Lagrådsremiss

Hemlig dataavläsning

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 24 oktober 2019

Mikael Damberg

Mikael Kullberg
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

De brottsbekämpande myndigheterna har för närvarande flera hemliga tvångsmedel till sitt förfogande. Den tekniska och samhälleliga utvecklingen har dock medfört svårigheter att använda dessa tvångsmedel. Informationen som ska avlyssnas, övervakas eller beslagtas är ofta krypterad. De brottsbekämpande myndigheterna har ingen faktisk möjlighet att bryta eller kringgå sådan kryptering. Kriminella hittar även metoder för att på andra sätt undkomma vissa hemliga tvångsmedel.

Regeringen föreslår därför att de brottsbekämpande myndigheterna får möjlighet att använda ett nytt hemligt tvångsmedel vid misstankar om allvarlig brottslighet. Det nya tvångsmedlet ska kallas hemlig dataavläsning. Hemlig dataavläsning bedöms leda till bättre och effektivare möjligheter att ta del av information som i dagsläget inte är tillgänglig. Det nya tvångsmedlet ska kunna användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll.

Möjligheten till hemlig dataavläsning ska enligt förslaget införas genom en särskild, tidsbegränsad lag. Vidare föreslås vissa ändringar i andra lagar som en följd av att den nya lagen införs. Den nya lagen och övriga lagändringar föreslås träda i kraft den 1 mars 2020.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om hemlig dataavläsning,
2. lag om ändring i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsdomstolarna och domstolarna under krig eller krigsfara m.m.,
3. lag om ändring i lagen (1991:572) om särskild utlänningskontroll,
4. lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål,
5. lag om ändring i offentlighets- och sekretesslagen (2009:400),
6. lag om ändring i lagen (2017:1000) om en europeisk utredningsorder.

2 Lagtext

2.1 Förslag till lag om hemlig dataavläsning

Härigenom föreskrivs följande.

Ord och uttryck i lagen

1 § Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem.

I lagen avses med

avläsningsbart informationssystem: en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst,

kommunikationsavlyssningsuppgifter: uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress,

kommunikationsövervakningsuppgifter: uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress,

platsuppgifter: uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits,

kameraövervakningsuppgifter: uppgifter som framkommer genom optisk personövervakning,

rumsavlyssningsuppgifter: uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.

Typer av uppgifter som får läsas av eller tas upp

2 § Tillstånd till hemlig dataavläsning får beviljas för att läsa av eller ta upp

1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter,
6. uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i 1–5, eller
7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i 1–6.

Vid hemlig dataavläsning som gäller kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät även hindras från att nå fram.

Grundläggande förutsättning för hemlig dataavläsning

3 § Ett tillstånd till hemlig dataavläsning får beviljas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Hemlig dataavläsning under en förundersökning

4 § Ett tillstånd till hemlig dataavläsning får, om åtgärden är av synnerlig vikt för utredningen och inte annat anges i 6 § första stycket, beviljas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,
2. brott som avses i 27 kap. 2 § andra stycket 2–7 rättegångsbalken,
3. försök, förberedelse eller stämpling till brott som avses i 1 eller 2, om en sådan gärning är belagd med straff, eller
4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Om inte annat anges i 5 § får hemlig dataavläsning under en förundersökning endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för brottet. Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Hemlig dataavläsning som gäller kameraövervakningsuppgifter får användas endast på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

5 § Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter får även beviljas för att utreda vem som skäligen kan misstänkas för ett brott som avses i 4 §. Avläsning eller upptagning av kommunikationsövervakningsuppgifter får då endast avse förfluten tid.

Hemlig dataavläsning enligt första stycket får endast avse ett avläsningsbart informationssystem som har använts vid ett brott eller i anslutning till en brottsplats vid brottstidpunkten eller som av någon annan anledning är av synnerlig vikt för utredningen.

6 § Ett tillstånd till hemlig dataavläsning som gäller rumsavlyssningsuppgifter får endast beviljas vid en förundersökning om brott som avses i 27 kap. 20 d § andra stycket rättegångsbalken.

Hemlig dataavläsning enligt första stycket får användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Om platsen är någon annan stadigvarande bostad än den misstänktes, får tillstånd till hemlig dataavläsning beviljas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.

Hemlig dataavläsning enligt första stycket får aldrig användas på en plats dit tillträdestillstånd enligt 13 § inte får beviljas.

Hemlig dataavläsning utanför en förundersökning

Förhindrande av vissa särskilt allvarliga brott

7 § Ett tillstånd till hemlig dataavläsning får beviljas om

1. det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar brott som anges i 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, eller

2. det finns en påtaglig risk för att sådan brottslig verksamhet kommer att utövas inom en organisation eller grupp och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Ett tillstånd enligt första stycket får beviljas endast om åtgärden är av synnerlig vikt för att förhindra sådan brottslig verksamhet som anges i det stycket.

Hemlig dataavläsning som gäller kameraövervakningsuppgifter får användas endast på en plats där den person som anges i första stycket kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Ett tillstånd får inte avse rumsavlyssningsuppgifter.

8 § Hemlig dataavläsning enligt 7 § får avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en person som anges i den bestämmelsen.

Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att en person som anges i 7 § under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Särskild utlänningskontroll

9 § Ett tillstånd till hemlig dataavläsning får beviljas för att läsa av eller ta upp uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av

1. ett utvisningsbeslut enligt 1 § 2 lagen (1991:572) om särskild utlänningskontroll, eller

2. ett avvisnings- eller utvisningsbeslut enligt 8 eller 8 a kap. utlänningslagen (2005:716) eller motsvarande äldre bestämmelser och det finns sådana omständigheter i fråga om utlänningen som avses i 1 § 2 lagen om särskild utlänningskontroll.

Ett tillstånd till hemlig dataavläsning får också beviljas för att läsa av eller ta upp uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Tillståndet får beviljas endast om Migrationsverket, regeringen eller en domstol har beslutat att 19–22 §§ lagen om särskild utlänningskontroll samt denna lag ska tillämpas på utlänningen. Det förfarande och de förutsättningar som gäller för ett beslut om att 19–22 §§ lagen om särskild

utlänningskontroll ska tillämpas i fråga om utlänningen gäller också för ett beslut i fråga om hemlig dataavläsning.

Ett tillstånd får beviljas endast om det finns synnerliga skäl och det är av betydelse för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott.

Ett tillstånd får inte avse kameraövervaknings- eller rumsavlyssningsuppgifter.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

10 § Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter får beviljas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i 2 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Vid hemlig dataavläsning enligt första stycket får meddelanden inte hindras att nå fram enligt 2 § andra stycket.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervakningsuppgifter får endast avse uppgifter i förfluten tid.

Förbud mot hemlig dataavläsning

11 § Ett tillstånd till hemlig dataavläsning får inte avse ett avläsningsbart informationssystem som stadigvarande används eller är särskilt avsett att användas

1. i verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,
2. i verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller
3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, i verksamhet för bikt eller enskild själavård.

Tillträdestillstånd

12 § Vid hemlig dataavläsning får den verkställande myndigheten, efter särskilt tillstånd, i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd får endast avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller en sådan person som anges i 7 § första stycket eller 9 § första stycket, får tillstånd beviljas endast om det finns synnerlig anledning att anta att informationssystemet finns där.

13 § Ett tillträdestillstånd enligt 12 § får inte avse en plats som stadigvarande används eller är särskilt avsedd att användas

1. för verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,

2. för verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller

3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, för bikt eller enskild själavård.

Tillståndsprövning

14 § Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagare. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen eller Polismyndigheten.

15 § Frågor om hemlig dataavläsning under en förundersökning prövas av den domstol som anges i 19 kap. rättegångsbalken. Om förundersökningen avser brott som anges i 27 kap. 2 § andra stycket 2–8 rättegångsbalken får frågan även prövas av Stockholms tingsrätt.

Frågor om hemlig dataavläsning enligt 7–10 §§ ska alltid prövas av Stockholms tingsrätt.

16 § När en ansökan eller anmälan om hemlig dataavläsning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet ska den som gjort ansökan och det offentliga ombudet närvara.

För offentliga ombud i ärenden om hemlig dataavläsning gäller 27 kap. 26 och 27 §§, 28 § andra stycket samt 29 och 30 §§ rättegångsbalken.

17 § Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens tillstånd i frågor om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning som gäller rumsavlyssningsuppgifter eller hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om åklagaren har gett ett tillstånd enligt första stycket, ska åklagaren utan dröjsmål skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som lästs av eller tagits upp inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

18 § I ett tillstånd till hemlig dataavläsning ska följande anges:

1. vilken tid tillståndet avser,

2. vilket avläsningsbart informationssystem tillståndet avser,

3. vilken typ av uppgift enligt 2 § första stycket som får läsas av eller tas upp,

4. villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, och

5. vem som är skäligen misstänkt för brottet, vid åtgärd som gäller rumsavlyssningsuppgifter.

Om tillståndet avser en plats enligt 4 § tredje stycket eller 6 § andra stycket ska även platsen anges i tillståndet. Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, ska det anges i beslutet.

Tiden för tillståndet får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet.

19 § På förfarandet enligt denna lag i övrigt tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte något annat anges i denna lag. Handläggningen ska ske skyndsamt.

20 § Ett beslut i frågor om hemlig dataavläsning får verkställas omedelbart.

Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, ska den som ansökt om åtgärden eller rätten omedelbart upphäva beslutet.

21 § När rätten har meddelat ett beslut i fråga om hemlig dataavläsning ska den underrätta Säkerhets- och integritetsskyddsnämnden om beslutet.

Genomförande av hemlig dataavläsning

Tillåtna tekniska metoder

22 § När ett tillstånd till hemlig dataavläsning har beviljats får de tekniska hjälpmedel som behövs för avläsningen och upptagningen användas.

Om det är nödvändigt får systemskydd brytas eller kringgås och tekniska sårbarheter utnyttjas.

Skyldighet att medverka

23 § Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation är på begäran av den verkställande myndigheten skyldig att medverka i samband med verkställighet av hemlig dataavläsning.

Den som medverkar enligt första stycket har rätt till ersättning för kostnader som uppstår vid sådan medverkan. Ersättningen ska betalas av den verkställande myndigheten.

Teknikanpassning och otillåten tilläggsinformation

24 § Den teknik som används i samband med hemlig dataavläsning ska anpassas efter det tillstånd som beviljats. Tekniken får inte göra det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet. Om sådana uppgifter har lästs av eller tagits upp ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas.

Uppgifter som anges i första stycket får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller för någon annan som uppgifterna avser.

Aktsamhetskrav

25 § När ett beslut om hemlig dataavläsning verkställs får någon olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser får dock inte åsidosättas, minskas eller skadas till följd av verkställigheten.

När verkställigheten avslutas ska den verkställande myndigheten vidta de åtgärder som behövs för att informationssäkerheten i det avläsningsbara informationssystem som tillståndet avser ska hålla åtminstone samma nivå som vid verkställighetens början.

Ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet har gått ut eller tillståndet upphävts.

26 § Den verkställande myndigheten ska utse en eller flera personer som får verkställa hemlig dataavläsning. Sådana personer ska vara särskilt lämpade för uppdraget och ha särskilda kunskaper om informationssäkerhet samt den särskilda kompetens, utbildning och erfarenhet som i övrigt är nödvändig.

Förbud att läsa av eller ta upp vissa uppgifter

27 § Hemlig dataavläsning enligt 2 § första stycket 6 eller 7 får inte avse uppgifter som enligt 27 kap. 2 § första stycket rättegångsbalken hindrar beslag.

Hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram.

Om det under verkställigheten kommer fram uppgifter som omfattas av första eller andra styckena ska verkställigheten omedelbart avbrytas och upptagningar och uppteckningar omedelbart förstöras i de delar som de omfattas av förbudet.

Överskottsinformation, granskning och underrättelse till enskilda

Förundersökning

28 § När hemlig dataavläsning används eller har använts under en förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 23 a och 24 §§ rättegångsbalken tillämpas för åtgärden. Det som gäller för hemlig rumsavlyssning ska dock tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

För underrättelse till en enskild vid hemlig dataavläsning under förundersökning gäller 27 kap. 31–33 §§ rättegångsbalken. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

Förhindrande av vissa särskilt allvarliga brott

29 § När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas.

För underrättelse till en enskild vid hemlig dataavläsning i fall som anges i 7 § gäller 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

Särskild utlänningskontroll

30 § När hemlig dataavläsning används eller har använts i fall som anges i 9 § ska 21 a § och 22 § första och andra styckena lagen (1991:572) om särskild utlänningskontroll tillämpas. Det som anges där om hemlig avlyssning och övervakning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

31 § När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6–8 §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet tillämpas. Det som anges där om inhämtning av uppgifter ska tillämpas för hemlig dataavläsning.

Tystnadsplikt

32 § Den som i samband med verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation har fått del av eller tillgång till en uppgift som hänför sig till användning av hemlig dataavläsning, får inte obehörigen föra vidare eller utnyttja det han eller hon fått del av eller tillgång till.

Rätt att meddela föreskrifter

33 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om

1. medverkan och ersättning enligt 23 §, och
2. underrättelser enligt 24 §.

---

1. Denna lag träder i kraft den 1 mars 2020.

2. Lagen upphör att gälla vid utgången av februari 2025.

2.2 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]	
Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § rättegångsbalken, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.	Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § rättegångsbalken *eller hemlig dataavläsning enligt 2 § första stycket 5 lagen (2019:000) om hemlig dataavläsning,* får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.

Om åklagaren har gett ett sådant tillstånd, ska han eller hon utan dröjsmål skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Denna lag träder i kraft den 1 mars 2020.

[1] Senaste lydelse 2014:1426

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

Härigenom föreskrivs att 20 § lagen (1991:572) om särskild 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 Polismyndigheten 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 Polismyndigheten 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.

I lagen (2019:000) om hemlig dataavläsning finns bestämmelser om att rätten kan meddela Säkerhetspolisen eller Polismyndigheten tillstånd enligt den lagen.

Denna lag träder i kraft den 1 mars 2020.

[1] Senaste lydelse 2014:589.

2.4 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 2 kap. 1, 2 och 4 §§ ska ha följande lydelse,

dels att det ska införas sex nya paragrafer, 4 kap. 28 c–28 h §§, och närmast före 4 kap. 28 c, 28 e, 28 f, 28 g och 28 h §§ nya rubriker av 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 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	*7. hemlig kameraövervakning,*
10. hemlig rumsavlyssning,	*8. hemlig rumsavlyssning,*
	9. hemlig dataavläsning,
	10. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning,
	11. tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning

[1] Senaste lydelse 2012:284.

	enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning,
11. överförande av frihetsberövade för förhör m.m., och	*12. överförande av frihetsberövade för förhör m.m., och*
12. rättsmedicinsk undersökning av en avliden person.	*13. rättsmedicinsk undersökning av en avliden person.*

Lagen hindrar inte att hjälp lämnas med någon annan åtgärd än en 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.

2 kap.

1 §[2]

Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–6, 9, 10 och 12* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–9 och 13* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.
Rättslig hjälp som avses i 1 kap. 2 § första stycket *7, 8 och 11* lämnas enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket *10–12* lämnas enligt de särskilda bestämmelserna i denna lag.

I 5 kap. 2 § finns bestämmelser om att den rättsliga hjälpen får förenas med villkor i vissa fall.

2 §[3]

Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–4, 7 och 11* får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket *5, 6, 8–10 och 12* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan och beslag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–4, 10 och 12* får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket *5–9, 11 och 13* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan och beslag.

[2] Senaste lydelse 2007:982.
[3] Senaste lydelse 2007:982.

4 §[4]

En ansökan om rättslig hjälp i Sverige enligt denna lag bör innehålla

– uppgift om den utländska domstol eller myndighet som handlägger ärendet,

– en beskrivning av det rättsliga förfarande som pågår,

– uppgift om den aktuella gärningen *med* tid och plats för *denna*, samt de bestämmelser som är tillämpliga i den ansökande staten,

– uppgift om den aktuella gärningen, tid och plats för *den*, samt *uppgift om* de bestämmelser som är tillämpliga i den ansökande staten,

– uppgift om vilken åtgärd som begärs och, i förekommande fall, i vilken egenskap en person ska höras,

– namn på och adress till de personer som är aktuella i ärendet.

I 4 kap. 8, 11, 14, 24 a, 25, 25 b, 25 c, 26 a, 29 och 29 a §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.

