse för att utreda vem som skäligen kan misstänkas för brottet. Om det finns en skäligen misstänkt person kan inhämtning ske i syfte att identifiera ytterligare personer som skäligen kan misstänkas för brott. Inhämtningen ska vidare vara av synnerlig vikt för utredningen. Det innebär, på samma sätt som vid övriga beslut om hemlig övervakning av elektronisk kommunikation, ett kvalitetskrav på de upplysningar som åtgärden kan ge. Upplysningarna får inte inskränka sig till detaljer av mindre betydelse. Uttrycket innefattar därutöver ett krav på att utredningsläget gör åtgärden nödvändig (prop. 1988/89:24 s. 24 f.). Begränsningen i första stycket 1–2 att åtgärden endast får avse en viss adress eller kommunikationsutrustning med viss koppling till en misstänkt person gäller inte. I stället gäller att övervakning som avser meddelanden endast får avse förfluten tid. Det innebär att inhämtning enligt bestämmelsen inte är möjlig i fråga om realtidsuppgifter om meddelanden (jfr 19 § första stycket 1). Vid tillämpningen av andra stycket bör åklagare och domstol begränsa tillståndet så att mängden överskottsinformation minimeras. Övervakningsuppgifter som avser de mobiltelefoner som används eller har använts i anslutning till ett visst brott bör normalt avgränsas till ett geografiskt område som motsvarar brottsplatsen och

området däromkring. Avgränsningen för hur stort området kring brottsplatsen som åtgärden får vidtas inom måste bedömas från fall till fall. Det är naturligt att ett större område kan bli föremål för övervakning om brottet har begåtts på landsbygden än om det skett i en storstad. Bestämmelsen ger även utrymme för att inhämta uppgifter inom områden som polisen befarar gärningsmannen har använt som flyktväg från brottsplatsen. Vid misstanke om brott som kan pågå en längre tid och där gärningsmannen kan tänkas förflytta sig, t.ex. vid människorov (4 kap. 1 § brottsbalken), kan övervakningsuppgifter behöva inhämtas avseende mer vidsträckta områden.

I *tredje stycket*, tidigare andra stycket, har begreppet telemeddelande ersatts av begreppet meddelande. Begreppet telenät har ersatts med elektroniskt kommunikationsnät, se kommentaren till 18 §.

21 § Frågor om hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* och hemlig kameraövervakning prövas av rätten på ansökan av åklagaren.

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

I ett tillstånd till hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation ska det anges vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område* tillståndet avser. Det ska vidare särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga *elektroniska kommunikationsnät*.

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

Paragrafen innehåller bestämmelser om prövningen av frågor om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation samt hemlig kameraövervakning och vad som ska anges i ett tillståndsbeslut.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

De nya beteckningarna för tvångsmedlen har även tagits in i *tredje stycket.* Dessutom har begreppet teleadress bytts ut. I ett beslut om hemlig avlyssning eller hemlig övervakning ska, i stället för teleadress, anges vilket telefonnummer eller annan adress eller vilken elektronisk kommunikationsutrustning som beslutet avser. Det ankommer således på domstolen eller åklagaren, när frågan om tvångsmedel prövas, att avgöra vad (telefonnummer, annan adress eller elektronisk kommunikationsutrustning) som beslutet ska avse, se kommentaren till 20 §. Ett beslut som ger tillstånd till hemlig avlyssning eller hemlig övervakning av kommunikation via e-post bör t.ex. normalt inte anknyta till viss elektronisk kommunikationsutrustning (själva datorn) utan till en viss e-postadress. Däremot kan det i vissa fall vara lämpligt att ett beslut om avlyssning eller övervakning knyts till en viss mobiltelefon. Vid tillstånd till inhämtning av uppgifter om vilka mobila kommunikationsutrustningar som har funnits inom ett visst geografiskt område ska det anges vilket geografiskt område tillståndet avser. Begreppet telenät har ersatts med elektroniskt kommunikationsnät, se vidare kommentaren till 18 §

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

Har åklagaren gett ett sådant tillstånd ska han eller hon genast göra en skriftlig anmälan om åtgärden till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva om det finns skäl för åtgärden. Finner rätten att det inte finns sådana skäl, ska den upphäva beslutet.

Har åklagarens beslut verkställts innan rätten gjort en sådan prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Finner rätten att det saknats sådana skäl får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av övervakningen.

Paragrafen, som är ny, innehåller regler om interimistiskt tillstånd till hemlig övervakning av elektronisk kommunikation. Övervägandena finns i avsnitt 6.2.3.

Av *första stycket* framgår att en förutsättning för ett interimistiskt tillstånd är att det kan befaras att inhämtande av rättens tillstånd skulle medföra sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen. I detta ligger att paragrafen ska kunna tillämpas endast i situationer när ändamålet med åtgärden riskerar att gå förlorat om rättens tillstånd skulle avvaktas. Så kan exempelvis vara fallet när en misstänkt person använder sig av ett telefonnummer som inte omfattas av ett tidigare meddelat tillstånd beträffande samma person. Ett annat exempel är att ett beslut om hemlig övervakning av elektronisk kommunikation har meddelats med stöd av 27 kap 20 § andra stycket och har lett till att en person skäligen kan misstänkas för brottet. Syftet med tvångsmedlet har då upphört och beslutet ska upphävas enligt 23 §. Det kan då finnas skäl att omgående fatta beslut om hemlig övervakning av elektronisk kommunikation enligt 20 § första stycket. Möjligheten att fatta interimistiska beslut bör framförallt tillgripas vid de tidpunkter (t.ex. på natten) då det inte är möjligt att få till stånd ett snabbt domstolsbeslut. Interimistiska beslut bör endast undantagsvis komma i fråga vid de tidpunkter en domstolsprövning är möjlig inom domstolarnas ordinarie öppettider eller inom jourdomstolssystemet. Ett interimistiskt tillstånd ges av åklagaren.

Av *andra stycket* framgår att åklagaren skriftligen ska anmäla ett interimistiskt tillstånd till rätten. Anmälan ska göras genast. Det innebär att den ska göras i samband med att beslutet meddelas. I anmälan ska åklagaren ange skälen för åtgärden. Rätten ska skyndsamt pröva om det finns skäl för åtgärden. Finner rätten att det inte finns sådana skäl, ska den upphäva beslutet.

Vid tillstånd till hemlig övervakning som avser inhämtande av historiska övervakningsuppgifter, kan verkställigheten redan ha skett innan rätten har prövat frågan. Av *tredje stycket* framgår att rätten i de fallen ska pröva om det funnits skäl för åtgärden. Rätten ska alltså göra en bedömning av de förutsättningar som förelåg vid åklagarens beslut. Finner rätten att det saknats skäl för åtgärden får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden. Ingenting hindrar dock att rätten fattar ett nytt

beslut om hemlig övervakning av elektronisk kommunikation om det har saknats förutsättningar för inhämtning vid tidpunkten för åklagarens beslut men förhållandena har ändrats så att sådana förutsättningar finns vid rättens prövning. Om rätten ger tillstånd till hemlig övervakning av elektronisk kommunikation avseende de aktuella uppgifterna medför tillståndet att uppgifterna får användas i utredningen, trots att det enligt rättens bedömning inte funnits sådana skäl vid åklagarens beslut. En person kan ha omfattats av åtgärden *dels* genom att han eller hon har utsatts för åtgärden (angående rekvisitet att någon har utsatts för hemlig övervakning av elektronisk kommunikation, se författningskommentaren till 31 § första stycket, prop. 2006/07:133 s. 84 f.), *dels* genom att uppgifter om t.ex. en mobiltelefon som används av honom eller henne har inhämtats vid en basstationstömning (en inhämtning avseende vilka mobila kommunikationsutrustningar som har funnits inom ett visst geografiskt område). Att uppgifterna inte får användas i en brottsutredning avser användning både i en förundersökning och användning i motsvarande utredning enligt 23 kap. 22 §.

22 § Hemlig *avlyssning av elektronisk kommunikation* får *inte* ske av telefonsamtal eller andra *meddelanden* mellan den misstänkte och hans *eller hennes* försvarare. Om det framkommer under avlyssningen att det är fråga om ett sådant samtal eller meddelande, *ska* avlyssningen avbrytas.

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

Paragrafen innehåller ett förbud mot hemlig avlyssning av meddelanden mellan den misstänkte och hans eller hennes försvarare.

I *första stycket* har hemlig teleavlyssning ersatts av det nya begreppet hemlig avlyssning av elektronisk kommunikation. Vidare har begreppet telemeddelanden ersatts av meddelanden, se kommentaren till 18 §.

23 § Om det inte längre finns skäl för ett beslut om hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning, ska åklagaren eller rätten omedelbart häva beslutet.

Paragrafen anger att beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation eller hemlig kameraövervakning omedelbart ska hävas när det inte längre finns skäl för åtgärden.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

23 a § Om det vid hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning 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.

Paragrafen reglerar de brottsbekämpande myndigheternas användning av överskottsinformation.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

24 § En upptagning eller uppteckning som har gjorts vid hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* eller en upptagning som har gjorts vid hemlig kameraövervakning ska granskas snarast möjligt. I fråga om sådan granskning tillämpas 12 § första stycket.

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

Upptagningar från hemlig kameraövervakning som saknar betydelse från brottsutredningssynpunkt ska förstöras omedelbart efter det att de har granskats. I de delar upptagningarna är av betydelse från brottsutredningssynpunkt ska de bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I de delar upptagningarna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott. De ska därefter omedelbart förstöras.

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

Paragrafen reglerar när upptagningar och uppteckningar som har gjorts vid hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation eller hemlig kameraövervakning ska granskas och hur sådana upptagningar och uppteckningar i övrigt ska hanteras.

I *första* och *andra styckena* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

25 § *När tillstånd till hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation har lämnats,* får de tekniska hjälpmedel som behövs för *åtgärden* användas.

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

Paragrafen innehåller bestämmelser som ger den som har fått tillstånd till hemlig avlyssning eller övervakning befogenheter att verkställa åtgärderna och en hänvisning till lagen om elektronisk kommunikation.

Första stycket har omformulerats för att även omfatta interimistiska beslut om tillstånd till hemlig övervakning av elektronisk kommunikation som har getts enligt 21 a §.

Vidare har i såväl *första* som *andra stycket* hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

26 § Offentliga ombud ska bevaka enskildas integritetsintressen i ärenden hos domstol om hemlig *avlyssning av elektronisk kommunikation* och hemlig kameraövervakning.

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

Paragrafen innehåller bestämmelser om offentliga ombud.

I paragrafen har hemlig teleavlyssning ersatts av det nya begreppet hemlig avlyssning av elektronisk kommunikation.

28 § När en ansökan om hemlig *avlyssning av elektronisk kommunikation* eller hemlig kameraövervakning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet ska 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.

Paragrafen innehåller bestämmelser om offentliga ombud.

I *första stycket* har hemlig teleavlyssning ersatts av det nya begreppet hemlig avlyssning av elektronisk kommunikation.

31 § Den som är eller har varit misstänkt för brott ska, om inte annat följer av 33 §, underrättas om hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning som han eller hon har utsatts för. Om *avlyssning* eller *övervakning av elektronisk kommunikation* har avsett *ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning* som innehas av någon annan än den misstänkte, ska, om inte annat följer av 33 § *eller inhämtning har skett med stöd av 20 § andra stycket och integritetsintrånget för den enskilde kan antas vara ringa,* även innehavaren underrättas. Om kameraövervakning har avsett en plats som innehas av någon annan än den misstänkte och som allmänheten inte har tillträde till, ska, om inte annat följer av 33 §, även innehavaren av platsen underrättas.

En underrättelse ska lämnas så snart det kan ske utan men för utredningen, dock senast en månad efter det att förundersökningen avslutades.

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

Paragrafen innehåller bestämmelser om underrättelseskyldighet vid användning av bl.a. hemlig avlyssning och hemlig övervakning av elektronisk kommunikation. Överväganden finns i avsnitt 8.1.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Dessutom har teleadress ersatts med telefonnummer eller annan adress

eller en viss elektronisk kommunikationsutrustning, se kommentaren till 20 §. I stycket har vidare gjorts ett tillägg av innebörd att underrättelse inte ska ske när inhämtning har skett i syfte att utreda vem som är skäligen misstänkt enligt 20 § andra stycket och integritetsintrånget för den enskilde kan antas vara ringa. Så kan vara fallet t.ex. vid en enstaka inhämtning avseende en viss mobiltelefon som enligt vad som framkommit genom en basstationstömning har befunnit sig på en brottplats när ett allvarligt brott har begåtts. Om inhämtningen inte leder till några ytterligare åtgärder kan integritetsintrånget i allmänhet anses vara ringa. Motsvarande gäller om innehavaren av den mobiltelefon som inhämtningen har avsett aldrig har behövt identifieras.

32 § En underrättelse enligt 31 § ska innehålla uppgift om vilket tvångsmedel som har använts och när det har skett. Den som är eller har varit misstänkt för brott ska få uppgift om vilken brottsmisstanke som har legat till grund för åtgärden eller som åtgärden har föranlett. Den som inte är eller har varit misstänkt för brott ska få uppgift om detta.

En underrättelse om hemlig *avlyssning av elektronisk kommunikation eller* hemlig *övervakning av elektronisk kommunikation* ska även innehålla uppgift om *vilket telefonnummer eller annan adress eller vilken elektronisk kommunikationsutrustning* som avlyssningen eller övervakningen har avsett. En underrättelse om hemlig kameraövervakning ska även innehålla uppgift om platsen för åtgärden.

I paragrafen anges vad en underrättelse till enskild om användning av bl.a. hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation ska innehålla.

I *andra stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Vidare har begreppet teleadress ersatts med telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning, se kommentaren till 20 §.

11.5 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 hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning enligt 27 kap. 18, 19 eller 20 a § rättegångsbalken, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, eller hemlig rumsavlyssning enligt lagen (2007:978) om hemlig rumsavlyssning 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 ska göras hos den som har fattat beslutet. Denne ska pröva beslagsfrågan.

Om undersökningsledaren eller åklagaren har meddelat ett beslut med stöd av första stycket, ska det genast anmälas hos rätten. Anmälan ska vara skriftlig och innehålla skälen för beslutet. Rätten ska pröva ärendet snabbt. Anser rätten att beslutet inte bör bestå, ska det upphävas.

Paragrafen innehåller regler som ger åklagare möjlighet att fatta interimistiskt beslut om bl.a. hemlig avlyssning och hemlig övervakning av elektronisk kommunikation vid krig eller krigsfara.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

11.6 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 Säkerhetspolisen eller en polismyndighet tillstånd enligt 27 kap. rättegångsbalken till hemlig *avlyssning av elektronisk kommunikation* eller, om det är tillräckligt, hemlig *övervakning av elektronisk kommunikation*.

Rätten kan för ett sådant ändamål som avses i 19 § första stycket, om det finns synnerliga skäl, även meddela Säkerhetspolisen 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 *eller henne* 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, *ska* hållas kvar till dess den närmare undersökts, öppnats eller granskats. Förordnandet *ska* innehålla underrättelse om att meddelande om åtgärden inte får lämnas till avsändaren, mottagaren eller någon annan, utan tillstånd av den som har begärt åtgärden.

Paragrafen innehåller bl.a. bestämmelser om förutsättningarna för användning av vissa tvångsmedel enligt denna lag.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

21 a § Om det vid hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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

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 innehåller regler om hantering av överskottsinformation vid hemlig avlyssning och övervakning.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

22 § En upptagning eller uppteckning som har gjorts vid hemlig *avlyssning av elektronisk kommunikation* ska granskas snarast möjligt.

Granskningen får utföras endast av rätten, Säkerhetspolisen, en polismyndighet eller en åklagare.

Om upptagningen eller uppteckningen innehåller något som inte är av betydelse för det ändamål som har föranlett avlyssningen, ska 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 ska dock 27 kap. 24 § andra och fjärde styckena rättegångsbalken 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, Säkerhetspolisen, en polismyndighet eller en åklagare. En sådan handling ska undersökas snarast möjligt. När undersökningen har slutförts, ska 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.