I 4 kap. 8, 11, 14, 24 a, 25, 25 b, 25 c, 26 a, *28 c*, 29 och 29 a §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.

Om ärendet är brådskande eller om *verkställighet* önskas inom viss tidsfrist, ska detta anges och motiveras.

Om ärendet är brådskande eller om *verkställigheten* önskas inom *en* viss tidsfrist, ska detta anges och motiveras.

En ansökan om rättslig hjälp ska göras skriftligen genom post, bud eller telefax. Den får även, efter överenskommelse i det enskilda fallet, översändas på annat sätt.

4 kap.

Hemlig dataavläsning i Sverige

Rättslig hjälp i Sverige med hemlig dataavläsning

28 c §

En ansökan om hemlig dataavläsning 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 det får ske enligt 17 § lagen (2019:000) om hemlig dataavläsning, själv besluta om åtgärden.

[4] Senaste lydelse 2013:836.

Upptagningar och uppteckningar behöver inte granskas enligt 28 § första stycket lagen om hemlig dataavläsning.

Om åklagaren har fattat beslut enligt första stycket, ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om hemlig dataavläsning. Upptagningar och uppteckningar får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning skett enligt 2 kap. 17 § endast om det är tillåtet enligt 28 § första stycket lagen om hemlig dataavläsning.

I fråga om underrättelse till en enskild enligt 28 § andra stycket lagen om hemlig dataavläsning ska bestämmelserna i 25 § tredje stycket detta kapitel tillämpas.

28 d §

Om en ansökan avser hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning får rättens beslut enligt 28 c § att tillåta hemlig dataavläsning verkställas med tillämpning av 25 a §.

Tekniskt bistånd i Sverige med hemlig dataavläsning

28 e §

Tekniskt bistånd med hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning i form av omedelbar överföring av meddelanden eller uppgifter om meddelanden får lämnas i Sverige enligt de förutsättningar som gäller enligt 25 b § andra, tredje och femte styckena. Vid hemlig dataavläsning i en annan stat än den som ansökt om tekniskt bistånd ska ett tillstånd enligt 28 f § ha lämnats.

Ansökan ska prövas av åklagare. För beslutet om tekniskt bistånd tillämpas 1 §, 18 § första stycket 1–

3 och tredje stycket och 20 § andra stycket lagen om hemlig dataavläsning.

Tillstånd från Sverige till gränsöverskridande hemlig dataavläsning

28 f §

Om ansökan avser tillstånd till gränsöverskridande hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning tillämpas det som gäller för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation enligt 26 a § första och andra styckena och 26 b §. De förutsättningar som gäller enligt 1–6, 11, 14 och 18 §§ lagen om hemlig dataavläsning tillämpas vid tillståndsprövningen. Rätten ska även tillämpa motsvarande förfarande som anges i 16 § den lagen. Tingsrättens beslut får inte överklagas.

Hemlig dataavläsning i utlandet

Rättslig hjälp och tekniskt bistånd i utlandet med hemlig dataavläsning

28 g §

Vid rättslig hjälp och tekniskt bistånd med hemlig dataavläsning i en annan stat tillämpas 26 §.

Tekniskt bistånd får endast avse hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning.

Om en underrättelse ska lämnas till en enskild tillämpas 28 § andra stycket lagen om hemlig dataavläsning.

Tillstånd från en annan stat till gränsöverskridande hemlig dataavläsning

28 h §

När ett tillstånd till hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning beslutats i en brottsutredning i Sverige och avläsningen eller upptagningen kommer att göras i en medlemsstat i Europeiska unionen, Island eller Norge utan hjälp från den andra staten, tillämpas 26 c §.

Denna lag träder i kraft den 1 mars 2020.

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

Härigenom föreskrivs att 18 kap. 19 § och 44 kap. 5 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
18 kap.	
19 §[1]	
Den tystnadsplikt som följer av 5–8, 9 och 10 §§, 11 § första stycket och 12 och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ 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 (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	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, hemlig rumsavlyssning *eller hemlig dataavläsning* på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av uppgifter enligt lagen (2012:278) 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.	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, hemlig kameraövervakning, *hemlig rumsavlyssning eller hemlig dataavläsning* 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	

[1] Senaste lydelse 2019:305.

stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

Lydelse enligt prop. 2018/19:162	*Föreslagen lydelse*
44 kap.	
5 §	
Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer	
1. av beslut som har meddelats med stöd av 7 § lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet,	
2. av 7 kap. 1 § 1 lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,	
3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043), *och*	3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043),
4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige.	4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige, *och*
	5. av 32 § lagen (2019:000) om hemlig dataavläsning.

Denna lag träder i kraft den 1 mars 2020.

2.6 Förslag till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

Härigenom föreskrivs i fråga om lagen (2017:1000) om en europeisk utredningsorder

dels att 1 kap. 4 §, 2 kap. 5 § och 3 kap. 10 § ska ha följande lydelse,

dels att det ska införas fem nya paragrafer, 2 kap. 19 a och 19 b §§, 3 kap. 37 a och 37 b §§ och 4 kap. 15 a §, och närmast före 2 kap. 19 a § och 3 kap. 37 a § nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
4 §	
En utredningsåtgärd enligt denna lag ska avse eller motsvara	
1. förhör under förundersökning,	
2. bevisupptagning vid domstol,	
3. förhör genom ljudöverföring eller ljud- och bildöverföring,	
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller en åtgärd enligt 27 kap. 15 § samma balk,	
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,	
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning *och* hemlig rumsavlyssning,	6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *och hemlig dataavläsning*,
7. tillfälligt överförande av en frihetsberövad person,	
8. rättsmedicinsk undersökning av en avliden person,	
9. kontrollerad leverans,	
10. bistånd i en brottsutredning med användning av en skyddsidentitet,	
11. inhämtande av bevis som finns hos en myndighet, eller	
12. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.	
2 kap.	
5 §	
Innan åklagaren utfärdar en utredningsorder ska åklagaren ansöka om domstolens tillstånd till att utfärda utredningsordern, om utredningsåtgärden avser	
1. kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken,	
2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning *eller* hemlig rumsavlyssning, eller	2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *eller hemlig dataavläsning*, eller

3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m.

I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken utfärda en utredningsorder för kvarhållande av försändelse, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *eller* hemlig kameraövervakning. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken *eller 17 § lagen (2019:000) om hemlig dataavläsning* utfärda en utredningsorder för kvarhållande av försändelse, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation*,* hemlig kameraövervakning *eller hemlig dataavläsning*. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

Innan en utredningsorder för husrannsakan, kroppsvisitation eller kroppsbesiktning utfärdas, får åklagaren enligt 28 kap. 4 § första stycket och 13 § första stycket rättegångsbalken ansöka om domstolens tillstånd till att utfärda utredningsordern.

För domstolens handläggning gäller vad som är föreskrivet i rättegångsbalken eller annan författning för den åtgärd som avses.

Hemlig dataavläsning

19 a §

En utredningsorder får utfärdas för hemlig dataavläsning i Sverige eller i en annan medlemsstat.

En utredningsorder för hemlig dataavläsning i Sverige eller i en annan medlemsstat än den stat till vilken ordern översänds enligt 7 § första stycket får endast avse en åtgärd enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning.

Om dataavläsningen enligt andra stycket ska ske i en annan medlemsstat än den stat till vilken ordern översänds enligt 7 § första stycket ska det av utredningsordern framgå att en underrättelse enligt 4 kap. 12 § har lämnats.

19 b §

När en utredningsorder för hemlig dataavläsning har utfärdats, ska 20 § andra stycket, 27 §

och 28 § första stycket lagen (2019:000) om hemlig dataavläsning tillämpas. I de fall där upptagningen eller uppteckningen görs i Sverige ska 28 § andra stycket lagen om hemlig dataavläsning tillämpas.

3 kap.

10 §

I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken, besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *eller* hemlig kameraövervakning.

I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken *eller 17 § lagen (2019:000) om hemlig dataavläsning*, besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation*,* hemlig kameraövervakning *eller hemlig dataavläsning.*

Hemlig dataavläsning

37 a §

Vid verkställighet av en utredningsorder för hemlig dataavläsning som gäller en åtgärd enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning tillämpas 34 § detta kapitel.

Vid verkställighet enligt 34 § 1 tillämpas 35 § andra stycket. 1 dessa fall får någon upptagning eller uppteckning inte göras i Sverige, och 28 § andra stycket lagen om hemlig dataavläsning ska inte tillämpas.

37 b §

Vid verkställighet av en utredningsorder för hemlig dataavläsning som sker med stöd av 34 § 2 eller i andra fall av verkställighet av en utredningsorder för

hemlig dataavläsning behöver upptagningar eller uppteckningar inte granskas enligt 28 § första stycket lagen (2019:000) om hemlig dataavläsning. Upptagningar och uppteckningar, som finns kvar i Sverige efter det att ärendet har avslutats hos åklagaren och bevismaterialet har överlämnats med stöd av 38 eller 40 §, får bevaras endast om detta är tillåtet enligt 28 § första stycket lagen om hemlig dataavläsning.

I fråga om underrättelse till en enskild enligt 28 § andra stycket lagen om hemlig dataavläsning ska bestämmelserna i 36 § andra stycket detta kapitel tillämpas.

4 kap.

15 a §

Det som anges om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation i 12–15 §§ tillämpas även för hemlig dataavläsning enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning.

Denna lag träder i kraft den 1 mars 2020.

3 Ärendet och dess beredning

Regeringen beslutade den 12 maj 2016 att ge en särskild utredare i uppdrag att utreda om svenska brottsbekämpande myndigheter ska ges möjlighet att använda hemlig dataavläsning (dir. 2016:36). Utredningen, som antog namnet Utredningen om hemlig dataavläsning (Ju 2016:12), överlämnade i november 2017 delbetänkandet Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89). I betänkandet analyseras om det finns behov av att införa hemlig dataavläsning som ett nytt hemligt tvångsmedel.

En sammanfattning av delbetänkandet och utredningens lagförslag finns i *bilaga 1* och *2*. Delbetänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2017/08898/Å).

4 Gällande rätt

4.1 De brottsbekämpande myndigheternas uppdrag

Polisen (Polismyndigheten och Säkerhetspolisen) har i uppdrag att bl.a. förebygga, förhindra och utreda brott och har således en brottsbekämpande funktion. Åklagare vid Åklagarmyndigheten och Ekobrottsmyndigheten ansvarar för ledningen av alla kvalificerade brottsutredningar där det finns skälig misstanke mot någon. Åklagare har dessutom till uppgift att besluta i åtalsfrågor och att föra det allmännas talan i brottmålsprocessen. Särskilda befattningshavare vid Tullverket har rätt att självständigt inleda förundersökning i fråga om vissa brott, t.ex. smuggling. Vid sidan av nu nämnda myndigheter finns det flera myndigheter som medverkar i brottsutredningar och på så sätt har en brottsbekämpande funktion. Det gäller t.ex. Skatteverket och Kustbevakningen. Även Försvarsmakten (militärpolisen) har ett visst brottsbekämpande uppdrag.

Polismyndigheten har ett generellt brottsbekämpande uppdrag och ska utreda och beivra brott som hör under allmänt åtal om det inte är fråga om brott mot rikets säkerhet eller terrorbrott, då det i stället är Säkerhetspolisens uppgift.

Säkerhetspolisens uppdrag kan i huvudsak delas in i fem områden: kontraspionage, kontraterrorism, författningsskydd, säkerhetsskydd och personskydd. Säkerhetspolisen arbetar dessutom med att förhindra spridning, anskaffning och produktion av massförstörelsevapen samt ansvarar vidare för utredningar som rör brott mot Sveriges säkerhet och terroristbrott. Tyngdpunkten i Säkerhetspolisens verksamhet är dock att förebygga brott. Säkerhetspolisen kan därför som regel inte bedriva sin verksamhet utifrån brottsanmälningar. Myndigheten måste i stället själv ha förmåga att identifiera aktörer som har avsikt att begå aktuella brott för att kunna bedöma vilka förutsättningar dessa har att sätta sina planer i verket. Det brottsförebyggande arbetet grundas därför i stor utsträckning på uppgifter som inhämtas i säkerhetsunderrättelseverksamhet. Denna verksamhet bedrivs i ett skede innan det finns tillräckliga skäl för att inleda förundersökning. I stor utsträckning bygger verksamheten på att uppgifter inhämtas innan en person eller gruppering har konkreta planer eller vidtagit åtgärder för att begå brott.

4.2 Grundläggande regler till skydd för den personliga integriteten

Regeringsformen

Den offentliga makten ska enligt 1 kap. 2 § regeringsformen utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv

och familjeliv. Bestämmelsen ger uttryck för en grundläggande målsättning med det allmännas verksamhet.

Enligt 2 kap. 6 § första stycket regeringsformen gäller vidare att var och en gentemot det allmänna är skyddad mot bl.a. husrannsakan och liknande intrång, undersökning av brev eller annan förtrolig försändelse samt hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Det finns också i paragrafens andra stycke en bestämmelse som tillförsäkrar enskilda ett generellt skydd gentemot det allmänna, mot betydande intrång i den personliga integriteten om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Skyddet enligt 2 kap. 6 § regeringsformen kan begränsas endast genom lag. Begränsningen får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får inte 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 (2 kap. 20 och 21 §§ regeringsformen). För utländska medborgare som är bofasta i riket gäller att särskilda begränsningar i dessa rättigheter får göras genom lag (2 kap. 25 § regeringsformen).

Europakonventionen

Den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) gäller som svensk lag. Lag eller annan föreskrift får inte meddelas i strid med Sveriges åtaganden på grund av konventionen (2 kap. 19 § regeringsformen).

Enligt artikel 8.1 Europakonventionen har var och en rätt till respekt för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Rätten till skydd för privatlivet är av mycket allmän art och skyddar bl.a. rätten att etablera och utveckla relationer med andra människor och omvärlden. Med korrespondens avses olika former för att överföra meddelanden mellan individer. Överföring av meddelanden med hjälp av telefon, telefax, radio och datorer omfattas av konventionens skydd för korrespondens (se Hans Danelius, Mänskliga rättigheter i europeisk praxis, 5 uppl. 2015 s. 432).

Dessa rättigheter får enligt artikel 8.2 Europakonventionen inte inskränkas annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter. Det innebär att en inskränkning måste ha stöd i inhemsk lag som i sin tur måste uppfylla rimliga anspråk på rättssäkerhet, såsom att skydda mot godtycke, vara tillgänglig för allmänheten och vara förutsebar. Att inskränkningen måste vara nödvändig i ett demokratiskt samhälle för något av de i artikeln skyddade intressena innebär i huvudsak att det ska finnas ett angeläget samhälleligt behov av åtgärden och att den måste stå i rimlig proportion till det syfte som ska tillgodoses (Hans Danelius, samma bok s. 369–370). Konventionsstaterna har ett visst handlingsutrymme att själva avgöra om begränsningarna är nödvändiga för ett givet syfte (eng. margin of appreciation). Europadomstolen förbehåller sig dock rätten att

överpröva denna bedömning inom ramen för prövningen av någons enskilda klagomål hos domstolen.

Frågan om förutsebarhet när det gäller spaningsåtgärder eller hemliga tvångsmedel har vid ett flertal tillfällen prövats av Europadomstolen. Domstolen har förklarat att innebörden av kravet på förutsebarhet inte innebär att en person på förhand måste kunna veta t.ex. när det är sannolikt att myndigheterna avlyssnar dennes samtal. Däremot måste lagstiftningen om sådana åtgärder vara så tydlig att den ger medborgarna en tillräcklig indikation om vilka omständigheter som krävs och vilka villkor som ställs för att myndigheterna ska få använda sig av åtgärderna (se t.ex. Europadomstolens dom den 4 december 2015 i målet Roman Zakharov mot Ryssland punkt 229 och där angivna rättsfall).

Europadomstolen har genom praxis utvecklat en minimistandard för de krav som bör ställas på lagstiftningen om dolda spaningsåtgärder eller hemliga tvångsmedel till undvikande av missbruk (se målet Roman Zakharov mot Ryssland punkt 231 och där angivna rättsfall).

Enligt denna bör följande anges i den nationella lagstiftningen.

– arten av de brott som kan leda till beslut om åtgärden
– en definition av de personkategorier som kan riskera att få sådana åtgärder riktade mot sig
– en begränsning i tid för hur länge åtgärden får pågå
– förfaranderegler för undersökning, användning och lagring av de uppgifter som inhämtas
– vilka försiktighetsåtgärder som ska vidtas vid överföring av information till andra parter.
– de omständigheter under vilka inspelningar kan eller måste raderas.