Paragrafen innehåller bl.a. bestämmelser om granskning av upptagning eller uppteckning som har gjorts vid hemlig avlyssning av elektronisk kommunikation.

I *första stycket* har hemlig teleavlyssning ersatts av det nya begreppet hemlig avlyssning av elektronisk kommunikation.

11.7 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. hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation*,
7. tekniskt bistånd med hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation*,
8. tillstånd till gränsöverskridande hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation*,
9. hemlig kameraövervakning,
10. hemlig rumsavlyssning,
11. överförande av frihetsberövade för förhör m.m., och
12. 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.

Paragrafen innehåller en uppräkning av de åtgärder som avses med rättslig hjälp enligt lagen.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

4 kap.

25 § En ansökan om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* av någon som befinner sig i Sverige handläggs av åklagare. Av ansökan ska det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd till åtgärden *eller, när så får ske, själv besluta om åtgärden.*

Upptagningar och uppteckningar behöver inte granskas enligt 27 kap. 24 § rättegångsbalken. *Om åklagaren har fattat beslut enligt första stycket, ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om hemlig övervakning av elektronisk kommunikation.* 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.

I fråga om underrättelse till en enskild enligt 27 kap. 31–33 §§ rättegångsbalken ska bestämmelserna i 27 kap. 31 § andra stycket och 33 § andra och tredje styckena samma balk inte tillämpas. Underrättelse ska lämnas så snart det kan ske efter det att åtgärden enligt första stycket har avslutats. Underrättelsen ska, utöver vad som följer av 27 kap. 33 § första stycket rättegångsbalken, skjutas upp om sekretess gäller enligt 18 kap. 17 § offentlighets- och sekretesslagen (2009:400). Om det på grund av sekretess inte har kunnat lämnas någon underrättelse inom ett år från det att åtgärden avslutades, får underrättelsen underlåtas. Underrättelse ska inte lämnas om utredningen gäller brott som motsvarar brott som anges i 27 kap. 33 § tredje stycket rättegångsbalken.

Paragrafen innehåller vissa bestämmelser om handläggningen av en ansökan om rättslig hjälp. Övervägandena finns i avsnitt 6.2.3.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Dessutom har stycket justerats med anledning av åklagares befogenhet att fatta ett interimistiskt beslut om åtgärden enligt 27 kap. 21 § andra stycket rättegångsbalken.

Av ändringen i *andra stycket* framgår att i de fall åklagaren har fattat ett interimistiskt beslut om hemlig övervakning av elektronisk kommunikation, återredovisning till den ansökande staten inte ska ske förrän rätten har godkänt åtgärden.

25 a § Rättens beslut enligt 25 § att tillåta hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* får verkställas genom omedelbar överföring av *meddelanden* eller uppgifter om *meddelanden* 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 och bestämmelserna i 27 kap. 31–33 §§ rättegångsbalken ska inte tillämpas.

Paragrafen behandlar verkställighet av beslut om hemlig avlyssning och övervakning.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

Vidare har begreppet telemeddelande ersatts av begreppet meddelande, se kommentaren till 27 kap. 18 § rättegångsbalken.

25 b § Tekniskt bistånd med hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* i form av omedelbar överföring av meddelanden eller uppgifter om *meddelanden* 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 hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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 *ska* det framgå under vilken tid åtgärden önskas. Ansökan *ska* vidare innehålla sådana uppgifter som behövs för att åtgärden *ska* kunna genomföras. Om den person som ansökan avser inte befinner sig i den ansökande staten, *ska* det också framgå av ansökan att ett sådant tillstånd som avses i 26 a § har lämnats av den stat där personen finns.

Ansökan *ska* prövas av åklagare. För beslutet om tekniskt bistånd tillämpas bestämmelserna i 27 kap. 18 § första *och tredje styckena*, 19 § första stycket, 20 § *tredje* stycket, 21 § andra och tredje styckena samt 23 § rättegångsbalken.

Om omedelbar överföring av *meddelanden* sker, får upptagning eller uppteckning inte göras i Sverige.

Paragrafen innehåller regler om tekniskt bistånd i Sverige med hemlig avlyssning eller övervakning.

I *första och andra styckena* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Vidare har begreppet telemeddelande ersatts av begreppet meddelande, se kommentaren till 27 kap. 18 § rättegångsbalken.

I *fjärde stycket* har hänvisningarna till rättegångsbalkens bestämmelser om förutsättningarna för åtgärderna justerats med anledning av förslaget att ett tillstånd till hemlig avlyssning av elektronisk kommunikation även ska ge möjlighet att inhämta övervakningsuppgifter (27 kap. 18 § tredje stycket rättegångsbalken). En redaktionell ändring har gjorts till följd av att bestämmelsen i tidigare 27 kap. 20 § andra stycket rättegångsbalken nu återfinns i 27 kap. 20 § tredje stycket rättegångsbalken.

I *femte stycket* har begreppet telemeddelande ersatts av begreppet meddelande.

25 c § Om en stat har begärt tekniskt bistånd enligt 25 b § men omedelbar överföring inte kan ske, *ska* åklagaren ge den ansökande staten tillfälle att få ansökan behandlad som en ansökan enligt 25 §. Prövningen av rättslig hjälp med hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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, *ska* det av ansökan framgå att ett sådant tillstånd som avses i 26 a § har lämnats av den stat där personen finns.

Paragrafen innehåller bestämmelser om prövningen av en begäran av tekniskt bistånd när omedelbar överföring inte kan ske.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

26 § Åklagare får ansöka hos en utländsk myndighet om rättslig hjälp eller tekniskt bistånd med hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* av någon som befinner sig i en annan stat eller i Sverige.

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

Av ansökan enligt första stycket ska det framgå under vilken tid åtgärden önskas och sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Om den andra staten kräver ett tillstånd enligt andra stycket, ska 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, ska det av ansökan framgå att ett sådant tillstånd som avses i 26 c § har lämnats av den stat där personen finns.

Om tillstånd lämnas enligt andra stycket, ska bestämmelserna om underrättelse till enskild i 27 kap. 31–33 §§ rättegångsbalken tillämpas endast när upptagning eller uppteckning av avlyssningen eller övervakningen sker i Sverige.

Paragrafen innehåller bestämmelser om rättslig hjälp och tekniskt bistånd i utlandet med hemlig avlyssning och övervakning.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

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 *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* av någon som befinner sig i Sverige. Ansökan handläggs av åklagare. Av ansökan *ska* det framgå under vilken tid åtgärden beräknas pågå. Ansökan *ska* också innehålla en bekräftelse på att ett beslut om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* har meddelats i den ansökande staten.

Åklagaren *ska* genast pröva om det finns förutsättningar för hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* och, om så är fallet, ansöka om rättens tillstånd till åtgärden.

De förutsättningar som gäller enligt 27 kap. *18–20, 21 och 22 §§* rättegångsbalken *ska* tillämpas vid tillståndsprövningen. Rätten *ska* även tillämpa motsvarande förfarande som anges i 27 kap. 26 och 28–30 §§ samma balk. Tingsrättens beslut får inte överklagas.

Paragrafen innehåller bestämmelser om tillstånd i Sverige till hemlig avlyssning eller hemlig övervakning efter ansökan av annan stat.

I *första och andra styckena* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

Enligt *tredje stycket* ska de förutsättningar som gäller enligt rättegångsbalken tillämpas vid tillståndprövningen. Bestämmelserna i 27

kap. 21 a § rättegångsbalken om interimistisk beslutanderätt för åklagaren är inte tillämpliga, eftersom ansökan i nu aktuella fall ska prövas av rätten.

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

Åklagaren *ska* genast underrätta den ansökande staten när ett beslut enligt 26 a § har meddelats. Om tillstånd vägras, *ska* underrättelsen ange att *avlyssningen* eller *övervakningen* inte får ske eller omedelbart *ska* upphöra. I sådant fall *ska* 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.

Paragrafen innehåller regler om när ett beslut enligt 26 a § ska meddelas och om underrättelser till ansökande stat när ett tillstånd enligt 26 a § har vägrats.

I *andra stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

26 c § Har beslut om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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* eller uppgifter om *meddelanden* som överförs 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 tillstånd till åtgärden.

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

Om beslut om hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* 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, *ska* 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 *ska* fortsätta i den andra staten, *ska* 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.

Paragrafen innehåller bestämmelser om tillstånd från en annan stat till gränsöverskridande hemlig avlyssning eller övervakning.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

11.8 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 hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation*, tekniskt bistånd med *sådan avlyssning eller övervakning, inhämtning av uppgifter enligt lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,* eller
3. i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

Paragrafen reglerar undantag från operatörernas skyldighet att utplåna och avidentifiera trafikuppgifter när de inte längre behövs för att överföra ett elektroniskt meddelande.

I *punkten 2* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Vidare har undantaget utvidgats till att även omfatta inhämtning av uppgifter enligt den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

10 a § *Lokaliseringsuppgifter som omfattas av beslut om inhämtning av uppgifter enligt 27 kap. rättegångsbalken eller lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, får behandlas utan hinder av bestämmelserna i 9-10 §§.*

Paragrafen, som är ny, behandlar vissa undantag från lagens regler om behandling av lokaliseringsuppgifter som inte är trafikuppgifter.

I 9 och 10 §§ finns bestämmelser om hur operatörer får behandla lokaliseringsuppgifter som inte är trafikuppgifter, exempelvis uppgifter som avser en enbart påslagen mobiltelefon. Uppgifter som rör fysiska personer eller abonnenter får behandlas endast sedan de har avidentifierats eller abonnenten har gett sitt samtycke till behandlingen. Det finns också begränsningar i fråga om vilka personer som får ta befattning med uppgifterna. Paragrafen föreskriver undantag från de angivna bestämmelserna när sådana uppgifter omfattas av beslut om inhämtning enligt 27 kap. rättegångsbalken eller enligt den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

16 c § Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2, 27 kap. 19 § rättegångsbalken *eller lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.*

Paragrafen reglerar för vilka ändamål uppgifter som har lagrats med stöd av 16 a § får behandlas.

Genom ändringen ersätts möjligheten att behandla lagrade uppgifter för att kunna lämnas ut enligt 22 § första stycket 3 (som har fått ett nytt innehåll) med en möjlighet att behandla uppgifterna för att kunna lämnas ut enligt den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

19 § En verksamhet *ska* bedrivas så att beslut om hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation* 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 *meddelanden ska* göras tillgängliga så att informationen enkelt kan tas om hand.

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.

Paragrafen innehåller regler om anpassningsskyldighet för operatörer.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

I *andra stycket* har begreppet telemeddelande ersatts av begreppet meddelande, se kommentaren till 27 kap. 18 § rättegångsbalken.

Definitionen av telemeddelande i nuvarande tredje stycket har tagits bort.

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

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

Paragrafen innehåller regler om tystnadsplikt för operatörer. Övervägandena finns i avsnitt 8.4.

I *punkten 2* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

Enligt *punkterna 4 och 5,* som är nya, ska även inhämtning enligt den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet liksom uppgifter som hänför sig till en begäran från myndigheterna att få tillgång till uppgifter om abonnemang omfattas av regleringen.

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

1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (2010:000), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,
2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet,
3. uppgift som avses i 20 § första stycket *1 och* 3 *samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits 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 Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,
5. uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),
6. uppgift som avses i 20 § första stycket 1 till polismyndighet, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten ska 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 ska kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och
8. uppgift som avses i 20 § första stycket 1 och 3 till regional alarmeringscentral som avses i lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler.

Ersättning för att lämna ut uppgifter enligt första stycket 8 ska vara skälig med hänsyn till kostnaderna för utlämnandet.

Paragrafen innehåller bestämmelser om operatörers skyldighet att på begäran lämna ut vissa uppgifter utan hinder av tystnadsplikt. Övervägandena finns i avsnitten 6.1, 7.2 och 7.3.

Första stycket 2 reglerar de brottsbekämpande myndigheternas tillgång till uppgifter om abonnemang vid misstanke om brott. De tidigare kraven att fängelse ska vara föreskrivet för brottet i fråga och att det enligt myndighetens bedömning kan föranleda annan påföljd än böter har tagits bort. Det innebär att de brottsbekämpande myndigheterna kan få ut

abonnemangsuppgifter även när det gäller misstanke om brott för vilket endast är föreskrivet böter eller som bedöms föranleda böter.

Första stycket 3 innehöll tidigare bestämmelser om operatörers skyldighet att lämna ut uppgifter som angår ett särskilt elektroniskt meddelande (20 § första stycket 3) till de brottsbekämpande myndigheterna, när det gällde misstanke om brott med ett minimistraff om två års fängelse. Dessa bestämmelser har tagits bort. De brottsbekämpande myndigheternas tillgång till sådana uppgifter regleras nu dels i 27 kap. rättegångsbalken, dels i den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. I punkten 3 har tagits in bestämmelser om polisens tillgång till vissa uppgifter om elektronisk kommunikation för att efterforska personer som har försvunnit under sådana omständigheter att det kan befaras föreligga fara för deras liv eller allvarlig risk för deras hälsa. Att polismyndigheterna ska svara för efterforskningen av försvunna personer i sådana fall framgår av förordningen (2003:789) om skydd mot olyckor. De uppgifter som får lämnas ut är abonnemangsuppgifter (20 § första stycket 1), uppgifter om ett särskilt elektroniskt meddelande (20 § första stycket 3) och uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

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 i ett elektroniskt kommunikationsnät* och som inte är avsett för honom eller henne själv eller för allmänheten får inte obehörigen föra det vidare.

Paragrafen innehåller regler om tystnadsplikt för den som i annat fall än som angetts i 20 och 21 §§ har avlyssnat eller på annat sätt fått tillgång till ett radiobefordrat meddelande.

I paragrafen har begreppet telemeddelande ersatts av begreppet meddelande i ett elektroniskt kommunikationsnät, se kommentaren till 27 kap. 19 § rättegångsbalken.

11.9 Förslaget till lag om ändring i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott

1 § Tillstånd till hemlig *avlyssning av elektronisk kommunikation* enligt 27 kap. 18 § första stycket rättegångsbalken, hemlig *övervakning av elektronisk kommunikation* enligt 27 kap. 19 § första stycket rättegångsbalken eller hemlig kameraövervakning enligt 27 kap. 20 a § första stycket rättegångsbalken får meddelas, om det med hänsyn till omständigheterna finns särskild anledning att anta att en person kommer att utöva brottslig verksamhet som innefattar

1. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,
2. mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,

4. högförräderi, krigsanstiftan, spionerі, grovt spionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet enligt 19 kap. 1, 2, 5, 6 eller 8 § eller 10 § tredje stycket brottsbalken,

5. terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet, eller

6. mord, dråp, grov misshandel, människorov eller olaga frihetsberövande enligt 3 kap. 1, 2 eller 6 § eller 4 kap. 1 § eller 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

Paragrafen innehåller vissa av de förutsättningarna som ställs upp för att tillstånd till tvångsmedelanvändning enligt lagen ska få meddelas.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

2 § Hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation* enligt 1 § får endast avse

1. *ett telefonnummer eller annan adress eller en elektronisk kommunikationsutrustning* som under den tid tillståndet avser innehas eller har innehafts av den som avses i 1 § eller annars kan antas ha använts eller komma att användas av honom eller henne, eller

2. *ett telefonnummer eller annan adress eller en elektronisk kommunikationsutrustning* som det finns synnerlig anledning att anta att den som avses i 1 § under den tid tillståndet avser har kontaktat eller kommer att kontakta.

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

Paragrafen reglerar den närmare avgränsningen av vad som får avlyssnas eller övervakas.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Teleadress har ersatts av telefonnummer eller annan adress eller elektronisk kommunikationsutrustning, se kommentaren till 27 kap. 20 § rättegångsbalken.

I *andra stycket* har telemeddelande ersatts med meddelande och telenät med elektroniskt kommunikationsnät, se kommentaren till 27 kap. 18 § rättegångsbalken.