Av Europadomstolens praxis följer att åtgärder som utgör ett större intrång i privatlivet bör tillhandahållas med tydligare bemyndiganden och bli föremål för fler restriktioner än verksamhet som medför ett mindre sådant intrång (Europadomstolens dom den 2 september 2010 i målet Uzun mot Tyskland punkt 43–48).

Europadomstolen har vidare konstaterat att nationell lagstiftning om dolda spaningsåtgärder och hemliga tvångsmedel måste innehålla kontrollmekanismer för att skydda mot missbruk. Vad som krävs i det avseendet beror på åtgärdernas karaktär, räckvidd och varaktighet, vilka motiv som krävs för att besluta, utföra och övervaka dem samt vilken typ av rättsmedel som finns i den nationella lagstiftningen (se t.ex. Europadomstolens dom den 25 september 2001 i målet P.G. och J.H. mot Storbritannien punkt 76–81 och målet Uzun mot Tyskland).

Enligt artikel 13 Europakonventionen ska var och en som fått sina fri- och rättigheter enligt konventionen kränkta ha tillgång till ett effektivt rättsmedel inför en nationell myndighet, även om kränkningen förövats av någon under utövning av offentlig myndighet. Enligt propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation (prop. 2011/12:55 s. 55) kräver inte artikeln ett rättsmedel inför domstol, utan även administrativa rättsmedel kan vara tillräckliga för att uppfylla konventionskraven. För att rättsmedlet ska anses vara effektivt får dock den rättsliga prövningen inte vara alltför begränsad. Den ska i princip sträcka sig lika långt som Europadomstolens egen prövning av om

konventionen blivit överträdd. I många fall är möjligheten att föra skadeståndstalan tillräcklig för att motsvara kraven på effektiva rättsmedel i artikel 13 (Hans Danelius, samma bok s. 546). Europadomstolen har framhållit att det vid hemlig telefonavlyssning är svårt att använda normala rättsmedel. Enligt domstolen kan det inte krävas att den som berörs ska underrättas om avlyssningen i förväg, utan kravet måste i detta sammanhang förstås så att det ska finnas ett så effektivt rättsmedel som möjligt med hänsyn till de särskilda omständigheterna. Domstolen har lagt vikt vid bl.a. om det funnits regler om underrättelse om tvångsmedlet i efterhand, när detta kunnat ske utan risk eller skada (samma bok s. 547).

FN:s konvention om medborgerliga och politiska rättigheter

FN:s 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. Sverige ratificerade konventionen den 26 november 1971 (SÖ 1971:42).

EU:s rättighetsstadga

En bestämmelse om rätt till respekt för bl.a. privatlivet och korrespondensen finns också i artikel 7 Europeiska unionens stadga om de grundläggande rättigheterna av den 7 december 2000, anpassad den 12 december 2007 i Strasbourg (rättighetsstadgan). I artikel 8 i rättighetsstadgan slås därutöver fast en rätt till skydd för personuppgifter som rör någon enskild. Denna rättighet har ingen direkt motsvarighet i Europakonventionen. Av artikel 52.3 följer att i den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen ska de ha samma innebörd och räckvidd som enligt konventionen. Det hindrar dock samtidigt inte unionsrätten från att tillförsäkra ett mer långtgående skydd (jfr artikel 52.3 och artikel 53).

Rättighetsstadgan riktar sig till medlemsstaterna endast när de tillämpar unionsrätten. Det innebär att rättigheterna i stadgan måste iakttas bara vid tillämpningen av nationell lagstiftning som genomför EU-rätt och nationell lagstiftning som omfattas av unionens tillämpningsområde (se t.ex. EU-domstolens dom den 26 februari 2013 i målet Åkerberg Fransson, C-617/10, punkt 21).

4.3 Hemliga tvångsmedel

Tre allmänna principer gäller för all tvångsmedelsanvändning, nämligen ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Dessa principer gäller alltid vid beslut om, och tillämpning av, de hemliga tvångsmedlen. Enligt ändamålsprincipen får ett tvångsmedel användas endast för det ändamål som framgår av lagstiftningen. Behovsprincipen innebär att ett tvångsmedel får användas endast om det finns ett påtagligt

behov och en mindre ingripande åtgärd är otillräcklig. Proportionalitetsprincipen innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden.

Rättegångsbalken (RB) innehåller inte någon definition av straffprocessuella tvångsmedel. Det rör sig dock om åtgärder som har en funktion inom straffprocessen men som inte är straff eller andra sanktioner. Åtgärderna utgör myndighetsutövning och är ett intrång i någons rättssfär. Vanligtvis innefattar användningen tvång mot person eller egendom (se t.ex. Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas?, 4 uppl. 2018 s. 5 och P-O Ekelöf m.fl., Rättegång, tredje häftet, 7 uppl. 2006 s. 38–39).

I förundersökning används straffprocessuella tvångsmedel i brottsutredande syfte eller för att en rättegång ska kunna genomföras. Exempel på sådana tvångsmedel är husrannsakan, kroppsvisitation, kroppsbesiktning, beslag, gripande, anhållande och häktning.

En grundläggande förutsättning för att använda straffprocessuella tvångsmedel är normalt att en förundersökning har inletts. I vart fall inleds en förundersökning i samband med att en åtgärd vidtas, t.ex. ett gripande (se dock t.ex. 23 kap. 22 § RB). Under vissa förutsättningar får emellertid några av de brottsbekämpande myndigheterna använda hemliga tvångsmedel redan i underrättelseverksamhet. Detta görs då i syfte att förhindra särskilt allvarlig brottslighet.

Bland de straffprocessuella tvångsmedlen intar de hemliga tvångsmedlen en särställning eftersom den berörde inte är medveten om att de används mot honom eller henne, men det antas att de äger rum mot hans eller hennes vilja. De intrång i den personliga integriteten som åtgärderna innebär medför att de, även i avsaknad av tvång, betecknas som tvångsmedel (se P-O Ekelöf m.fl., samma bok s. 42).

Behandlingen av personuppgifter vid användning av hemliga tvångsmedel regleras huvudsakligen i brottsdatalagen (2018:1177) med tillhörande registerförfattningar (t.ex. lagen [2018:1693] om polisens behandling av personuppgifter inom brottsdatalagens område) som genomför Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (dataskyddsdirektivet). Dessa registerförfattningar innehåller regler till skydd för den personliga integriteten när personuppgifter behandlas i den brottsbekämpande verksamheten och när de överförs till annan verksamhet.

De hemliga tvångsmedlen är:

- hemlig avlyssning av elektronisk kommunikation
- hemlig övervakning av elektronisk kommunikation
- hemlig kameraövervakning
- hemlig rumsavlyssning.

Även kvarhållande (och kontroll) av försändelse anses vara ett hemligt tvångsmedel eftersom den mot vilken åtgärden riktas inte känner till att så

sker och det kan antas att den äger rum mot dennes vilja. Av samma skäl har också regeringen tidigare ansett att inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) utgör ett hemligt tvångsmedel (se prop. 2011/12:55 s. 111). Kvarhållande och kontroll av försändelse har inte betydelse i frågan om hemlig dataavläsning och berörs därför inte vidare i denna lagrådsremiss.

Hemlig avlyssning av elektronisk kommunikation

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. Ett elektroniskt kommunikationsnät är ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och 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 § lagen (2003:389) om elektronisk kommunikation (LEK). I begreppet adress ingår olika typer av nummer, t.ex. telefonnummer och andra identifikationsnummer och adresser, såsom e-postadresser (prop. 2011/12:55 s. 62). Tvångsmedlet kan tillämpas på alla former av kommunikation genom elektroniska kommunikationsnät och är tillämpligt på muntlig och skriftlig kommunikation, liksom även på datakommunikation.

Tillstånd till hemlig avlyssning av elektronisk kommunikation får lämnas vid misstanke om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, för vissa särskilt uppräknade brott som framför allt Säkerhetspolisen utreder samt om det i ett enskilt fall kan antas att brottets straffvärde överstiger fängelse i två år, 27 kap. 18 § andra stycket RB.

Hemlig avlyssning av elektronisk kommunikation får i förundersökningsfallen endast ske om någon är skäligen misstänkt för ett brott. Ett tillstånd till hemlig avlyssning ger också rätt att vidta sådana åtgärder som kan vidtas inom ramen för ett tillstånd till hemlig övervakning av elektronisk kommunikation (27 kap. 18 § tredje stycket RB).

Enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) får tillstånd till hemlig avlyssning av elektronisk kommunikation meddelas redan i underrättelseskedet, dvs. innan en förundersökning har inletts, om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva sådan brottslig verksamhet som nämns i lagrummet. Sådant tillstånd får också beviljas om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas sådan brottslig verksamhet som avses i lagen och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Ytterligare ett fall då hemlig avlyssning får förekomma utan att en förundersökning pågår är inom ramen för särskild utlänningskontroll. Tillstånd till hemlig avlyssning av elektronisk kommunikation får nämligen beviljas om det är av betydelse för att utreda om en utlänning eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff

för terroristbrott och det finns synnerliga skäl, 19–20 §§ lagen (1991:572) om särskild utlänningskontroll (LSU).

Hemlig avlyssning av elektronisk kommunikation får såväl i förundersökningsfallen som i underrättelsefallen avse ett telefonnummer eller annan adress som, under den tid som tillståndet avser, innehas eller har innehafts av den misstänkte (eller, i underrättelsefallen, den person som avses) eller som annars kan antas ha använts eller komma att användas av denne. Åtgärden får också avse ett telefonnummer eller en annan adress som det finns synnerlig anledning att anta att den personen, under den tid som tillståndet avser, har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta (27 kap. 20 § första stycket RB och 2 § preventivlagen).

När tillstånd till hemlig avlyssning av elektronisk kommunikation har lämnats, får de tekniska hjälpmedel som behövs för åtgärden användas (27 kap. 25 § första stycket RB och 9 § preventivlagen). Polisen får alltså verkställa ett beslut om hemliga avlyssning av elektronisk kommunikation inte bara genom att använda traditionell avlyssningsutrustning utan också genom att använda såväl hårdvara som programvara, se propositionen Hemlig teleavlyssning och hemlig teleövervakning (prop. 1994/95:227 s. 29).

Hemlig övervakning av elektronisk kommunikation

Hemlig övervakning av elektronisk kommunikation innebär att uppgifter i hemlighet hämtas in om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Genom hemlig övervakning av elektronisk kommunikation får meddelanden även hindras från att nå fram. Till skillnad från hemlig avlyssning av elektronisk kommunikation ger inte tvångsmedlet tillgång till uppgifter om innehållet i meddelanden. Det som kan hämtas in är i stället trafikuppgifter och uppgifter om lokalisering.

Tillstånd till hemlig övervakning av elektronisk kommunikation kan beviljas vid en förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader, för vissa särskilt uppräknade brott som framför allt Polismyndigheten utreder (t.ex. dataintrång och icke ringa barnpornografibrott) samt för vissa särskilt uppräknade brott som framför allt Säkerhetspolisen utreder (27 kap. 19 § andra stycket RB).

Åtgärden får i förundersökningsfallen tillåtas dels om någon är skäligen misstänkt för brott och då avse de telefonnummer eller adresser som gäller vid hemlig avlyssning av elektronisk kommunikation (se ovan), dels i syfte att utreda vem som skäligen kan misstänkas för brottet. I den senare situationen gäller dock att tvångsmedlet får användas endast vid en förundersökning som avser brott som kan leda till hemlig avlyssning av elektronisk kommunikation (27 kap. 19 § fjärde stycket RB) och att övervakning som innebär att uppgifter hämtas in om meddelanden endast får avse förfluten tid (27 kap. 20 § andra stycket RB).

Enligt både preventivlagen och lagen om särskild utlänningskontroll gäller samma förutsättningar för tillstånd till hemlig övervakning av elektronisk kommunikation som för hemlig avlyssning såväl avseende vilken brottslighet som krävs som vilka telefonnummer eller adresser som får övervakas.

Vid hemlig övervakning av elektronisk kommunikation får de tekniska hjälpmedel användas som behövs för åtgärden (se ovan om hemlig avlyssning av elektronisk kommunikation).

Inhämtning av elektronisk kommunikation i underrättelseverksamhet

Inhämtningslagen reglerar förutsättningarna för Polismyndigheten, Säkerhetspolisen och Tullverket att i underrättelseverksamhet hämta in övervakningsuppgifter om elektronisk kommunikation från teleoperatörerna. De uppgifter som kan hämtas in motsvarar de som kan hämtas in genom hemlig övervakning av elektronisk kommunikation när den åtgärden används för att utreda vem som skäligen kan misstänkas för brottet. Uppgifter får hämtas in, om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott vilka har ett straffminimum på fängelse i minst två år eller om det är fråga om brottslig verksamhet som innefattar vissa särskilt angivna samhällsfarliga brott inom Säkerhetspolisens ansvarsområde (2 §).

Hemlig kameraövervakning

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. I förarbetena till lagstiftningen om hemlig kameraövervakning förtydligas att tvångsmedlet inte omfattar ljudupptagning, se propositionen Hemlig kameraövervakning (prop. 1995/96:85 s. 37).

Tillstånd till hemlig kameraövervakning kan lämnas vid förundersökning som rör de brott som kan aktualisera tillstånd till hemlig avlyssning av elektronisk kommunikation (27 kap. 20 a § andra stycket RB). Övervakningen får som huvudregel användas endast om någon är skäligen misstänkt för brottet. Åtgärden får endast avse sådan plats där den skäligen misstänkte kan antas komma att uppehålla sig (27 kap. 20 b § RB). Om det inte finns någon skäligen misstänkt för brottet får hemlig kameraövervakning dock användas för att övervaka den plats där brottet har begåtts eller en nära omgivning till denna plats, dock endast om syftet är att fastställa vem som skäligen kan misstänkas för brottet (27 kap. 20 c §).

För hemlig kameraövervakning enligt preventivlagen gäller samma förutsättningar som för hemlig avlyssning av elektronisk kommunikation avseende vilken brottslighet som kan aktualisera åtgärden (1 §). Den får endast avse en plats där den som ska övervakas kan antas komma att uppehålla sig eller en plats där den brottsliga verksamheten kan antas komma att utövas eller en nära omgivning till denna plats (3 §).

Hemlig kameraövervakning får inte förekomma inom ramen för särskild utlänningskontroll.

Hemlig rumsavlyssning

Hemlig rumsavlyssning innebär avlyssning eller upptagning som görs i hemlighet, och med ett tekniskt hjälpmedel som är avsett att återge ljud, och avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till. Rumsavlyssning får endast användas vid förundersökning avseende brott för vilket det inte är föreskrivet lindrigare straff än fängelse fyra år, spionerі, brott mot lagen (2018:558) om företagshemligheter som kan antas ha begåtts eller understötts av främmande makt samt för vissa andra särskilt uppräknade brott (t.ex. människohandel, våldtäkt mot barn, grovt övergrepp i rättssak) om det i det enskilda fallet kan antas att brottets straffvärde överstiger fängelse i fyra år (27 kap. 20 d § RB).

Tvångsmedlet får användas endast när någon är skäligen misstänkt för något av de angivna brotten. Det får inte användas i underrättelseverksamhet. Dessutom får åtgärden endast avse en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Om åtgärden avser någon annan stadigvarande bostad än den misstänktes får hemlig rumsavlyssning användas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.

4.4 Rättssäkerhetsgarantier och skyddet för den personliga integriteten i lagstiftningen om hemliga tvångsmedel

4.4.1 Domstolsprövning

I förundersökningsfallen gäller som utgångspunkt att en domstol ska pröva frågor om hemliga tvångsmedel. Ansökan görs av åklagaren när det gäller hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning (27 kap. 21 § RB).

Även i underrättelsefallen enligt preventivlagen och lagen om särskild utlänningskontroll gäller att det är domstol som prövar frågor om tillstånd till hemliga tvångsmedel. I dessa fall är emellertid Stockholms tingsrätt den enda domstol som har rätt att pröva ansökan. Enligt preventivlagen görs ansökan av åklagaren (6 §) medan yrkande enligt lagen om särskild utlänningskontroll framställs av Säkerhetspolisen eller Polismyndigheten (21 §). När det däremot gäller inhämtningslagen är det Åklagarmyndigheten på ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket som fattar beslut om inhämtning av uppgifter. Säkerhets- och integritetsskyddsnämnden ska inom en månad efter att ett ärende om inhämtning avslutats underrättas om ett beslut om inhämtning av uppgifter enligt lagen (5 § inhämtningslagen).