8 § I ett beslut om tillstånd till tvångsmedel ska det anges

1. vilket eller vilka tvångsmedel som får användas,

2. vilken eller vilka av punkterna i 1 § 1–6 som ligger till grund för tillståndet, och

3. under vilken tid tillståndet gäller.

I ett beslut om tillstånd till hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* ska det, förutom de uppgifter som framgår av första stycket, anges

1. *vilket telefonnummer eller annan adress eller vilken elektronisk kommunikationsutrustning* tillståndet avser, och

2. om åtgärden får verkställas utanför allmänt tillgängliga *elektroniska kommunikationsnät.*

I ett beslut om tillstånd till hemlig kameraövervakning ska, förutom de uppgifter som framgår av första stycket, den plats anges som tillståndet avser.

Paragrafen reglerar vad ett tillståndsbeslut ska innehålla.

I *andra stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Teleadress har ersatts av telefonnummer eller annan adress eller elektronisk kommunikationsutrustning och telenät med elektroniska kommunikationsnät, se kommentaren till 27 kap. 18 och 20 §§ rättegångsbalken.

9 § Vid hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation* får de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen användas.

Paragrafen innehåller bestämmelser som ger den som har tillstånd till hemlig avlyssning eller hemlig övervakning befogenheter att kunna verkställa åtgärderna.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

11 § *Hemlig avlyssning av elektronisk kommunikation* får inte ske av telefonsamtal eller andra *meddelanden* där den som yttrar sig inte skulle ha kunnat höras som vittne, enligt 36 kap. 5 § andra–sjätte styckena rättegångsbalken, om det som har sagts eller på annat sätt framkommit. Om det av avlyssningen framgår att det är fråga om ett sådant samtal eller meddelande, ska avlyssningen omedelbart avbrytas.

Upptagningar och uppteckningar från en hemlig *avlyssning av elektronisk kommunikation* ska, i den utsträckning de omfattas av förbudet, omedelbart förstöras.

Paragrafen innehåller bestämmelser som förbjuder hemlig avlyssning av samtal där den som yttrar sig inte skulle ha kunnat höras som vittne enligt 36 kap. 5 § andra–sjätte styckena rättegångsbalken, om det som har sagts eller på annat sätt framkommit.

I paragrafen har hemlig teleavlyssning ersatts av det nya begreppet hemlig avlyssning av elektronisk kommunikation. Telemeddelande har ersatts med meddelande, se kommentaren till 27 kap. 18 § rättegångsbalken.

13 § En upptagning eller uppteckning som har gjorts vid hemlig *avlyssning av elektronisk kommunikation* eller hemlig *övervakning av elektronisk kommunikation* ska granskas snarast möjligt. Detsamma gäller en upptagning som har gjorts vid hemlig kameraövervakning. Granskningen får utföras endast av rätten, en åklagare, Rikspolisstyrelsen, Säkerhetspolisen eller en polismyndighet. Efter anvisning av rätten, en åklagare eller någon av de nämnda myndigheterna får granskningen utföras även av en sakkunnig eller någon annan som har anlitats i ärendet.

Upptagningar och uppteckningar ska, i de delar de är av betydelse för att förhindra förestående brott, bevaras så länge det behövs för att förhindra brott. I de delar upptagningarna och uppteckningarna innehåller

sådana uppgifter om brott som enligt 12 § får användas för att utreda brott ska de bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. De ska därefter förstöras.

Trots vad som sägs i andra stycket får brottsutredande myndigheter behandla uppgifter från upptagningar och uppteckningar som rör förestående brott eller uppgifter om brott som enligt 12 § får användas för att utreda brott i enlighet med vad som är särskilt föreskrivet i lag.

Paragrafen reglerar de brottsbekämpande myndigheternas hantering av uppgifter som har framkommit vid användning av hemliga tvångsmedel enligt lagen.

I *första stycket* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

16 § Den som har varit utsatt för en åtgärd enligt 1 § 6 ska underrättas om åtgärden. Om åtgärden har avsett *ett telefonnummer eller annan adress, en elektronisk kommunikationsutrustning* eller en plats som innehas av någon annan, ska även denne underrättas. Vid hemlig kameraövervakning behöver dock innehavaren av en sådan plats till vilken allmänheten har tillträde inte underrättas.

Underrättelsen ska lämnas så snart det kan ske efter det att det ärende i vilket åtgärden vidtogs avslutades.

En underrättelse behöver inte lämnas till den som redan har fått del av eller tillgång till uppgifterna. En underrättelse behöver inte heller lämnas om den med hänsyn till omständigheterna uppenbart är utan betydelse.

Paragrafen reglerar när det finns en skyldighet att underrätta enskild om att han eller hon har varit utsatt för en åtgärd enligt 1 § 6.

I första stycket har teleadress ersatts med telefonnummer eller annan adress eller elektronisk kommunikationsutrustning, se kommentaren till 27 kap. 20 § rättegångsbalken.

17 § En underrättelse enligt 16 § ska innehålla uppgift om vilket tvångsmedel som har använts och uppgift om tiden för åtgärden. Vid hemlig *avlyssning av elektronisk kommunikation* och hemlig *övervakning av elektronisk kommunikation* ska underrättelsen även innehålla uppgift om *vilket telefonnummer eller annan adress eller vilken elektronisk kommunikationsutrustning* som åtgärden har avsett. Vid hemlig kameraövervakning ska underrättelsen även innehålla uppgift om platsen för åtgärden. Den som har varit utsatt för en åtgärd enligt 1 § 6 ska få uppgift om vilken misstanke som har legat till grund för åtgärden. Den som inte är eller har varit misstänkt ska få uppgift om detta.

Paragrafen reglerar innehållet i en underrättelse enligt 16 §.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Teleadress har ersatts med telefonnummer eller annan adress eller elektronisk kommunikationsutrustning, se kommentaren till 27 kap. 20 § rättegångsbalken.

11.10 Förslaget till lag om ändring i lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott

3 § Tillstånd enligt 27 kap. rättegångsbalken till hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning får meddelas även om brottet inte omfattas av de krav som ställs upp i 27 kap. 18 § andra stycket, 19 § *tredje* stycket, eller 20 a § andra stycket rättegångsbalken.

Paragrafen innehåller bestämmelser om utvidgade möjligheter att använda vissa tvångsmedel.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. En redaktionell ändring har gjorts till följd av att bestämmelsen i tidigare 27 kap. 19 § andra stycket rättegångsbalken nu återfinns i 27 kap. 19 § tredje stycket.

4 § Om det kan befaras att inhämtande av rättens tillstånd till hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation* eller hemlig kameraövervakning skulle medföra en sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får tillstånd till åtgärden ges av åklagaren.

Paragrafen reglerar åklagares möjlighet att fatta interimistiska beslut.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

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

10 kap.

23 § Om inte annat följer av 19–22 §§ får en uppgift som angår misstanke om ett begånget brott och som är sekretessbelagd enligt 24 kap. 8 §, 25 kap. 1 §, 2 § andra stycket eller 3–8 §§, 26 kap. 1–6 §§, 29 kap. 1 §, 31 kap. 1 § första stycket, 2 eller 12 §, 33 kap. 2 §, 36 kap. 3 § eller 40 kap. 2 eller 5 § lämnas till en åklagarmyndighet, polismyndighet eller någon annan myndighet som har till uppgift att ingripa mot brottet endast om misstanken angår

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i ett år,
2. försök till brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, eller
3. försök till brott för vilket det inte är föreskrivet lindrigare straff än fängelse i ett år, om gärningen innefattat försök till överföring av sådan allmänfarlig sjukdom som avses i 1 kap. 3 § smittskyddslagen (2004:168).

I paragrafen finns bestämmelser om brytande av sekretess vid misstanke om vissa brott. Övervägandena finns i avsnitt 6.1.

Ändringen innebär att en myndighet som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst inte längre med stöd av denna bestämmelse får

lämna ut uppgifter om meddelanden som angår misstanke om brott till de brottsbekämpande myndigheterna. Utlämnande ska i fortsättningen endast kunna ske med stöd av rättegångsbalken eller den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i underrättelseskedet.