I förundersökningsfallen finns möjlighet för åklagare att i vissa fall besluta om tillstånd till hemliga tvångsmedel interimistiskt, i avvaktan på rättens beslut. Om åklagaren har gett ett sådant tillstånd ska denne utan dröjsmål skriftligt anmäla beslutet till rätten och ange skälen för åtgärden. Rätten ska skyndsamt pröva ärendet och om den finner att det inte finns

skäl för åtgärden ska beslutet upphävas. Om åklagarens beslut har verkställts innan rätten hunnit göra en sådan prövning och det senare visar sig att det saknats skäl för åtgärden får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av avlyssningen eller övervakningen, eller för någon annan som uppgifterna avser (27 kap. 21 a § RB).

Även enligt preventivlagen finns möjlighet till interimistiskt åklagarbeslut beträffande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning (6 a §). Betydelsen av olägenheten av att inhämta rättens tillstånd är emellertid i den bestämmelsen knuten till möjligheterna att förhindra den brottsliga verksamheten i stället för, som i förundersökningsfallen, utredningen.

Det är inte möjligt att utan domstolsprövning tillåta hemlig rumsavlyssning. Undantag gäller endast i vissa situationer om Sverige befinner sig i krig eller krigsfara. Enligt 28 § lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. gäller nämligen att om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § RB, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.

Vid prövningen av om det finns skäl att tillåta tvångsmedlet i fråga har domstolen och, i förekommande fall, åklagaren alltid att avgöra om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse. Denna proportionalitetsprincip återfinns i bl.a. 27 kap. 1 § tredje stycket RB, 5 § preventivlagen och 2 § 2 inhämtningslagen. Som redan nämnts gäller dock principen vid tillämpningen av all tvångsmedelslagstiftning.

För att hemliga tvångsmedel ska få tillåtas ställs det också upp vissa kvalificerande krav som tar sikte på behovet av åtgärden i det enskilda fallet. Det krävs att åtgärden är av synnerlig vikt för utredningen (förundersökningsfallen), är av synnerlig vikt för att förhindra brottslighet (5 § preventivlagen) alternativt att det ska föreligga synnerliga skäl för åtgärden (20 § LSU). För inhämtning av uppgifter enligt inhämtningslagen krävs att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka sådana brott som avses i den lagen.

Beslutets innehåll

Vad ett beslut om hemliga tvångsmedel ska innehålla under en förundersökning regleras i 27 kap. 21 § RB. I underrättelseverksamhet finns motsvarande regler i 8 § preventivlagen och 21 § LSU (vilken hänvisar till 27 kap. RB). I beslutet ska det anges vilken tid beslutet gäller. Tiden får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet. Om tiden löper ut krävs ett nytt beslut.

I ett tillstånd till hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation ska det anges vilket telefonnummer eller annan adress alternativt vilken elektronisk kommunikationsutrustning som tillståndet avser. Det ska också anges om åtgärden får verkställas utanför allmänt tillgängliga elektroniska kommunikationsnät. Om tillståndet gäller inhämtning av uppgifter om vilka mobila kommunikationsutrustningar

som har funnits inom ett visst geografiskt område (hemlig övervakning av elektronisk kommunikation) ska det anges vilket geografiskt område tillståndet avser.

När det gäller tillstånd till hemlig kameraövervakning ska det anges vilken plats tillståndet gäller. I ett beslut att tillåta hemlig rumsavlyssning ska det, utöver vilken plats tillståndet avser, också anges vem som är skäligen misstänkt för brottet.

I samtliga fall gäller att rätten också, när det finns skäl därtill, i övrigt ska ange villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.

Vid beslut om inhämtning av uppgifter enligt inhämtningslagen 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.

4.4.2 Skydd för vissa yrkesgrupper

Vissa personkategorier är till följd av sitt yrke undantagna från vittnesplikten under vissa förutsättningar (36 kap. 5 § andra–sjätte styckena RB). Detta gäller bl.a. advokater, präster och läkare. Dessa personer har även en priviligierad ställning vid hemlig avlyssning av elektronisk kommunikation och hemlig rumsavlyssning. Det finns nämligen särskilda bestämmelser om användningen av dessa hemliga tvångsmedel när den som tvångsmedlet riktas mot kommunicerar med någon i den nyss nämnda personkretsen (27 kap. 22 § RB). Hemlig avlyssning av elektronisk kommunikation får inte avse telefonsamtal eller andra meddelanden där någon som yttrar sig inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram. På motsvarande sätt får hemlig rumsavlyssning inte avse samtal eller annat tal där en sådan person talar. Om det under avlyssningen kommer fram att det är fråga om ett sådant samtal eller meddelande, ska avlyssningen omedelbart avbrytas och upptagningar och uppteckningar, dvs. det material där uppgifter från tvångsmedelsanvändningen finns sparat, omedelbart förstöras i de delar som de omfattas av förbud. Motsvarande bestämmelse beträffande hemlig avlyssning av elektronisk kommunikation finns i preventivlagen (11 §).

4.4.3 Skyldigheten att avbryta användningen av det hemliga tvångsmedlet

I såväl förundersöknings- som underrättelsefallen gäller att ett beslut om att tillåta ett hemligt tvångsmedel omedelbart ska upphävas om det inte längre finns skäl för beslutet. Beslutet hävs av åklagare eller rätten utom i fall enligt inhämtningslagen, där i stället den brottsbekämpande myndigheten själv ska häva beslutet (27 kap. 23 § RB, 10 § preventivlagen och 4 § inhämtningslagen). Enligt preventivlagen gäller dessutom att Polismyndigheten eller Säkerhetspolisen omedelbart ska underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.

4.4.4 Användning av överskottsinformation

Om det vid hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation eller hemlig kameraövervakning i förundersökningsfallen har kommit fram uppgifter om annat brott än det som har legat till grund för beslutet om avlyssning eller övervakning, s.k. överskottsinformation, får uppgifterna användas för att utreda brottet. En förundersökning eller motsvarande utredning om brottet får dock inledas på grund av sådana uppgifter endast om det är föreskrivet fängelse i ett år eller därutöver för brottet och det kan antas att brottet inte endast leder till böter, eller om det finns särskilda skäl. Överskottsinformation från hemlig rumsavlyssning får användas för att utreda brott endast om uppgifterna rör ett brott som hade kunnat leda till tillstånd till hemlig rumsavlyssning eller som har minst tre års fängelse i straffskalan. I annat fall får uppgifterna inte användas för brottsutredande ändamål, vare sig för att inleda en förundersökning eller som tillägg till en redan pågående förundersökning (27 kap. 23 a § RB).

I underrättelsefallen gäller delvis olika förutsättningar för användande av överskottsinformation. I samtliga fall gäller dock att uppgifter om förestående brott alltid får användas för att förhindra brott. När det gäller överskottsinformation som kommit fram vid tvångsmedelsanvändning enligt preventivlagen får sådan information användas för att utreda ett brott endast om det är fråga om ett brott som omfattas av lagen (inklusive försök, förberedelse eller stämpling till sådant brott) eller om det är fråga om ett annat brott för vilket det är föreskrivet fängelse i tre år eller däröver (12 §). Vid särskild utlänningskontroll får överskottsinformation som kommit fram vid hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation användas för att utreda ett brott (21 a §). Förundersökning eller motsvarande utredning får dock inledas på grund av dessa uppgifter endast om det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller om det finns särskilda skäl. Uppgifter som har kommit fram vid inhämtning enligt inhämtningslagen 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 beslut om att inleda en förundersökning (7 §).

Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel har i sitt slutbetänkande lämnat förslag på förändrade regler för användningen av överskottsinformation (SOU 2018:61). Betänkandet bereds i Regeringskansliet.

4.4.5 Granskning, bevarande och förstörande av insamlat material

När hemliga tvångsmedel använts ska den upptagning eller uppteckning som gjorts granskas snarast möjligt. När det är fråga om hemliga tvångsmedel under förundersökning får rätten, förundersökningsledaren eller åklagaren, alternativt sakkunnig eller annan som någon av dessa bestämt, genomföra granskningen. De delar som är av betydelse för att utreda brott ska bevaras till dess förundersökningen har lagts ned eller avslutats eller,

om åtal väckts, målet slutligt har avgjorts. I de delar som 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 (27 kap. 24 § RB).

Enligt både preventivlagen och lagen (1991:572) om särskild utlänningskontroll ska granskning av uppteckningar eller upptagningar göras snarast möjligt. Granskningen får utföras av rätten, Säkerhetspolisen, Polismyndigheten eller åklagare. Enligt preventivlagen får granskning göras även av sakkunnig eller någon annan som har anlitats i ärendet (13 § preventivlagen och 22 § LSU). Den lagen anger att upptagningar och uppteckningar, i de delar de är av betydelse för att förhindra förestående brott, ska bevaras så länge det behövs för att förhindra brott. I de delar upptagningarna och uppteckningarna innehåller sådana uppgifter om brott som enligt lagen får användas för att utreda brott ska de bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. De ska därefter förstöras (13 § preventivlagen).

Enligt lagen om särskild utlänningskontroll ska upptagningar och uppteckningar omedelbart förstöras om de innehåller något som inte är av betydelse för ändamålet med avlyssningen i denna del. I fråga om brott eller förestående brott som inte är av betydelse för ändamålet med avlyssningen gäller motsvarande bestämmelser som i förundersökningsfallen (22 § LSU).

Enligt inhämtningslagen ska uppteckningar, 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 (8 § inhämtningslagen).

4.4.6 Offentliga ombud

Offentliga ombud bevakar enskildas integritetsintressen i ärenden hos domstol om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning. Samma regler om offentliga ombud gäller för förundersökningsfallen som för underrättelsefallen (27 kap. 26–30 §§ RB, 6 § preventivlagen och 21 § LSU). Däremot finns inte några regler om offentligt ombud vid hemlig övervakning av elektronisk kommunikation. Inte heller finns krav på offentligt ombud vid tillämpning av inhämtningslagen.

Ett offentligt ombud har rätt att ta del av vad som förekommer i ärendet, yttra sig i ärendet och överklaga rättens beslut (27 kap. 26 § RB). När en ansökan eller anmälan om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning eller hemlig rumsavlyssning har kommit in till rätten ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla sammanträde. Vid sammanträdet ska åklagaren och det offentliga ombudet närvara (27 kap. 28 § RB).

Utredningen om regeländringar för vissa hemliga tvångsmedel har i sitt slutbetänkande lämnat förslag på förändringar av de offentliga ombudens roll (SOU 2018:30). Betänkandet bereds i Regeringskansliet.

4.4.7 Underrättelse till enskilda

Det finns en skyldighet att i efterhand underrätta den enskilde om att hemliga tvångsmedel har använts. I förundersökningsfallen gäller som huvudregel att den som är eller har varit misstänkt för brott ska underrättas om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning eller hemlig rumsavlyssning som han eller hon har utsatts för (27 kap. 31 § RB). Om hemlig avlyssning eller övervakning av elektronisk kommunikation har avsett ett telefonnummer, adress eller kommunikationsutrustning som innehas av någon annan än den misstänkte ska enligt huvudregeln även denna person underrättas. Om hemlig kameraövervakning eller hemlig rumsavlyssning har avsett en plats som innehas av någon annan än den misstänkte och som allmänheten inte har tillträde till, ska 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 (27 kap. 31 § RB).

Det finns dock undantag från underrättelseskyldigheten. Om det gäller sekretess enligt vissa angivna sekretessgrunder ska underrättelsen skjutas upp till dess att sekretess inte längre gäller. Om sekretessen gör att underrättelsen inte kan lämnas inom ett år från det att förundersökningen avslutades faller underrättelseskyldigheten bort. I sådana fall ska i stället Säkerhets- och integritetsskyddsnämnden underrättas, 14 b § förundersökningskungörelsen (1947:948). Ytterligare ett undantag från underrättelseskyldigheten är att underrättelse inte ska lämnas om förundersökningen angår vissa särskilt angivna brott, huvudsakligen brott mot Sveriges säkerhet (27 kap. 33 § RB).

Även preventivlagen innehåller regler om underrättelseskyldighet för de brott som huvudsakligen utreds av Polismyndigheten. Underrättelse till enskild ska lämnas så snart det kan ske efter att det ärende som åtgärden vidtogs i avslutades. Om det gäller sekretess enligt vissa angivna sekretessgrunder ska underrättelsen skjutas upp till dess att sekretess inte längre gäller. Om sekretessen gör att underrättelsen inte kan lämnas inom ett år från det att det ärende i vilket åtgärden vidtogs avslutades bortfaller underrättelseskyldigheten (18 § andra stycket). Underrättelse ska i sådant fall i stället lämnas till Säkerhets- och integritetsskyddsnämnden enligt förordningen (2007:1144) om fullgörande av underrättelseskyldighet enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

För åtgärder som vidtas enligt lagen om särskild utlänningskontroll gäller ingen underrättelseskyldighet. Detta har motiverats med att det brott som lagen avser är terroristbrott och att det i likhet med vad som gäller enligt rättegångsbalken inte bör krävas underrättelser i sådana fall. Dessutom kan underrättelse i praktiken inte lämnas så länge som den avlyssnade eller övervakade personen finns kvar i landet och efter utvisning är det knappast möjligt att lämna några underrättelser, se propositionen Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m. (prop. 2006/07:133 s. 52).

I fråga om inhämtning av uppgifter om elektronisk kommunikation enligt inhämtningslagen finns ingen bestämmelse om underrättelse till

enskild. Däremot ska Säkerhets- och integritetsskyddsnämnden underrättas om varje beslut om inhämtning senast en månad efter att inhämtningen avslutats (5 §).

4.4.8 Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden ska bidra till att värna rättssäkerheten och skyddet för den personliga integriteten i förhållande till den brottsbekämpande verksamheten. Nämndens uppgifter framgår av lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet och förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden. Nämnden ska bl.a. utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och därmed sammanhängande verksamhet. Tillsynen ska särskilt syfta till att säkerställa att verksamheten bedrivs i enlighet med lag eller annan författning och ska utövas genom inspektioner och andra undersökningar.

Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan författning avhjälps. Nämnden är också skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel samt om användningen av tvångsmedlen och därmed sammanhängande verksamhet har skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde om att kontrollen har utförts.

Som framgår i föregående avsnitt ska Säkerhets- och integritetsskyddsnämnden få underrättelse från åklagaren i de fall underrättelse till enskild har underlåtits på grund av sekretess. Säkerhets- och integritetsskyddsnämnden ska också underrättas om beslut om inhämtning enligt inhämtningslagen (5 §).

4.5 Beslag och husrannsakan

I följande två avsnitt ges en översikt över dagens regelverk om beslag och husrannsakan. Det ska dock noteras att Beslagsutredningen har lämnat tämligen omfattande förslag till förändringar av regelverket i ett betänkande (SOU 2017:100). Förslagen bereds i Regeringskansliet.

4.5.1 Beslag

Beslag är ett straffprocessuellt tvångsmedel som innebär att en brottsbekämpande myndighet tillfälligt tar hand om annans egendom. Bestämmelser om beslag finns i 27 kap. RB. Det finns inga regler som tillåter beslag i underrättelseverksamhet.

Beslag får göras för olika ändamål. För det första får föremål som skäligen kan antas ha betydelse för utredning om brott tas i beslag (bevisbeslag). Det avser föremål som kan ha bevisvärde antingen för den fortsatta utredningen eller för det slutliga avgörandet av målet. Syftet med beslaget kan till exempel vara att avgöra om en gärning är brottslig, försöka knyta en gärningsman till brottet eller belysa gärningsmannens uppsåt eller

brottets svårhet. En annan typ av beslag avser föremål som skäligen kan antas vara avhänt någon genom brott (återställandebeslag). Syftet med ett sådant beslag är att återställa det beslagtagna föremålet till den rättmätige ägaren. Ett tredje ändamål med beslag är att säkerställa ett framtida förverkande av föremål på grund av brott (förverkandebeslag). Sådana beslag tar endast sikte på sakförverkande och får användas för att till exempel säkra förverkande av sådant som har varit föremål för brott eller som använts som hjälpmedel vid brott. Slutligen får beslag göras i syfte att utreda frågan om s.k. utvidgat förverkande enligt 36 kap. 1 b § brottsbalken. Eftersom ett sådant beslag syftar till att säkra föremål och handlingar som behövs för att utreda frågan är detta en form av bevisbeslag.