26 § Sekretess hindrar inte att en uppgift om en enskilds adress, telefonnummer och arbetsplats eller uppgift i form av fotografisk bild av en enskild lämnas till en myndighet, om uppgiften behövs där för delgivning enligt delgivningslagen (2010:000).

Om den enskilde hos en myndighet som *tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst* har begärt att abonnemanget ska hållas hemligt och om uppgiften är sekretessbelagd enligt 29 kap. 3 §, får den 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.

I paragrafen finns bestämmelser om brytande av sekretess om en viss uppgift behövs för delgivning.

Televerksamhet i *andra stycket* har bytts ut mot tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Begreppen är desamma som i lagen om elektronisk kommunikation och är avsedda att ha samma innebörd här.

18 kap.

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

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig *avlyssning av elektronisk kommunikation,* hemlig *övervakning av elektronisk kommunikation*, hemlig kameraövervakning eller hemlig rumsavlyssning på grund av beslut av domstol, undersökningsledare eller åklagare *eller inhämtning av uppgifter enligt lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.*

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

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

I paragrafen regleras vilka tystnadsplikter som har företräde framför rätten att meddela och offentliggöra uppgifter.

I *andra och tredje styckena* har hemlig teleavlyssning och hemlig teleövervakning ersatts av de nya begreppen hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Vidare har andra stycket ändrats så att uppgifter som inhämtats enligt den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet omfattas av begränsningar i rätten att meddela

och offentliggöra uppgifter. Motsvarande ordning gäller redan för bl.a. uppgifter som inhämtas genom hemlig övervakning respektive avlyssning av elektronisk kommunikation.

29 kap.

2 § Sekretess gäller hos en myndighet som *tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst för uppgift om 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 elektronisk meddelande eller som på något annat sätt har sänt eller tagit emot ett sådant meddelande. Detsamma gäller innehavaren av ett abonnemang som använts för ett elektronisk meddelande när det är fråga om uppgift om något annat än innehållet i meddelandet.*

Paragrafen innehåller bestämmelser om sekretess hos myndighet som bedriver televerksamhet. Övervägandena finns i avsnitten 5.2 och 6.1.

Televerksamhet har bytts ut mot tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Vidare har telefonsamtal eller annat telemeddelande ersatts med elektroniskt meddelande. Begreppen är desamma som i lagen om elektronisk kommunikation och är avsedda att ha samma innebörd här (se definitionerna i 1 kap. 7 § och 6 kap. 1 § lagen om elektronisk kommunikation). Bestämmelsen har justerats för att bättre stämma överens med reglerna i 6 kap. 20 § andra och tredje stycket lagen om elektronisk kommunikation som innehåller motsvarande regler om tystnadsplikt när verksamheten inte bedrivs av en myndighet. Bestämmelsen i 6 kap. 20 § lagen om elektronisk kommunikation har, efter anpassning av terminologin, ersatt 45 § telelagen (1993:597) (prop. 2002/03:110 s. 397). Av förarbetena till den bestämmelsen framgår att med andra uppgifter som avser ett särskilt [tele]meddelande, t.ex. avses mellan vilka abonnemang som ett telefonsamtal har förmedlats. Att tystnadsplikten såvitt avser andra uppgifter än uppgifter om innehållet i ett meddelande inte gäller i förhållande till innehavaren av ett abonnemang som har använts för ett elektroniskt meddelande innebär enligt samma proposition att en betalningsansvarig abonnent har möjlighet att få uppgifter om t.ex. utväxlade telefonsamtal som debiteras honom (prop. 1992/93:200 s. 310).

38 kap.

5 § Sekretess gäller för uppgift vid särskild sambandstjänst inom totalförsvaret, om uppgiften avser *ett elektroniskt meddelande* som utomstående utväxlar *i ett elektroniskt kommunikationsnät*.

Paragrafen innehåller regler om sekretess för uppgifter vid särskild sambandstjänst inom totalförsvaret. Övervägandena finns i avsnitten 5.2 och 5.3.

Begreppen telemeddelande och telenät har bytts ut mot elektroniskt meddelande och elektroniskt kommunikationsnät.

44 kap.

4 § Rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer av

1. 2 kap. 14 § första stycket 1 och 3 postlagen (2010:1045),
2. 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation, när det är fråga om uppgift om innehållet i ett elektroniskt meddelande eller som annars rör ett särskilt sådant meddelande, och
3. 6 kap. 21 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig *avlyssning av elektronisk kommunikation eller* hemlig *övervakning av elektronisk kommunikation* på grund av beslut av domstol, undersökningsledare eller åklagare *eller om inhämtning av uppgifter enligt lagen (0000:00) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.*

Paragrafen behandlar postlagen och lagen om elektronisk kommunikation. Övervägandena finns i avsnitt 8.4.

I paragrafen har hemlig teleavlyssning och hemlig teleövervakning ersatts av hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. Vidare har paragrafen ändrats så att uppgifter som inhämtats enligt den föreslagna lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet och som omfattas av tystnadsplikt enligt 6 kap. 21 § lagen om elektronisk kommunikation omfattas av begränsningar i rätten att meddela och offentliggöra uppgifter.

Sammanfattning av betänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38)

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 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.

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 bestämmelserna 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 särskilt förslaget om övervakning även utan misstänkt gärningsman).

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 utredningar 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.

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 integritetsfråga 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 anledning 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 omfattas 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 väsentligt 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 De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation 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 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.

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 brottsutredande 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 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.

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 ITrelaterade 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 liknandetillvägagångssätt 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 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 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.

Författningsförslaget i betänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38)

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, hemlig teleavlyssning 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*	Uppgifter *får efter tillstånd* i hemlighet hämtas in om *meddelanden* som befordras eller har befordrats *med tekniskt hjälpmedel till eller från ett*

att sådana meddelanden hindras från att nå fram.	*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* avse	*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. *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	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. *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.	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 *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.	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* prövas av rätten på ansökan av åklagaren.	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 *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 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 *telenät*.	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 teleavlyssning* eller *hemlig teleövervakning*, skall åklagaren eller rätten omedelbart häva beslutet.

Om det inte längre finns skäl för ett beslut om *avlyssning* eller *övervakning enligt 18 respektive 19 §,* skall åklagaren eller rätten omedelbart häva beslutet.

23 a §[32]

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 §[33]

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

[32] Nuvarande lydelse enligt förslag i prop. 2004/05:143
[33] Nuvarande lydelse enligt förslag i prop. 2004/05:143

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.

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.

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 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.

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 *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*.
Tillstånd till hemlig kameraövervakning får meddelas enligt lagen (1995:1506) om hemlig kameraövervakning, även om brottet inte omfattas av 2 § 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 telemeddelande*. 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.*

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 *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

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

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.

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.

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 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 uppgift 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

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

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

tillämpas.

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.

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***

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

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

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.	
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 §	
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 ansökande 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.

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 *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 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 *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.	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 *hemlig teleavlyssning* eller *hemlig teleövervakning* och, om så är fallet, ansöka om rättens tillstånd till åtgärden.	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	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

eller hämtats in inte får användas eller att det endast får användas på de villkor som åklagaren ställer.	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	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	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.	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.	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 *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	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

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 tillståndet.

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

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

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

på begäran av svensk åklagare besluta att tillåta kameraövervakningen.	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 verkställas och så att verkställandet inte röjs.*
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	

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

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.

Innehållet i och uppgifter om avlyssnade eller övervakade *meddelanden* 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.

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

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

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

25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål.	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 någon annan myndighet som skall ingripa mot brottet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år,*	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),	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	Den som i verksamhet som anges i 19 § första stycket lämnar ut innehållet i och uppgifter om avlyssnade eller övervakade

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

telemeddelanden har inte rätt till ersättning.	*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.

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 domstolar	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

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.

Förteckning över remissinstanserna (SOU 2005:38)

Remissvar har inkommit från Riksdagens ombudsmän (JO), Göta hovrätt, Hovrätten för Västra Sverige, Stockholms tingsrätt, Nacka tingsrätt, Skövde tingsrätt, Malmö tingsrätt, Göteborgs tingsrätt, Sundsvalls tingsrätt, Kammarrätten i Stockholm, Länsrätten i Skåne län, Länsrätten i Östergötlands län, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Kriminalvårdsstyrelsen, Säkerhetspolisen, Brottsförebyggande rådet, Brottsoffermyndigheten, Datainspektionen, Försvarsmakten, Försvarets radioanstalt, Krisberedskapsmyndigheten, Försvarets underrättelsenämnd, Kustbevakningen, Tullverket, Skatteverket, Statskontoret, Post- och telestyrelsen, Juridiska fakultetsnämnden vid Stockholms universitet, Juridiska fakultetsstyrelsen vid Lunds universitet, Sveriges advokatsamfund, Sveriges domareförbund, Svenska polisförbundet, Svenska journalistförbundet, Amnesty International, Svenska avdelningen av Internationella juristkommissionen, Svenska Helsingforskommittén för Mänskliga rättigheter, Sveriges kommuner och landsting, Svenska Stadsnätsföreningen, Svenska IT-företagens Organisation, Bahnhof AB, B2 Bredband AB, Comhem AB, Hi3G Access AB, Tele2 Sverige AB, Telenor AB, TeliaSonera Sverige AB, Vodafone Sverige AB, Stiftelsen för Internetinfrastruktur, Stockholms handelskammare, Filmproducenternas Rättighetsförening, Föreningen Konstnärliga och Litterära Yrkesutövares Samarbetsnämnd (KLYS), IFPI svenska gruppen, Svenska Antipiratbyrån, Svenska Artisters och Musikers Intresseorganisation (SAMI), Svenska Tonsättares Internationella Musikbyrå (STIM).

Försvarets underrättelsenämnd har meddelat att nämnden inte har några synpunkter att lämna.

STIM och KLYS har meddelat att man avstår från att yttra sig.

Svenska Helsingforskommittén för Mänskliga rättigheter, B2 Bredband AB, Comhem AB, Hi3G Access AB och Telenor AB har inte kommit in med yttrande.

Polismetodutredningens sammanfattning av delbetänkandet (SOU 2009:1)

Bakgrund

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

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

1. Det ska finnas en skäligen misstänkt person.
2. Misstanken ska röra
   a) brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader (även anstiftan och medhjälp),
   b) dataintrång, barnpornografibrott som inte är ringa, narkotikabrott eller narkotikasmuggling, eller
   c) försök, förberedelse eller stämpling till brott under a) och b).
3. Åtgärden ska vara av synnerlig vikt för utredningen.
4. Åtgärden ska avse uppgifter om telemeddelanden som befordras eller har befordrats till eller från teleadresser med viss anknytning till den misstänkte.
5. Åtgärden ska beslutas av domstol.

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

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

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

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

Det saknas statistik över antalet fall där de brottsbekämpande myndigheterna begär ut uppgifter med stöd av lagen om elektronisk kommunikation. Polisen har gjort beräkningar över antalet fall där man har begärt att få ut uppgifter enligt 6 kap. 22 § första stycket 3 LEK under år 2007 och uppskattat det till ca 9 500. Den siffran omfattar inte Säkerhetspolisens och Tullverkets ärenden. Mot bakgrund av kravet i lagen om elektronisk kommunikation på att det ska vara fråga om misstanke om brott med ett straffminimum på två års fängelse, står det klart att utredningarna enbart rör allvarlig brottslighet och att myndigheterna många gånger har begärt uppgifter vid flera tillfällen i samma utredning. En anledning till det relativt stora antalet beslut är att det inledningsvis i många förundersökningar rörande grova brott saknas en skäligen misstänkt person och därmed finns det inte heller möjlighet att använda sig av hemlig teleövervakning enligt rättegångsbalken. En hjälp i arbetet med att identifiera misstänkta personer är att inhämta uppgifter om elektronisk kommunikation på och i närheten av en brottsplats, längs flyktvägar och liknande. En annan anledning till det relativt stora antalet beslut är användningen vid brottslighet av mobiltelefoner med anonyma kontantkort, där myndigheterna många gånger behöver inhämta uppgifter flera gånger i syfte att identifiera den som använder ett visst abonnemang.

Uppdraget som redovisas i detta betänkande

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

Regeringen konstaterar i direktiven till den här utredningen att det finns ett operativt behov av att få tillgång till uppgifter om elektronisk kommunikation för att kartlägga brottslig verksamhet och i övrigt arbeta brottsförebyggande. Regeringen anger att såväl tekniken kring elektronisk kommunikation som polisens och tullens underrättelseverksamhet har genomgått stora förändringar under senare

år och att det mot den bakgrunden kan ifrågasättas om bestämmelsen i 6 kap. 22 § första stycket 3 LEK är ändamålsenligt utformad.

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

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

En allmän utgångspunkt

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

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

Tydliga och rättssäkra befogenheter för utfående av uppgifter om elektronisk kommunikation

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

Regleringen i lagen om elektronisk kommunikation uppfyller inte i tillräcklig grad de krav på rättssäkerhet och integritetsskydd som måste finnas vid det här slaget av integritetskänsliga åtgärder. Den ska därför upphävas.

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

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

Hemlig teleövervakning i förundersökningar

När ska inhämtning få ske?

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

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

Vem ska fatta beslut?

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

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

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

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

Tillgång till uppgifter om elektronisk kommunikation i underrättelseverksamhet

När ska inhämtning få ske?

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

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

Såsom vid andra tvångsmedel ska inhämtning få beslutas och genomföras endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Vem ska fatta beslut?

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

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

delegera beslutanderätten. Det ska få ske till annan person på ledningsnivå.

I vilken omfattning ska uppgifterna få användas?

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

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

Tillgång till lokaliseringsuppgifter

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

Inhämtning av uppgifter om abonnemang

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

Överprövning

En domstols beslut om hemlig teleövervakning kan överklagas. När undersökningsledaren eller åklagaren har fattat beslut om en sådan åtgärd ska den som innehar den teleadress som övervakningen avser kunna begära rättens prövning av beslutet. Däremot ska beslut av den

brottsbekämpande myndigheten om inhämtning av uppgifter i underrättelseverksamhet inte på motsvarande sätt kunna bli före mål för rättens prövning. I stället bör det för de fallen finnas andra rättssäkerhetsgarantier, bl.a. i form av en kontinuerlig och effektiv tillsyn av Säkerhets och integritetsskyddsnämnden.

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

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

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

Särskild tillsyn av Säkerhets och integritetsskyddsnämnden

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

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

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

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

Regeringens redovisning till riksdagen

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

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

Sekretess och tystnadsplikt

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

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

Ikraftträdande

Förslagen ska träda i kraft den 1 januari 2010.

Författningsförslaget i betänkandet En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen (SOU 2009:1)

1. Förslag till lag om ändring i rättegångsbalken

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

Nuvarande lydelse	*Föreslagen lydelse*
27 kap.	
19 §[34]	
Hemlig teleövervakning innebär att uppgifter i hemlighet hämtas in om telemeddelanden som befordras eller har befordrats till eller från en viss teleadress eller att sådana meddelanden hindras från att nå fram.	Hemlig teleövervakning innebär att uppgifter i hemlighet hämtas in om telemeddelanden som befordras eller har befordrats till eller från en viss teleadress eller att sådana meddelanden hindras från att nå fram. *Vad som sägs om hemlig teleövervakning ska även gälla inhämtning i hemlighet av lokaliseringsuppgifter. Med sådana uppgifter avses* *1. uppgifter om vilka mobila elektroniska kommunikationsutrustningar som har funnits inom ett visst avgränsat geografiskt område, eller* *2. uppgifter om i vilket avgränsat geografiskt område en viss mobil elektronisk kommunikationsutrustning finns eller har funnits.*

Hemlig teleövervakning får användas vid förundersökning angående
1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader,
2. brott enligt 4 kap. 9 c § brottsbalken, brott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, brott enligt 1 § narkotikastrafflagen (1968:64), brott enligt 6 § första stycket lagen (2000:1225) om straff för smuggling, eller

[34] Senaste lydelse 2003:1146.

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

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

20 §[35]

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

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

1. en teleadress som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte, eller

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

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

20 d §

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

21 §[36]

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

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

[35] Senaste lydelse 2003:1146.
[36] Senaste lydelse 2008:855.

kan antas bli av stor omfattning eller av särskilt ingripande slag, får frågor enligt 20 d § även prövas av undersökningsledaren eller åklagaren.