Föremål inklusive skriftliga handlingar får tas i beslag. Beslag får i allmänhet göras oberoende av brottets beskaffenhet. Beslag av försändelser hos ett post- eller telebefordringsföretag eller beslag för utredning om förverkande av utbyte av brottslig verksamhet förutsätter dock att brottet är av viss svårhetsgrad (27 kap. 3 § RB). Att föremål ägs av någon annan än den som har föremålet i sin besittning hindrar inte att det tas i beslag. Beslag förutsätter inte heller att det finns någon som kan misstänkas för det brott som har föranlett beslaget. Därför kan beslag riktas mot såväl misstänkta som andra. Beslag får dock endast beslutas om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse (27 kap. 1 § RB).

I 27 kap. 2 § RB regleras det s.k. beslagsförbudet. Det innebär att en skriftlig handling inte får tas i beslag om den kan antas innehålla uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § RB inte får höras som vittne om och handlingen innehas av honom eller henne eller av den som tystnadsplikten gäller till förmån för. Högsta domstolen har i rättsfallet NJA 2015 s. 631 slagit fast att beslagsförbudet omfattar även annan information än skrift och andra bärare av information än papper.

4.5.2 Husrannsakan

Regler om husrannsakan finns i 28 kap. RB. Om det finns anledning att anta att ett brott, på vilket fängelse kan följa, har begåtts får husrannsakan företas i hus, rum eller slutet förvaringsställe för att söka efter föremål som kan tas i beslag eller i förvar eller annars för att utröna omständigheter som kan vara av betydelse för utredning om brottet eller om förverkande av utbyte av brottslig verksamhet. Hos annan än den som skäligen kan misstänkas för brottet får husrannsakan företas bara om brottet har begåtts hos honom eller henne eller om den misstänkte har gripits där eller om det annars finns synnerlig anledning att det kommer att anträffas föremål som kan tas i beslag eller i förvar eller att annan utredning om brottet eller om förverkande av utbyte av brottslig verksamhet kan vinnas (28 kap. 1 § RB).

Det är i normalfallet undersökningsledaren eller åklagaren som förordnar om husrannsakan men även rätten får besluta i frågan. Om det är fara i dröjsmål får en polisman företa husrannsakan utan sådant förordnande (28 kap. 4 § RB). Tjänstemän vid Tullverket och Kustbevakningen har motsvarande befogenhet, 26 § lagen (2000:1225) om straff för smuggling.

Ett beslut om husrannsakan ska föregås av en proportionalitetsavvägning (28 kap. 3 a § RB).

Reglerna om husrannsakan och beslag hör samman på så sätt att en husrannsakan ofta är nödvändig för att möjliggöra ett beslag. Husrannsakan i beslagssyfte förutsätter också att det sökta föremålet kan tas i beslag.

Till skillnad från beslag finns det regler som tillåter husrannsakan utanför en förundersökning, se 19 § lagen om särskild utlänningskontroll.

4.6 Annan relevant lagstiftning

4.6.1 Lagen (2000:562) om internationell rättslig hjälp i brottmål

I lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB) finns bestämmelser om att svenska myndigheter, främst åklagare och domstolar, kan bistå andra stater vid utredning om och lagföring för brott (1 kap. 4 §). Lagen innehåller även bestämmelser om att svenska åklagare eller domstolar kan begära bistånd i en förundersökning eller rättegång (1 kap. 7 §).

I 1 kap. 2 § räknas upp alla de åtgärder som omfattas av lagen, t.ex. förhör under förundersökning, beslag och olika hemliga tvångsmedel. En uttalad målsättning med lagen är att svenska åklagare och domstolar ska kunna lämna rättslig hjälp till utländska myndigheter med alla de åtgärder som kan vidtas vid en svensk förundersökning eller rättegång, se propositionen Internationell rättslig hjälp i brottmål (prop. 1999/2000:61 s. 79–80). När ett nytt tvångsmedel införts i nationell rätt har det också införts motsvarande bestämmelser i lagen om internationell rättslig hjälp i brottmål, se propositionen Hemlig rumsavlyssning (prop. 2005/06:178 s. 89).

En annan grundsyn i lagen är att rättslig hjälp i Sverige, bl.a. med hemliga tvångsmedel, lämnas under de förutsättningar som gäller för motsvarande åtgärd i en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning (2 kap. 1 §). När det gäller hemliga tvångsmedel ställs därutöver upp ett krav på dubbel straffbarhet (2 kap. 2 §), dvs. att den straffbara gärning som biståndet avser även ska vara en straffbar gärning i Sverige. En svensk åklagare kan på motsvarande sätt begära bistånd i en annan stat, bl.a. med hemliga tvångsmedel.

I 4 kap. 25–28 b §§ LIRB finns detaljerade bestämmelser om handläggningen av dessa ärenden och verkställigheten av ett hemligt tvångsmedel, t.ex. om granskning och underrättelse till enskild vid verkställighet i Sverige och om att åklagaren i vissa fall måste inhämta rättens tillstånd till åtgärden.

Mot bakgrund av Europeiska unionens konvention om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater från 2000 (SÖ 2005:42) finns vissa bestämmelser i lagen som rör hemliga tvångsmedel, men som avviker från det traditionella sättet att samarbeta när en stat ansöker om hjälp i en annan stat som efter en prövning verkställer åtgärden där. Dessa bestämmelser gäller endast gentemot en medlemsstat i Europeiska unionen, Island eller Norge.

En sådan särreglering är tekniskt bistånd med hemlig avlyssning eller övervakning av elektronisk kommunikation. Tekniskt bistånd innebär att avlyssningen eller övervakningen görs gentemot en person som finns i en

annan stat än den som bistår med avlyssningen eller övervakningen och då meddelandena eller uppgifterna om meddelandena, under betryggande former, omedelbart kan överföras till den ansökande staten. Det kan t.ex. röra sig om svenska myndigheter som bistår tyska myndigheter med att avlyssna någon som finns i Danmark. För ett sådant bistånd gäller särskilda förutsättningar (4 kap. 25 b § andra stycket 3 och fjärde stycket). Omedelbar överföring av meddelanden eller uppgifter om meddelanden kan också äga rum när den som avlyssnas eller övervakas finns i Sverige (4 kap. 25 a §).

En annan särreglering i lagen gäller tillstånd till gränsöverskridande hemlig avlyssning eller övervakning av elektronisk kommunikation (4 kap. 26 a–c §§). Det är i egentlig mening inte fråga om att något bistånd lämnas, utan att en tillåtelse lämnas till att en stat avlyssnar eller övervakar en person som finns i den stat som lämnar tillståndet. Det kan t.ex. röra sig om att svenska myndigheter tillåter att danska myndigheter avlyssnar någon som finns i Sverige. I dessa fall gäller samma förutsättningar som för motsvarande åtgärd i rättegångsbalken (4 kap. 26 a § tredje stycket).

På motsvarande sätt kan en svensk åklagare ansöka om tekniskt bistånd med eller tillstånd till gränsöverskridande hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. I 5 kap. 2 § LIRB finns bestämmelser om att rättslig hjälp får förenas med villkor som är påkallade med hänsyn till enskilds rätt eller som när nödvändiga från allmän synpunkt. Det kan bl.a. röra sig om villkor som gäller om hur avlyssnat eller övervakat material får användas efter det att materialet har överlämnats till den ansökande staten (prop. 1999/2000:61 s. 147).

4.6.2 Lagen (2017:1000) om en europeisk utredningsorder

Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området ersätter samarbetet mellan EU:s medlemsstater som tidigare skedde enligt bestämmelserna om internationell rättslig hjälp i brottmål (se föregående avsnitt). Direktivet genomfördes i huvudsak genom lagen (2017:1000) om en europeisk utredningsorder. Lagen gäller i förhållande till alla EU-medlemsstater utom Danmark och Irland (1 kap. 2 §). Gentemot dessa två stater tillämpas lagen om internationell rättslig hjälp i brottmål. En europeisk utredningsorder innebär – något förenklat – att en åklagare eller domstol i den stat där brottsutredningen eller rättegången pågår beslutar om att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning.

I lagen räknas upp vilka utredningsåtgärder som omfattas av lagens tillämpningsområde, bl.a. hemliga tvångsmedel (1 kap. 4 §). En allmän utgångspunkt i direktivet och lagen är att en medlemsstat endast kan utfärda en utredningsorder eller är skyldig att erkänna och verkställa en sådan order om den åtgärd som avses är tillgänglig i den aktuella medlemsstaten. Svenska myndigheter är således inte skyldiga att erkänna och verkställa hemliga tvångsmedel som inte är tillgängliga i Sverige, men kan inte heller själva utfärda en utredningsorder avseende ett sådant tvångsmedel.

En europeisk utredningsorder avseende hemliga tvångsmedel får utfärdas i Sverige av åklagare om de förutsättningar som gäller för att vidta utredningsåtgärden under en svensk förundersökning är uppfyllda och åtgärden är proportionerlig (2 kap. 1 och 3 §§). Dessutom krävs att domstol har lämnat tillstånd att utfärda ordern. Åklagaren har dock viss möjlighet att fatta interimistiska beslut. När det gäller hemlig avlyssning eller övervakning av elektronisk kommunikation kan en utredningsorder utfärdas för avlyssning eller övervakning i Sverige eller i en annan medlemsstat, såväl i den medlemsstat till vilken ordern översänds som i en tredje medlemsstat (2 kap. 17 §). Liksom i lagen om internationell rättslig hjälp i brottmål kan det bli aktuellt med omedelbart överförande av meddelanden eller uppgifter om meddelanden (även om begreppet tekniskt bistånd inte används). I de fall ett sådant överförande är möjligt och upptagningen eller upptecknigen sker i Sverige tillämpas 27 kap. 31–33 §§ rättegångsbalken om underrättelse till enskild. Vid samtliga hemliga tvångsmedel, även hemlig kameraövervakning och hemlig rumsavlyssning, tillämpas 27 kap. 22–24 §§ samma balk om t.ex. granskning.

När en europeisk utredningsorder avseende hemliga tvångsmedel har utfärdats i en annan medlemsstat och sänts över till Sverige är utgångspunkten att den ska erkännas och verkställas här (3 kap. 1 §). Det krävs dock att den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och att övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning är uppfyllda. En utredningsorder behöver ska inte heller erkännas och verkställas om en vägransgrund i 3 kap. 5–7 §§ är tillämplig. En utredningsorder avseende hemliga tvångsmedel handläggs av åklagare, men domstol prövar om utredningsordern ska erkännas och verkställas (3 kap. 8 och 9 §§). Åklagaren har viss möjlighet att fatta interimistiska beslut om erkännande och verkställighet (3 kap. och 10 §). Om utredningsordern kan erkännas och verkställas i Sverige, ska beslut meddelas om att verkställighet ska äga rum, en s.k. verkställbarhetsförklaring (3 kap. 19 §). För verkställigheten av utredningsordern finns särskilda bestämmelser om hemliga tvångsmedel i 3 kap. 34–37 §§.

Liksom i lagen om internationell rättslig hjälp i brottmål finns, beträffande hemlig avlyssning och övervakning av elektronisk kommunikation, möjlighet till omedelbar överföring till den andra staten. Det uppställs också en möjlighet till upptagning eller upptecknig i Sverige av meddelanden eller uppgifter om meddelanden. Dessa överlämnas sedan enligt vad som föreskrivs i särskilda bestämmelser (3 kap. 38 och 39 §§).

Det finns också särskilda regler om underrättelse till annan medlemsstat och om underrättelse från annan medlemsstat till Sverige när hemlig avlyssning eller övervakning av elektronisk kommunikation kan ske på den andra statens territorium utan bistånd från denna (4 kap. 12–15 §§).

4.6.3 Lagen (2003:389) om elektronisk kommunikation

Lagen (2003:389) om elektronisk kommunikation (LEK) syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster.

Allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster får endast tillhandahållas efter anmälan till tillsynsmyndigheten (Post- och telestyrelsen) (2 kap. 1 § LEK). Som utgångspunkt gäller att den som bedriver sådan anmälningspliktig verksamhet ska utplåna eller avidentifiera lagrade eller på annat sätt behandlade trafikuppgifter som avser användare som är fysiska personer eller som avser abonnenter, när uppgifterna inte längre behövs för att överföra ett elektroniskt meddelande (6 kap. 5 § LEK). Med trafikuppgifter avses uppgifter som behandlas i syfte att befordra elektroniska meddelanden via ett elektroniskt kommunikationsnät eller för att fakturera meddelandena. Ett viktigt undantag till regeln om utplånande och avidentifierande är att detta inte gäller för elektroniska meddelanden som omfattas av beslut om hemlig avlyssning eller övervakning av elektronisk kommunikation, tekniskt bistånd med sådan avlyssning eller övervakning eller inhämtning av uppgifter enligt inhämtningslagen (6 kap. 8 § LEK).

Lagen innehåller också bestämmelser om lokaliseringsuppgifter som inte är trafikuppgifter. Sådana uppgifter får som utgångspunkt behandlas endast sedan de har avidentifierats eller användaren eller abonnenten gett sitt samtycke till behandlingen (6 kap. 9 §). Även beträffande dessa uppgifter finns ett undantag som innebär att de får behandlas utan nyss nämnda begränsning om de omfattas av beslut om inhämtning av uppgifter enligt 27 kap. RB eller inhämtningslagen (6 kap. 10 a §).

Vid verkställighet av hemlig avlyssning eller övervakning av elektronisk kommunikation finns möjlighet för de brottsbekämpande myndigheterna att få information från operatörer och andra som tillhandahåller tjänster på området. Enligt 6 kap. 19 § LEK ska nämligen vissa verksamheter bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs. De verksamheter som avses är för det första tillhandahållande av ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program som avses i 1 kap. 2 § yttrandefrihetsgrundlagen. Vidare avses tillhandahållande av tjänster inom ett allmänt kommunikationsnät vilka består av en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet, som medger funktionell tillgång till internet. Slutligen avses också tillhandahållande av en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

Flera av reglerna i 6 kap. LEK genomför bestämmelser i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), vilket antogs bl.a. för att säkerställa full respekt för rättigheter enligt artikel 7 och 8 i EU:s rättighetsstadga. Direktivet är föremål för översyn inom EU.

4.6.4 Sekretessfrågor

Enligt 2 kap. 1 § tryckfrihetsförordningen har, till främjande av ett fritt meningsutbyte och en fri och allsidig upplysning och ett fritt konstnärligt

skapande, var och en rätt att ta del av allmänna handlingar. Rätten får dock begränsas bl.a. om det krävs med hänsyn till intresset att förebygga eller beivra brott och skyddet för enskildas personliga eller ekonomiska förhållanden (2 kap. 2 § första stycket tryckfrihetsförordningen). Regler om sådana begränsningar finns i offentlighets- och sekretesslagen. Offentlighets- och sekretesslagen innehåller bestämmelser som är av särskild betydelse när reglerna om hemliga tvångsmedel ska beskrivas.

Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs (18 kap. 1 § OSL). I 18 kap. 2 § OSL regleras sekretessen i de brottsbekämpande myndigheternas underrättelseverksamhet. För uppgift som hänför sig till sådan verksamhet gäller sekretess bl.a. om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. För uppgifter i verksamhet som avser rättsligt samarbete på begäran av en annan stat eller en mellanfolklig domstol, gäller sekretess bl.a. för uppgift som hänför sig till en angelägenhet som angår tvångsmedel, om det kan antas att det varit en förutsättning för den andra statens eller den mellanfolkliga domstolens begäran att uppgiften inte skulle röjas (18 kap. 17 § OSL).

I 35 kap. OSL regleras sekretess till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott, m.m. Av 1 § följer bl.a. att sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen.

Det finns bestämmelser i särskilda lagar som reglerar tystnadsplikt. Av intresse i detta sammanhang är att det i 6 kap. 21 § LEK finns en reglering om tystnadsplikt för den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av en uppgift som hänför sig till angelägenhet som avser användning av hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § RB eller tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § LIRB.

4.7 Användningen av hemliga tvångsmedel

Varje år redovisar regeringen användningen av hemliga tvångsmedel i en skrivelse till riksdagen. Skrivelsen baseras på Åklagarmyndighetens årliga redovisning, vilken myndigheten sammanställer tillsammans med Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket.

Redovisningen innehåller bl.a. uppgifter om antalet meddelade tillstånd om hemliga tvångsmedel, hur många personer som varit föremål för åtgärder och om uppgifterna som kommit fram gjort nytta. Det framgår av redovisningarna att hemliga tvångsmedel används i en mycket liten del av alla förundersökningar.

Av regeringens redovisning av användningen av hemliga tvångsmedel under 2017 (skr. 2018/19:19) och Åklagarmyndighetens redovisning av användningen av vissa hemliga tvångsmedel under 2017 kan bl.a. följande utläsas:

- Hemlig avlyssning av elektronisk kommunikation omfattade 1 378 personer, vilket är en ökning från 2016 då 1 253 personer avlyssnades. Under 2017 beviljades 4 465 tillstånd till hemlig avlyssning av elektronisk kommunikation.
- Hemlig övervakning av elektronisk kommunikation omfattade 2 162 personer, vilket är en minskning från 2016 då 2 290 personer övervakades. Under 2017 beviljades 7 991 tillstånd till hemlig övervakning av elektronisk kommunikation.
- Hemlig kameraövervakning omfattade 152 personer, vilket är en ökning från 2016 då 117 personer övervakades. Under 2017 beviljades 153 tillstånd till hemlig kameraövervakning.
- Hemlig rumsavlyssning omfattade 63 personer. Det är en ökning från 2016 då motsvarande siffra var 55 personer. Under 2017 beviljades 77 tillstånd till hemlig rumsavlyssning.
- Under 2017 fattades 595 beslut om inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet av Polismyndigheten och Tullverket. Det är en minskning från 2016 då 688 beslut fattades. Säkerhetspolisen fattade under 2017 163 beslut av motsvarande slag.
- Polismyndigheten har under 2017 inte använt hemliga tvångsmedel enligt preventivlagen.
- I Säkerhetspolisens verksamhet har det fattats 309 beslut om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning.

En viktig faktor för rättfärdigandet av hemliga tvångsmedel är att de ska göra nytta. Med nytta menas i det här sammanhanget bl.a. och framför allt att uppgifterna har bidragit till att förundersökningen kunnat drivas framåt på ett bättre sätt än vad som annars varit möjligt. Även om det ska noteras att ett tvångsmedel kan ha flera olika nyttoparametrar anges bl.a. följande om nyttan i 2017 års redovisning.

- Hemlig avlyssning av elektronisk kommunikation har i 50 procent av fallen utgjort underlag i förhörssituation och i 54 procent av fallen lett till att effektiv spaning kunnat genomföras. I 35 procent av fallen har uppgifterna bidragit till att den misstänkte kunnat åtalas och i 16 procent av fallen att den misstänkte kunnat avföras från utredningen.
- Nyttan av hemlig övervakning av elektronisk kommunikation redovisas genom anonymiserade exempel från tillämpningen. Där framgår att det i åtskilliga fall lett till att en gärningsman bl.a. kunnat knytas till en brottsplats och i andra fall att en misstänkt kunnat avföras från utredningen.

– Hemlig kameraövervakning har i 48 procent av fallen gjort underlag i förhörssituation och i 80 procent av fallen medfört att effektiv spaning har kunnat genomföras. I 38 procent av fallen har uppgifterna bidragit till att den misstänkte kunnat åtalas och i 16 procent av fallen att den misstänkte kunnat avföras från utredningen.
– Hemlig rumsavlyssning har i 27 procent av fallen utgjort underlag i förhörssituation och i 67 procent av fallen medfört att effektiv spaning har kunnat bedrivas. I 17 procent av fallen har uppgifterna bidragit till att den misstänkte kunnat åtalas och i 33 procent av fallen att den misstänkte kunnat avföras från utredningen.
– Nyttan av inhämtning av uppgifter i underrättelseverksamhet redovisas genom anonymiserade exempel där det framgår att brottslig verksamhet i åtskilliga fall kunnat avvärjas och kriminella nätverk kunnat kartläggas.

5 Vad är hemlig dataavläsning?

5.1.1 Tidigare utredningar

Frågan om hemlig dataavläsning aktualiserades för första gången när Beredningen för rättsväsendets utveckling (BRU) lämnade sitt delbetänkande Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38). I betänkandet föreslogs bland annat att hemlig dataavläsning skulle införas som ett hemligt tvångsmedel i Sverige. I remissförfarandet riktades dock viss kritik mot förslaget om hemlig dataavläsning och det ledde inte till lagstiftning.

Sju år senare lämnade Utredningen om vissa hemliga tvångsmedel betänkandet Hemliga tvångsmedel mot allvarliga brott (SOU 2012:44). I betänkandet gjordes bland annat utvärderingar av vissa tidsbegränsade lagar på området för hemliga tvångsmedel. Av betänkandet framgår att de brottsbekämpande myndigheterna framhållit att det finns stora behov av att införa regler om hemlig dataavläsning. Det ingick inte i utredningens uppdrag att lämna förslag om lagstiftning i frågan, men utredningen påpekade vikten av att saken skulle utredas.

Regeringen har även i Den svenska strategin mot terrorism särskilt framhållit att de brottsbekämpande myndigheterna måste ges förutsättningar att, trots den tekniska utvecklingen, kunna upprätthålla förmågan att inhämta information (skr. 2014/15:146 s. 16–17).

5.1.2 Begreppet hemlig dataavläsning

Det finns inte någon legaldefinition av hemlig dataavläsning. Följande definition har dock ingått i utredningens direktiv, som ligger till grund för utredningens överväganden och för denna lagrådsremiss.

> Hemlig dataavläsning är en metod för de brottsbekämpande myndigheterna att med någon form av tekniskt hjälpmedel i hemlighet bereda sig tillgång till en dator eller annan teknisk utrustning som kan användas

för kommunikation och därigenom få besked om hur utrustningen används eller har använts och vilken information som finns i den.

Metoden för hemlig dataavläsning kan alltså sägas innebära två delar, dels att den brottsbekämpande myndigheten bereder sig tillgång till teknisk utrustning som kan användas för kommunikation, dels att myndigheten tar del av uppgifter som finns i utrustningen. De uppgifter som hemlig dataavläsning är tänkta att komma åt finns alltså i den tekniska utrustningen, t.ex. i en mobiltelefon eller en dator. Det skiljer sig från vad som är fallet vid hemlig avlyssning eller övervakning av elektronisk kommunikation, där uppgifterna hämtas in på väg till eller från någons tekniska utrustning. Det skiljer sig också från hemlig rumsavlyssning och hemlig kameraövervakning, där uppgifterna hämtas in genom utrustning som tillhör och monteras av de brottsbekämpande myndigheterna.

5.1.3 Uppgifter som hemlig dataavläsning skulle kunna ge tillgång till

Hemlig dataavläsning skulle i dagsläget kunna ge de brottsbekämpande myndigheterna tillgång till flera olika typer av uppgifter, däribland sådana som redan i dag kan hämtas in genom tvångsmedelsanvändning. Nedan följer exempel på uppgifter som hemlig dataavläsning skulle kunna ge tillgång till:

1. innehållet i telefonsamtal och videosamtal, såväl vanliga mobilsamtal som samtal via särskilda program eller appar, även om de är krypterade
2. innehållet i e-postmeddelanden och andra meddelanden
3. innehållet på de webbsidor som den person åtgärden riktas mot besöker samt uppgifter om personens aktiviteter på dessa sidor
4. uppgifter om var den person åtgärden riktas mot befinner sig, t.ex. efter aktivering av en mobiltelefons GPS-funktion
5. uppgifter om vad den person åtgärden riktas mot gör, vilka denne umgås med, vilken plats han eller hon är på samt (när det inte är känt vem den misstänkte är) identifiering av denne, t.ex. efter aktivering av den tekniska utrustningens kamerafunktion.
6. innehållet i samtal, t.ex. efter aktivering av den tekniska utrustningens mikrofon
7. kontaktuppgifter till samtliga kontakter som finns lagrade på den tekniska utrustning som åtgärden riktas mot
8. allt innehåll, t.ex. fotografier, dokument och andra filer, inloggningsuppgifter och program, som finns lagrade på den tekniska utrustning som åtgärden riktas mot
9. uppgifter om lösenord, både till den tekniska utrustningen och till olika sociala nätverk, e-posttjänster samt andra forum
10. uppgifter om var, när och hur den tekniska utrustningen används och har använts.

Redan i dag kan de brottsbekämpande myndigheterna få tillstånd att hämta in många av de uppgifter som skulle kunna hämtas in genom hemlig data-

avläsning. I många fall motsvaras emellertid inte rätten att hämta in uppgifterna av en faktisk möjlighet att göra så. Det beror till stor del på att internetbaserad kommunikation allt oftare har krypterat innehåll (t.ex. samtal och meddelanden via vanligt förekommande mobiltelefonappar som Whatsapp, Imessage eller Facetime). Meddelanden och samtal som de brottsbekämpande myndigheterna i och för sig har rätt att lyssna av enligt ett tillstånd till hemlig avlyssning av elektronisk kommunikation kan därför inte fångas upp i läsbart eller avlyssningsbart skick. Därför kan det sägas att myndigheterna har rättslig men inte alltid faktisk tillgång till dessa uppgifter.

5.2 Hur kan hemlig dataavläsning verkställas?

Utredningen redogör för att verkställigheten av hemlig dataavläsning kan delas upp i fem faser, nämligen kartläggning och planering, intrång, installation, avläsning och avslutning.

Kartläggning och planering

För att hemlig dataavläsning ska kunna ge tillgång till de uppgifter som eftersöks måste den verkställande brottsbekämpande myndigheten ha skaffat sig kunskaper om målpersonen. I första hand syftar denna kartläggning till att identifiera vilken typ av teknisk utrustning (målobjekt) som målpersonen använder eftersom åtgärden ska riktas mot målobjektet. Målobjektet kan vara både fysiskt (t.ex. en dator eller mobiltelefon) och immateriellt (t.ex. ett e-postkonto, en app eller ett program). Kartläggningen av målobjektet uppvisar i alla delar stora likheter med traditionellt inre och yttre polisiärt spaningsarbete.

Intrång

När kartläggning och planering genomförts och tillstånd från domstol har inhämtats kan den praktiska verkställigheten inledas. Där ska myndigheten identifiera det aktuella it-systemets sårbarheter, alltså omständigheter som gör det känsligt för angrepp. Det kan röra sig om både tekniska brister, såsom bristfälliga och osäkra system och mänskliga svagheter, såsom slarv och tanklöshet.

Genom en attackmetod (s.k. exploit) går det att utnyttja en sårbarhet i ett datorsystem för att komma åt skyddad information. Begreppet exploit är ett samlingsnamn som används om själva attacken, metoden eller programmet som används samt sårbarheten som angriparen drar fördel av. Det kan vara t.ex. att logga in på en annan persons e-postkonto med dennes inloggningsuppgifter eller förmå användaren att ladda ned en skadlig programkod.

En förutsättning för en lyckad intrångsfas är alltså att det finns en sårbarhet som kan utnyttjas för intrång. Hemlig dataavläsning skulle kunna verkställas utan intrång i själva kommunikationssystemet genom att använda särskild hårdvara på eller vid teknisk utrustning för att t.ex. registrera knapptryckningar som sedan skickas till eller samlas in av den brottsbekämpande myndigheten. Det kräver dock obemärkt fysisk tillgång till utrustningen.

Installation

Om den brottsbekämpande myndigheten redan har tillgång till den misstänktes inloggningsuppgifter till t.ex. ett e-postkonto eller socialt medium och det är informationen som finns där som efterfrågas behövs det inte vidtas fler åtgärder. Ibland är det dock nödvändigt att installera hårdvara eller programvara i en utrustning. Förutom själva programvaran som ska installera det tekniska hjälpmedlet krävs ett program som kan läsa av uppgifterna som myndigheten ska komma åt. Programmen kommer att se olika ut beroende på förutsättningarna i det enskilda fallet. När det är fråga om installation av en hårdvara är svårigheten med installationen att undvika att utrustningen eller den som installerar den upptäcks.

Avläsning

Avläsningsfasen består av insamlingen av den information som myndigheten efterfrågar. Om den känner till nödvändiga lösenord till exempelvis ett användarkonto består avläsningen av att ta del av de e-postmeddelanden som är av vikt för utredningen. Detta kan göras i myndighetens lokaler. När avläsning gjorts med programvara som installerats i den misstänktes utrustning kan uppgifterna skickas elektroniskt till myndigheten, varför den även då kan sköta avläsningen i sina lokaler. I förekommande fall krävs att myndigheten har program som omvandlar uppgifterna till läsbar information. I vissa fall kommer det inte att vara möjligt att hämta in uppgifterna löpande på distans. Då är avläsning möjlig först när den utrustning som använts har avinstallerats och återförts till myndigheten.

Utredningen redogör för att Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket redan i dag har en gemensam struktur för bearbetning av den information som hämtas in med hemliga tvångsmedel. Den gemensamma systemlösningen finns inom ramen för Samordnad Teknisk Inhämtning (STI) där data från den hemliga tvångsmedelsanvändningen tas omhand och sedan fördelas till den verksamhetsgren inom respektive myndighet som ska ha den. Samarbetet inom STI bedöms av myndigheterna kunna tillgodose även verkställighet och insamling av uppgifter från hemlig dataavläsning.

Avslutning

När verkställigheten har avslutats ska den teknik som använts tas bort eller göras obrukbar. Den brottsbekämpande myndigheten ska då hämta tillbaka utrustningen, eller avaktivera, avinstallera, tidsbegränsa eller på annat sätt utesluta möjligheten att fortsätta nyttja det tekniska hjälpmedlet. Hur det går till beror på vilken teknik som har valts och vilka resurser som krävs.

5.2.1 Varför används inte hemlig dataavläsning redan?

Enligt 2 kap. 6 § första stycket regeringsformen är var och en gentemot det allmänna skyddad mot bl.a. husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Enligt andra stycket är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan

samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Dessa rättigheter får endast begränsas genom lag och endast under vissa villkor (avsnitt 4.2).

Det finns i dag inte något tydligt lagstöd för att använda hemlig dataavläsning. Användning av metoden skulle med dagens reglering kunna innebära ett dataintrång. Av 4 kap. 9 c § första stycket brottsbalken framgår nämligen att den som olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift kan dömas för detta brott. För dataintrång kan också dömas den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift. Straffansvar för dataintrång förutsätter således att åtgärden är olovlig. Det innebär att en åtgärd som sker i enlighet med gällande rätt inte är straffbar. Om befintlig lagstiftning ger stöd för en viss åtgärd kan åtgärden alltså inte utgöra dataintrång. Det finns därför skäl att närmare granska de bestämmelser och förarbeten som sätter gränserna för befintliga hemliga tvångsmedel.

Enligt 27 kap. 18 § RB innebär hemlig avlyssning av elektronisk kommunikation 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. Bestämmelsens ordalydelse ger ingen ledning om på vilka sätt åtgärden får verkställas. Av 27 kap. 25 § första stycket RB framgår emellertid att 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.

Regleringen i 27 kap. 25 § RB kom dock inte i första hand till för att klargöra de brottsbekämpande myndigheternas befogenheter utan för att ålägga privata aktörer på telemarknaden att bistå de brottsbekämpande myndigheterna vid verkställighet av hemliga tvångsmedel, vilket framgår av propositionen om en telelag och en förändrad verksamhetsform för Televerket, m.m. (prop. 1992/93:200 s. 258–261). Bestämmelsen ändrades några år senare. I propositionen Hemlig teleavlyssning och hemlig teleövervakning uttalade regeringen dessutom att det inte råder något tvivel om att verkställighet med hjälp av datorprogram omfattas av uttrycket tekniskt hjälpmedel (prop. 1994/95:227 s. 29).

Det går att hävda att tekniken för hemlig dataavläsning (t.ex. installation av programvara i en telefon eller modifiering av ett datorprogram i en dator) skulle kunna vara tillåten vid verkställighet av hemlig avlyssning eller övervakning av elektronisk kommunikation genom dagens reglering. En sådan tolkning kan emellertid ifrågasättas eftersom den ovan nämnda ändringen i rättegångsbalken tillkom i andra syften än för att tillåta tekniken för hemlig dataavläsning.

Sammanfattningsvis utesluter alltså inte dagens lagstiftning att verkställighet av hemlig avlyssning av elektronisk kommunikation genomförs genom sådan teknik som kan användas för hemlig dataavläsning. I ljuset av tidigare förarbetsuttalanden framstår dock en sådan verkställighetsåtgärd som tveksam. Regelverket bör tolkas med försiktighet, vilket talar för att åtgärder som utgör hemlig dataavläsning kan vidtas endast om regleringen uttryckligen tillåter dem.