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

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

I ett tillstånd till hemlig teleavlyssning eller hemlig teleövervakning ska det anges vilken teleadress som tillståndet avser. Det ska vidare särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga telenät. *I ett beslut att tillåta inhämtning av lokaliseringsuppgifter ska det anges vilken teleadress eller vilket avgränsat geografiskt område tillståndet avser.*

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

21 a §

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

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

21 b §

Har hemlig teleövervakning avseende en viss teleadress beslu-

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

23 §[37]

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

33 §[38]

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

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

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

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

En underrättelse enligt 31 § ska inte heller lämnas när

[37] Senaste lydelse 2008:855.
[38] Senaste lydelse 2007:981.

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

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

3. uppgift om vem som innehar teleadressen inte fastställs.

Denna lag träder i kraft den 1 januari 2010.

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

Härigenom föreskrivs följande.

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

2 § Inhämtning får avse

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

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

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

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

5 § I ett beslut om inhämtning av uppgifter ska det anges vilken tid och, i förekommande fall, vilken teleadress och vilket avgränsat geografiskt område tillståndet avser. Tiden får inte bestämmas längre än nödvändigt och får, såvitt gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.
Inhämtning av uppgifter får beslutas och genomföras endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

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

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

8 § Uppteckningar av uppgifter ska granskas snarast möjligt.
Uppteckningar ska, i de delar de är av betydelse för att förebygga eller förhindra brott, bevaras så länge det behövs för att förebygga eller förhindra brott. De ska därefter förstöras.
Trots vad som sägs i andra stycket får brottsbekämpande myndigheter behandla uppgifter från uppteckningar i enlighet med vad som är särskilt föreskrivet i lag.

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

Denna lag träder i kraft den 1 januari 2010.

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

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

Nuvarande lydelse

16 kap.

1 §[39]

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

3. denna lag enligt	
5 kap. 1 §	såvitt avser uppgift om kvarhållande av försändelse på befordringsföretag, hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning eller hemlig rumsavlyssning på grund av beslut av domstol, undersökningsledare eller åklagare
9. 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation	
6 kap. 21 § lagen (2003:389) om elektronisk kommunikation	såvitt avser uppgift om kvarhållande av försändelse på befordringsföretag eller om hemlig teleavlyssning och hemlig teleövervakning på grund av beslut av domstol, undersökningsledare eller åklagare

Föreslagen lydelse

16 kap.

[39] Senaste lydelse 2008:815

1 §

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

---

3. denna lag enligt

---

5 kap. 1 §	såvitt avser uppgift om kvarhållande av försändelse på befordringsföretag, hemlig teleavlyssning, hemlig teleövervakning, hemlig kameraövervakning eller hemlig rumsavlyssning på grund av beslut av domstol, undersökningsledare eller åklagare, *eller inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet*

---

9. 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation

---

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

Denna lag träder i kraft den 1 januari 2010.

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

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

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

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

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
8 §[40]	
Bestämmelserna i 5–7 §§ gäller inte	
1. när en myndighet eller en domstol behöver tillgång till sådana uppgifter som avses i 5 § för att lösa tvister,	
2. för elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om hemlig teleavlyssning, hemlig teleövervakning, tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning, eller	2. för elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om hemlig teleavlyssning, hemlig teleövervakning, tekniskt bistånd med hemlig teleavlyssning eller med hemlig teleövervakning, *inhämtning av uppgifter enligt lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, eller*
3. i den utsträckning uppgifter som avses i 5 § är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.	
	10 a §
	Bestämmelserna i 9 och 10 §§ gäller inte när lokaliseringsuppgifter omfattas av beslut om inhämtning av uppgifter enligt 27 kap. rättegångsbalken eller lagen (0000:00) om tillgång till uppgifter om viss elektronisk kommunikation i de brottsbekämpande myndigheternas

[40] Senaste lydelse 2005:493.

underrättelseverksamhet.

21 §[41]

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

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

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

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

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

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

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

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

22 §[42]

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

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

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

2. uppgift som avses i 20 § första stycket 1 och som gäller

2. uppgift som avses i 20 § första stycket 1 och som gäller

[41] Senaste lydelse 2008:719.
[42] Senaste lydelse 2006:737.

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,

4. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

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

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

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

misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som *ska* ingripa mot brottet,

3. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

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

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

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

bestämmelser om unga lagöverträdare, och

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

Ersättning för att lämna ut uppgifter enligt första stycket 8 *skall* vara skälig med hänsyn till kostnaderna för utlämnandet.

trädare, och

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

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

Denna lag träder i kraft den 1 januari 2010.

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

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

dels att 2 § ska ha följande lydelse,

dels att nuvarande 6 § ska betecknas 7 §,

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

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

6 §

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

Denna lag träder i kraft den 1 januari 2010.

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

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

Nuvarande lydelse	*Föreslagen lydelse*
14 b §[43]	
Underrättelseskyldighet enligt 27 kap. 31 § rättegångsbalken, 8 § lagen (1995:1506) om hemlig kameraövervakning eller 15 § lagen (2007:978) om hemlig rumsavlyssning, ska fullgöras av den *åklagare* som är eller har varit förundersökningsledare.	Underrättelseskyldighet enligt 27 kap. 31 § rättegångsbalken, 8 § lagen (1995:1506) om hemlig kameraövervakning eller 15 § lagen (2007:978) om hemlig rumsavlyssning, ska fullgöras av den som är eller har varit förundersökningsledare.
När en underrättelse har underlåtits enligt 27 kap. 33 § andra stycket rättegångsbalken, 8 § lagen om hemlig kameraövervakning eller 15 § lagen om hemlig rumsavlyssning, ska den *åklagare* som är eller har varit förundersökningsledare underrätta Säkerhets- och integritetsskyddsnämnden om detta.	När en underrättelse har underlåtits enligt 27 kap. 33 § andra stycket rättegångsbalken, 8 § lagen om hemlig kameraövervakning eller 15 § lagen om hemlig rumsavlyssning, ska den som är eller har varit förundersökningsledare underrätta Säkerhets- och integritetsskyddsnämnden om detta.
Om den *åklagare* som avses i denna paragraf inte kan fullgöra underrättelseskyldigheten enligt första och andra styckena ska denna i stället fullgöras av en annan åklagare.	Om den *förundersökningsledare* som avses i denna paragraf inte kan fullgöra underrättelseskyldigheten enligt första och andra styckena ska denna i stället fullgöras av annan åklagare, *polisman eller tjänsteman vid Tullverket.*

Denna förordning träder i kraft den 1 januari 2010.

[43] Senaste lydelse 2007:1142.

Förteckning över remissinstanserna (SOU 2009:1)

Bilaga 5

Efter remiss har yttrande över promemorian avgetts av Riksdagens ombudsmän (JO), Göta hovrätt, Hovrätten för Västra Sverige, Stockholms tingsrätt, Malmö tingsrätt, Sundsvalls tingsrätt, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Brottsförebyggande rådet, Brottsoffermyndigheten, Datainspektionen, Försvarets radioanstalt, Signalspaningsnämnden, Kustbevakningen, Tullverket, Skatteverket, Post- och telestyrelsen, Juridiska fakultetsnämnden vid Stockholms universitet, Sveriges advokatsamfund, Polisförbundet, Svenska journalistförbundet, Svenska Stadsnätsföreningen, IT- & Telekomföretagen, Telenor Sverige AB, TeliaSonera AB, Stockholms handelskammare, Svenska Antipiratbyrån, Swedish Network Users' Society (SNUS) och Hi3G Access AB.

Amnesty International, Svenska avdelningen av Internationella Juristkommissionen, Bahnhof AB, Tele 2 AB, Filmproducenternas Rättighetsförening, Föreningen Konstnärliga och Litterära Yrkesutövares Samarbetsnämnd (KLYS), IFPI Svenska gruppen, Svenska Artisters och Musikers Intresseorganisation (SAMI) och Svenska Tonsättares Internationella Musikbyrå (STIM) har inbjudits att lämna synpunkter men har avstått från att yttra sig.