5.3 Hemlig dataavläsning i några nordiska länder

I flera andra länder finns lagstiftning som möjliggör hemlig dataavläsning eller en motsvarighet till åtgärden. Danmark var det första av de nordiska länderna att införa tvångsmedlet 2002 när en regel om ”dataaflæsning” infördes i ”retsplejeloven”. Enligt bestämmelsen får brottsbekämpande myndigheter avläsa upplysningar i ett informationssystem. Med informationssystem förstås datorer eller andra databehandlingsanläggningar, t.ex. vissa mobiltelefoner och elektroniska kalendrar. Både program- och hårdvara kan användas för att genomföra avläsningen. För att dataavläsning ska få användas krävs att det finns bestämd grund att anta att informationssystemet används av en misstänkt i samband med en planlagd eller begången brottslig handling. Det krävs vidare att det rör sig ett brott som kan bestraffas med fängelse i sex år eller mer eller att det rör ett särskilt utpekat brott som t.ex. landsförräderi eller terroristbrott. Åtgärden måste dessutom antas vara av avgörande betydelse för utredningen för att kunna tillåtas. Det går inte att använda sig av dataavläsning i underrättelseverksamhet.

Även i Finland finns lagstiftning, bland annat i tvångsmedelslagen och polislagen, som i delar motsvarar hemlig dataavläsning. Det finns dock inte något tvångsmedel som ensamt motsvarar hemlig dataavläsning. I stället finns det några tvångsmedel som huvudsakligen täcker samma område och som kan ge motsvarande uppgifter som hemlig dataavläsning kan ge. De åtgärder som avses är bl.a. teleavlyssning och inhämtande av information i stället för teleavlyssning, teknisk avlyssning och bostadsavlyssning samt teknisk observation av utrustning. För att få använda tvångsmedlen krävs att de kan antas vara av synnerlig vikt för utredning av ett brott. Vilka brott som kan föranleda tvångsmedelsanvändning varierar från tvångsmedel till tvångsmedel. Tillstånd till teleavlyssning kan t.ex. lämnas om den misstänkte är skäligen misstänkt för något av de i lagen särskilt angivna brotten, vilka i huvudsak består av grova brott av olika slag (bl.a. grov spridning av barnpornografisk bild och brott som begåtts i terroristiskt syfte). Vissa tvångsmedel får även användas i underrättelseverksamhet.

Sedan hösten 2016 finns åtgärden också i Norge, då regler om ”dataavlesing” infördes i ”straffeprosessloven”. Tillstånd till dataavläsning ska endast kunna avse bestämda datasystem eller användarkonton till nätverksbaserade kommunikations- och lagringstjänster. Det krävs att det är ett datasystem som den misstänkte ”besitter eller kan antas å ville bruke”. Med ”bruke” avses det direkta användandet av en dator, telefon eller annan utrustning. Ett tillstånd till dataavlesing ger möjlighet att avläsa all information som finns tillgänglig genom den aktuella datorn, oavsett om informationen är lagrad i den eller på annat ställe. Samma sak gäller vid avläsning av ett bestämt användarkonto. När det gäller vilka brott som kan aktualisera dataavläsning gäller som utgångspunkt att maxstraffet för brottet ska vara fängelse i tio år eller mer. Därtill anges viss särskilt angivna brott som t.ex. brott avseende rikets säkerhet, narkotikabrottslighet och människohandel. För att tillstånd ska kunna beviljas måste en person ”med skjellig grunn” kunna misstänkas för en sådan handling eller försök till sådan handling som avses i bestämmelsen. Dataavläsning kan även användas i underrättelseverksamhet.

6 Brottsutveckling av betydelse för förslaget

6.1 It-relaterad brottslighet

Brås rapportering om it-brottslighet

I Brottsförebyggande rådets (Brå) rapport It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem (Brå 2016:17) framgår att en kraftig ökning skett av antalet anmälda brott som kan identifieras som it-relaterade. Med it-relaterade brott avses alla brott som har någon koppling till it, dvs. såväl rena it-brott (t.ex. dataintrång) som brott som begås utanför it-miljö, men där spår och bevisning kan finnas i it-miljö (Brå-rapporten s. 8). Under perioden 2006–2015 var ökningen 949 procent. I absoluta tal var ökningen störst för brottstypen datorbedrägeri och därefter bedrägeri med hjälp av internet. Möjligheten att följa den it-relaterade brottslighetens utveckling med hjälp av kriminalstatistiken är dock starkt begränsad och det går inte att dra några säkra slutsatser om it-inslagen för övriga brott. Det går inte heller att utifrån siffrorna utläsa om det handlar om nya brott eller om en förflyttning av brott, dvs. om traditionella brott har flyttat över till it-miljö. Studien visar i vart fall att it-inslagen i de polisanmälda brotten totalt sett har mer än fördubblats mellan åren 2006 och 2014. Siffrorna bör dock tolkas med stor försiktighet då de sannolikt utgör en kraftig underskattning av den totala andelen brott med it-inslag (Brå-rapporten s. 32).

En förklaring till det ökade antalet anmälningar som per definition har it-inslag är att utvecklingen av sociala medier avspeglas i ökningar av hot, ofredanden och andra brott som sker via sådana kommunikationsvägar.

Även polisens beslag av misstänkta personers mobiltelefoner har ökat (Brå-rapporten s. 39).

Europols rapportering om it-brottslighet

Europols arbetsgrupp EC3 (European Cybercrime Center) arbetar med att stärka de brottsbekämpande myndigheternas möjligheter att motverka it-brottslighet. EC3 ger årligen ut rapporten IOCTA (Internet Organised Crime Threat Assessment) i vilken det finns redogörelser för trender, tendenser och fokusområden när det gäller it-brottslighet.

I IOCTA 2017 slås fast att viss it-brottslighet är vanligt förekommande och högprioriterad i det brottsbekämpande arbetet. Cyberattacker nämns som ett exempel. Attackerna kan vända sig mot såväl statliga organ som banker och andra finansiella aktörer. Inte sällan är en attack med ekonomiskt motiv förknippad med utpressning mot den attacken riktas mot.

Ett område som under flera år lyfts fram som ett problem av IOCTA är användandet av sabotageprogram (eng. malware). Med sabotageprogram menas oönskad programvara i dator, mobil eller annan teknisk utrustning. Kriminella kan genom dessa förmå användare av teknisk utrustning att, medvetet eller omedvetet, installera oönskad programvara i utrustningen. Sabotageprogrammet kan därefter vidta åtgärder med innehållet i utrustningen, såsom att kryptera filer eller söka efter viss information. Det finns

flera exempel på sabotageprogram som potentiellt skulle kunna manipulera kontrollen av kraftnät, finansiella tjänster, försvar eller sjukvårdsregister, vilket kan få katastrofala följder (IOCTA 2017 s. 19). Europol bedömer att trenden med sabotageprogram kommer att fortsätta, även om ökningstakten har börjat avta (IOCTA 2018 s. 7).

Ett annat område som Europol belyser är utnyttjandet av barn i sexuella syften på internet. Kriminaliteten bottnar i användandet av internet som plattform för att kommunicera, lagra och dela barnpornografiskt material för personer som på olika sätt utnyttjar barn. Kryptering, ip-anonymisering, molnlagring och vissa program används i stor utsträckning när dessa brott begås. Darknet och liknande tjänster ger förövare möjlighet att sprida och ta emot barnpornografiskt material och utbyta tekniker för att minska eller begränsa brottsbekämpande myndigheters chanser att komma åt dem (IOCTA 2017 s. 35). Darknet är vanligtvis krypterade nätverk på en del av internet som inte är tillgänglig via vanliga sökmotorer. Darknet möjliggör för användarna att kommunicera utan att varken kommunikationen eller användarna kan spåras eller i vart fall att sådan spårning väsentligen försvåras. Problemet med sexuellt utnyttjande av barn på internet ökar i omfattning och förekomsten av barnpornografiskt material fortsätter att öka. Särskilt svårt att bekämpa på grund av tekniska problem och svårigheter med olika jurisdiktioner är direktsända övergrepp på barn som styrs över internet (IOCTA 2018 s. 7).

Slutligen framhåller Europol att terroristgrupperingar är mycket aktiva på internet och använder det främst för kommunikation, koordinering, propagandaspridning och informationsutbyte. De flesta terrorister brukar det öppna internet, men det förekommer också viss aktivitet på Darknet avseende finansieringskampanjer och användande av illegala marknader (IOCTA 2017 s. 13).

6.2 Terroristbrottslighet

Nationell strategi mot terrorism

I augusti 2015 antog regeringen en ny strategi mot terrorism, Förebygga, förhindra och försvåra – den svenska strategin mot terrorism (skr. 2014/15:146). Sammanfattningsvis syftar åtgärderna till att motverka radikalisering och rekrytering till extremist- och terroristgrupper och påverka individers avsikt att begå eller stödja terroristbrottslighet. Förmågan och möjligheten att begå terroristattentat ska motverkas och minskas. Skyddet för individer ska stärkas och samhällets sårbarhet för terroristattentat ska minska. Om ett terroristattentat ändå genomförs måste samhället också kunna hantera konsekvenserna av det.

Av European Union Terrorism Situation and Trend Report 2017 framgår att det under 2017 rapporterades 205 misslyckade, omintetgjorda eller genomförda terrorattacker i EU. Statistiken gäller attacker från jihadister, rörelser ur extremvänstern och extremhögern, separatister samt vissa ickespecificerade dåd. Antalet planerade attacker med koppling till jihadism har mer än fördubblats från 2016, men endast en tredjedel av terrorattackerna har faktiskt genomförts. I denna statistik ingår terrordådet på Drottninggatan i Stockholm den 7 april 2017.

Risken för terroristattentat i Sverige

Risken för terroristattentat i Sverige påverkas av det allmänna världsläget. Krigshändelser och terrordåd som utförs i närliggande länder kan påverka den s.k. hotnivåskala som beslutas av chefen på Säkerhetspolisen. Denna har under senare år varierat och nått högre nivåer än vad som tidigare varit vanligt. Informationen som ligger till grund för beslutet om vilken hotnivå som ska gälla kommer bland annat från Nationellt centrum för terrorhotbedömning (NCT).

Det främsta terrorhotet mot Sverige kommer från islamistiskt motiverad terrorism. Det finns individer både i Sverige och utomlands som betraktar terrorattentat mot mål i Sverige som legitima och ett fåtal av dessa har såväl avsikt som förmåga att genomföra attentat. Ett eventuellt terrorattentat kan planeras eller genomföras på uppdrag av aktörer såväl i Sverige som utomlands, men kan även utföras på initiativ av enskilda individer. Det finns också ett visst hot från politiskt motiverade rörelser, men det framstår som mindre sannolikt att individer från den miljön kommer att begå terrorattentat (NCT:s rapport Helårsbedömning år 2018).

För den numera kraftigt försvagade extremistiska rörelsen Daesh, som tidigare var en del av al-Qaidas nätverk, har internet och sociala medier spelat en central roll i spridandet av propaganda för radikalisering och rekrytering (skr. 2014/15:146). Även om Daesh inte längre utgör samma hot och inte heller längre attraherar individer att ansluta sig till rörelsen på samma sätt som förut, utgörs risken numera i stället av att radikaliserade individer återvänder till EU, vilket kan bidra till att stärka de inhemska extremiströrelserna här (se European Union Terrorism Situation and Trend Report 2017).

Skärpta regler för terroristbrottslighet

Den svenska terrorismlagstiftningen har förändrats vid flera tillfällen under senare tid. Lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet har ändrats vid flera tillfällen. Bland annat har viss ny brottslighet lagts till i katalogen över brottslighet som ska anses särskilt allvarlig. Det har också kriminaliserats att motta utbildning avseende särskilt allvarlig brottslighet och att resa eller påbörja resa i terrorismsyfte. Vidare har lagen (2003:148) om straff för terroristbrott ändrats till följd av vissa nya brottsbeteckningar (synnerligen grovt vapenbrott och grovt olaga hot) och underlåtenhet att förhindra terroristbrott straffbelagts. I lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall har det gjorts brottsligt att samla in, tillhandahålla eller ta emot pengar eller annan egendom i syfte att egendomen ska användas eller med vetskap om att den är avsedd att användas för en förbjuden terroristresa.

Dessa ändringar medför bl.a. att antalet brott som kan föranleda hemlig avlyssning av elektronisk kommunikation och viss annan tvångsmedelsanvändning har ökat.

Regeringen har nyligen beslutat en proposition med förslag på ett särskilt straffansvar för samröre med en terroristorganisation. Slutligen har regeringen gett en särskild utredare i uppdrag att genomföra en systematisk

översyn av den straffrättsliga lagstiftningen på terrorismområdet och föreslå en ny reglering som bör samlas i ett regelverk. Uppdraget ska redovisas under hösten 2019.

6.3 Organiserad brottslighet

Kriminella nätverk och grupperingar

Enligt Brottsförebyggande rådets (Brå) rapport Kriminella nätverk och grupperingar – polisers bild av maktstrukturer och marknader (Rapport 2016:12) har kartan för den kriminella miljön i Sverige ritats om de senaste tjugo åren. Antalet sammanslutningar i den kriminella miljön har ökat samtidigt som det har tillkommit självdefinierade grupper med namn och attribut som tydligt visar grupptillhörighet.

Tillväxten av kriminella grupper och nätverk har blivit ett stort problem. Konflikter som uppstår i den kriminella miljön leder till skjutningar på allmän plats och utmanar myndigheternas förmåga att upprätthålla lag och ordning. Det kan leda till att människor känner otrygghet och kan minska legitimiteten hos samhällets institutioner. Detta gäller enligt Brå särskilt i socialt utsatta områden där kriminella grupper har fått ett stort handlingsutrymme.

Polisens bild av organiserad brottslighet

I Polismyndighetens rapport om allvarlig och organiserad brottslighet från oktober 2017 har myndigheten redovisat en nationell lägesbild över organiserad brottslighet i Sverige. Enligt rapporten begås sådan brottslighet till stor del utanför formaliserade nätverksstrukturer. Många kriminella gäng är således löst sammansatta, men det finns också rörelser med starka hierarkier (t.ex. mc-gäng). Situationen i de utsatta områdena är sådan att unga löper stor risk att involveras i brottslighet, vilket medför en ökad risk att antalet aktörer inom allvarlig och organiserad brottslighet på sikt kan komma att öka. Utvecklingen i dessa områden bedöms vara den avgörande faktorn för de parallella samhällsstrukturernas tillväxt. Våldet har blivit grövre och ökat i omfattning med ett ökat antal skjutningar.

Allt fler kriminella aktörer bedöms ägna sig åt it-brottslighet och komplex cyberbrottslighet, främst olika former av dataintrång, som kan ha stor inverkan på samhällets tekniska infrastruktur. Bland annat kan bedrägerier genomföras på nya sätt, t.ex. genom utpressningsvirus som infekterar en dator eller mobiltelefon. Den ökade användningen av krypterings- och anonymiseringstjänster har också gjort det enklare att få tillgång till och dela bilder och filmer som innehåller sexuella övergrepp mot barn. Det finns en ökande trend att sådant material produceras för ekonomisk vinning.

Narkotikahandel är fortfarande en central del av ekonomisk brottslighet och våld och konflikter i kriminella kretsar är ofta narkotikarelaterade. Internet har en växande roll i marknadsföring och försäljning då en stor del av drogförsäljningen sker på Darknet och betalning i de fallen nästan uteslutande görs med kryptovalutan bitcoin. Nätförsäljning medför att droger är mer lättillgängliga och mer varierade.

I en rapport som Polismyndigheten och Tullverket gemensamt arbetat fram (Drogsituationen, Lägesbild i Sverige 2013–2016) anges bl.a. att marknaden för olaglig narkotika och andra droger utgör en mycket dynamisk kriminell marknad i Europa som drivs framåt på grund av marknadskonkurrens och tekniska innovationer. Det krävs i hög utsträckning internationellt samarbete mot den gränsöverskridande narkotikabrottsligheten för att begränsa tillgången på narkotika i Sverige. Den narkotikarelaterade dödligheten i Sverige utmärker sig genom att individerna som överdoserar är yngre och en allvarlig del i utvecklingen är ett ökat antal dödsfall som kan kopplas till nya psykoaktiva substanser inhandlade på internet.

Det finns, enligt Polismyndigheten och Tullverket, indikationer på att personer i Sverige i högre utsträckning än i andra länder köper narkotika på internet. Problemet är känt för de brottsbekämpande myndigheterna men webbaserade drogmarknader är extra svåra att kontrollera. Det beror bl.a. på att olika delar av narkotikakedjan från tillverkare till slutkund ofta finns i olika länder och att marknaden blivit mer komplex med kryptovalutor, anonymiserad internettrafik och dolda marknadsplatser.

6.4 Dödligt våld

Det dödliga våldet i Sverige har varit tämligen konstant under de senaste 20 åren. 2015 var dock ett undantag i negativ riktning med 112 rapporterade dödsfall. Detta motsvarar en ökning med 24 procent jämfört med det genomsnittliga antalet offer för dödligt våld under 2000-talet. År 2016 noterades en viss sänkning, men 2017 noterades den högsta siffran under perioden 2002 – 2017 då 113 personer föll offer för dödligt våld. Ökningen kan delvis förklaras med att antalet offer i ärenden med fler än ett fall hade ökat och att brott som involverar skjutvapen har ökat under senare år (Konstaterade fall av dödligt våld, Brå 2017).

Även om studierna inte redogör för vilket motiv inom de kriminella konflikterna som blivit vanligast eller om det finns någon systematisk förändring över tid kan det rimligen antas att konflikter relaterade till organiserad brottslighet ligger bakom i vart fall en del av ökningen (se t.ex. Skjutningar i kriminella miljöer, Brå 2019:3 s. 15).

7 Ny teknik försvårar verkställigheten av hemliga tvångsmedel

7.1 Kryptering

Ett tillstånd till hemlig avlyssning av elektronisk kommunikation ger de brottsbekämpande myndigheterna rätt att ta del av innehållet i den kommunikation som ska avlyssnas. Ett problem vid verkställighet av ett sådant tillstånd, som uppmärksammades redan av Beredningen för rättsväsendets utveckling (SOU 2005:38), är att en mycket stor del av all kommunikation är krypterad och därmed inte möjlig att läsa i klartext. Skälet

till denna alltmer spridda kryptering är att det på senare tid har utvecklats allt fler enkla, billiga och användarvänliga krypteringstjänster för den som önskar skydda sin kommunikation. Dels finns möjlighet att på egen hand köpa programvara för att kryptera meddelanden, dels är det mycket vanligt att leverantörer av meddelandetjänster har inbyggda funktioner i programvaran som utför kryptering. Vad gäller det senare kan nämnas Facebooks Messenger, Whatsapp och Instagram, Microsofts Skype och MSN, Googles Gmail samt Apples Imessage och Facetime. Dessa program har en användarvänlig inbyggd krypteringstjänst för att hindra utomstående från att ta del av kommunikationen.

Krypteringstjänster har i mycket stor utsträckning ett legitimt syfte och möjliggör för användare att kunna kommunicera med varandra utan risk att utomstående ska kunna ta del av innehållet.

Även en stor del av internettrafiken är krypterad. Enligt utredningen kan knappt tio procent av den internettrafik som får lov att avlyssnas med stöd av reglerna om hemlig avlyssning av elektronisk kommunikation läsas i klartext. Av dessa knappa tio procent utgör merparten surfande hos nyhetsbyråer och på pornografiska webbplatser.

Också behovet av att skydda information som finns lagrad i datorer, servrar, mobiltelefoner och annan teknisk utrustning har tillgodosetts genom att det utvecklats en rad krypteringstjänster som byggts in i stora operativsystem (till exempel Microsofts tjänst Bitlocker och Apples Filevault). Även smarttelefoner har en inbyggd krypteringslösning. Telefonen kan då kräva lösenkod eller fingeravtryck eller någon annan uppgift från användaren för att låsas upp. Denna typ av kryptering av teknisk utrustning har i de flesta fall ett helt legitimt syfte, t.ex. gör lösenkoden på en smarttelefon att personliga uppgifter inte kommer i orätta händer om telefonen tappas bort eller blir stulen. Men krypteringen för också med sig att myndigheterna får svårt att ta del av innehållet i beslagtagna mobiltelefoner vid undersökningar av dem.

7.2 Anonymisering

Den kryptering som beskrivs i föregående avsnitt leder alltså till problem för myndigheterna när det gäller att ta del av innehållet i kommunikation. När det gäller möjligheten att ta reda på vem som står bakom kommunikationen är det i stället anonymisering som är ett problem. Med detta avses olika slags tjänster som gör det möjligt att dölja sin aktivitet på internet. Ett exempel på enkel anonymiserad internetkommunikation, eller i vart fall sådan som blir svårare att spåra, är då en telefon ansluter till ett wifinätverk på ett café eller en flygplats.

Under senare år har det dykt upp en rad tjänster som på ett avancerat sätt kan tillgodose anonymisering på internet. Ett exempel på en sådan tjänst är Tor, som genom kraftig kryptering erbjuder helt anonymiserad kommunikation. Anonymiseringstjänster har ofta ett legitimt syfte och är ett bra sätt för enskilda att bevara sin integritet på internet, t.ex. för den källa som vill lämna upplysningar för publicering i media.

Samtidigt som anonymiseringen är en viktig tjänst för många medborgare ger den upphov till problem när misstänkta personers kontakter

ska kartläggas. Hemlig övervakning av elektronisk kommunikation kan i stora delar bli verkningslös om de övervakade personerna använder sig av anonymiseringstjänster.

7.3 Även kriminella använder kryptering och anonymisering

Som redogörs för i föregående avsnitt är kryptering och anonymisering helt legitima och mycket användbara tjänster för många människor. Baksidan är dock att lika effektivt som legitim verksamhet döljs, döljs också kriminell verksamhet.

Europol har i en rapport från 2016 konstaterat att individer och grupperingar som ägnar sig åt terrorism och extremistiska aktiviteter använder kryptering och anonymisering för att komma undan brottsbekämpande myndigheter och underrättelseverksamhet (European Union Terrorism Situation and Trend Report 2016). Vad gäller terroristgrupperingar framgår bl.a. att medlemmarna uppmuntras att täcka sina spår med krypterad mjukvara och det förekommer att grupperingarna själva utvecklar egna verktyg. Det är dock vanligast att de använder sig av redan befintlig kryptering, ofta i smarttelefoner. Sådana grupperingar publicerar också instruktioner för hur man ska hålla sig anonym på den digitala arenan.

Beträffande Darknet har Europol konstaterat att det innehåller marknadsplatser för praktiskt taget all möjlig illegal verksamhet. Exempelvis går det där att köpa narkotika, vapen, förfalskade dokument och stulna idhandlingar. Det går dessutom att köpa kriminella tjänster som t.ex. hackningstjänster och penningtvätt.

Det finns flera domar i Sverige som bekräftar att det via Darknet skett omfattande drogförsäljning i landet. Aktiviteter på Darknet har också förekommit i mål om barnpornografibrott och urkundsförfalskning.

8 Bör hemlig dataavläsning införas som ett nytt hemligt tvångsmedel?

8.1 Utgångspunkter för att bedöma behovet av hemlig dataavläsning

Införandet av nya tvångsmedel eller ett utökat användningsområde för befintliga tvångsmedel kräver att det görs noggranna avvägningar beträffande behovet av åtgärden, åtgärdens förväntade effektivitet och nytta samt vilka integritetsintrång som åtgärden kan förväntas medföra. Ett nytt tvångsmedel måste motsvaras av ett faktiskt behov, vilket ska vägas mot vikten av att värna rättssäkerhet och personlig integritet, se t.ex. Integritetsskyddskommitténs betänkande Skyddet för den personliga integriteten (SOU 2007:22, del 1 s. 176–177).

Som nämns i avsnitt 5.1.3 skulle hemlig dataavläsning kunna användas för att samla in olika typer av uppgifter. För att besvara frågan om det finns

ett behov av åtgärden bör det klargöras vilka typer av uppgifter som behovsanalysen omfattar. I likhet med utredningen anser regeringen att behovsanalysen bör utgå från fem olika uppgiftstyper:

– innehåll i och uppgifter om meddelanden som överförs eller överförts i elektroniskt kommunikationsnät
– platsuppgifter (av utredningen benämnt lokaliseringsuppgifter)
– optisk personövervakning
– avlyssning av samtal m.m.
– uppgifter som finns elektroniskt lagrade och uppgifter som visar hur viss teknisk utrustning används.

De fyra första uppgiftstyperna avser uppgifter som de brottsbekämpande myndigheterna redan i dag kan få tillstånd att i hemlighet samla in genom hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning. Den sista uppgiftstypen avser uppgifter som inte är möjliga att i hemlighet eller löpande få tillgång till i dag. Uppgifterna kan dock till viss del inhämtas i hemlighet redan i dag, men endast om de överförs i ett elektroniskt kommunikationsnät (och då genom hemlig avlyssning av elektronisk kommunikation). Uppgifterna kan även inhämtas genom beslag trots att de inte har överförts i ett elektroniskt kommunikationsnät. En sådan inhämtning kan dock inte göras i hemlighet (jfr dock förslagen om senarelagd underrättelse om beslag i SOU 2017:100). De brottsbekämpande myndigheterna kan således få tillgång till vissa av dessa uppgifter i dag. Det görs dock under något andra förutsättningar än om hemlig dataavläsning kan användas.

När det gäller de fyra första uppgiftstyperna har det vid införandet av vart och ett av dessa hemliga tvångsmedel gjorts en bedömning att det finns ett reellt behov för de brottsbekämpande myndigheterna att kunna samla in uppgifterna. Det har inte framkommit något som tyder på att den bedömningen inte skulle ha fortsatt giltighet. Tvärtom har regeringen återkommande i sin årliga redovisning till riksdagen om användningen av hemliga tvångsmedel konstaterat att de brottsbekämpande myndigheternas användning av hemliga tvångsmedel har varit ett ändamålsenligt och nödvändigt instrument i brottsbekämpningen (se t.ex. skr. 2018/19:19 s. 39, skr. 2017/18:69 s. 35 och skr. 2016/17:69 s. 36). I den delen måste det därför göras en analys av i vilken utsträckning det finns ett reellt behov av nya metoder eller tekniker för att kunna komma åt uppgifterna. Även när det gäller den femte uppgiftstypen är det klarlagt att det i vart fall till viss del finns ett behov av uppgifterna. Sådana uppgifter används nämligen mycket frekvent i brottsutredningar och de brottsbekämpande myndigheterna kommer i vart fall delvis åt uppgifterna genom beslag. Beslag kan dock i princip inte användas i hemlighet (även om ett förslag om en sorts hemliga beslag bereds inom Regeringskansliet, se SOU 2017:100). I den delen får därför frågan om behovet av att kunna samla in uppgifter i hemlighet en mer framträdande plats.

8.2 Behovet av hemlig dataavläsning som metod för att verkställa befintliga hemliga tvångsmedel

Regeringens bedömning: Det finns ett påtagligt behov av nya och bättre metoder för att i hemlighet komma åt uppgifter som redan i dag får hämtas in med befintliga tvångsmedel men som på grund av den tekniska utvecklingen och brotts- och samhällsutvecklingen i övrigt inte går att komma åt.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Majoriteten av de remissinstanser som kommenterar behovet av hemlig dataavläsning instämmer i utredningens bedömning. De instämmer också i den problembild som utredningen redovisar. Bland andra *Riksdagens ombudsmän (JO), Stockholms tingsrätt, Göteborgs tingsrätt, Justitiekanslern, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Brottsförebyggande rådet, Tullverket, Myndigheten för samhällsskydd och beredskap, Svenska kyrkan* och *Sveriges kristna råd* delar bedömningen att det finns ett klart behov av hemlig dataavläsning. Även *Sveriges advokatsamfund* anser att ett sådant behov finns genom att den information som på laglig väg kan hämtas in har reducerats kraftigt. Säkerhetspolisen tillägger att de senaste årens tekniska utveckling, liksom brotts- och samhällsutveckling i övrigt, inneburit att de brottsbekämpande myndigheterna inte längre kan ta del av många av de uppgifter som man tidigare fick del av genom användande av straffprocessuella tvångsmedel. *Säkerhets- och integritetsskyddsnämnden* anser att det på teleområdet finns behov av att under en förundersökning genom hemlig dataavläsning få del av uppgifter avseende elektronisk kommunikation. Det rör sig enligt nämnden om en ny verkställighetsform som såvitt kan bedömas inte medför några möjligheter att få fram annan information än vad tvångsmedlen ger i dag. Nämnden anser däremot inte att utredningen förmått visa ett påtagligt behov av hemlig dataavläsning vid hemlig kameraövervakning och hemlig rumsavlyssning. Det kommer att innebära en väsentlig utökning av myndigheternas möjlighet att i hemlighet kartlägga enskildas liv. Dessa tvångsmedel tillhör de mest integritetskränkande och bör som utgångspunkt användas restriktivt.

Stockholms universitet (Juridiska fakulteten) anför att utredningen inte har redovisat statistik eller någon övergripande bild av behovets omfattning och anser därför att det inte kommit fram ett tillräckligt starkt behov av att införa hemlig dataavläsning.

Skälen för regeringens bedömning

Innehåll i och uppgifter om meddelanden

Den tekniska utvecklingen har inneburit att allt mindre kommunikation sker via traditionell telefoni. Det beror både på de nya internetbaserade kommunikationstjänster som utvecklats och som används allt mer och på att det finns en generell utveckling som innebär att traditionell telefoni övergår till att vara ip-baserad. Med detta menas förenklat att samtalsöverföringen görs i form av datapaket som sätts ihop till ett obrutet flöde

hos mottagaren, vilket skiljer sig från den teknik som används vid traditionell telefoni.

Enligt utredningen råder det konsensus bland brottsbekämpande myndigheter om att hemlig avlyssning och övervakning av elektronisk kommunikation i dag är långt ifrån lika effektiva metoder för avlyssning och övervakning av datakommunikation som de varit tidigare (se myndigheternas behovsbeskrivning avseende hemlig dataavläsning, bilaga 2 till utredningens betänkande s. 603–689). I remissbehandlingen anför bl.a. *Åklagarmyndigheten* och *Ekobrottsmyndigheten* att framför allt kryptering och anonymisering har lett till att befintliga hemliga tvångsmedel har minskat i effektivitet på senare år. Även *Sveriges advokatsamfund* anser att det finns ett behov av mer effektiva metoder för att bekämpa och utreda brott. Enligt utredningen är mer än 90 procent av den avlyssnade internettrafiken i dag krypterad. Det beror enligt utredningen på ny teknik, kriminellas medvetenhet om polisens metoder och framför allt den ökande krypteringsgraden i kommunikation mellan kriminella. Följden av den ökade krypteringen är att det är svårt att på förhand förutse om tvångsmedelsanvändningen kommer att vara lyckosam och att det ofta är tillfälligheter som avgör om användningen ger resultat. Det har framhållits att i stort sett samtliga appar och program som används för kommunikation har inbyggda funktioner för skydd och säkerhet som minskar värdet av tvångsmedlen och att problemen ökar för varje år. Vidare har de brottsbekämpande myndigheterna uppgett att den kommunikation som kan avlyssnas är tämligen ointressant.

Stockholms universitet (Juridiska fakulteten) ifrågasätter inte myndigheternas upplevda behov men saknar statistik och en övergripande bild av behovets omfattning. Universitetet anser att utredningen i detta avseende uppvisar sådana brister att den inte kan läggas till grund för att införa hemlig dataavläsning. Det är i och för sig så att det saknas fullständig statistik över hur kriminaliteten ökat, minskat eller bytt skepnad över tid och hur det påverkar behovets omfattning. Det finns dock, förutom de brottsbekämpande myndigheternas uppfattning om behovet, även uppgifter från Brottsförebyggande rådet och Europol (se avsnitt 6.1) som visar brottsutvecklingen över tid och dess betydelse för behovet av hemlig dataavläsning. Som anges i avsnitt 8.4 anser regeringen dessutom inte att det finns något utpräglat behov av exakta statistiska uppgifter för att göra nödvändiga överväganden i frågan. Regeringen delar således inte bedömningen att underlaget är så bristfälligt att det inte kan läggas till grund för att införa hemlig dataavläsning.

Regeringen redovisar årligen till riksdagen hur reglerna om hemliga tvångsmedel har använts under det gångna året (avsnitt 4.7). Av de två senaste årens redovisningar framgår att kryptering utgör ett problem vid verkställighet av hemlig avlyssning av elektronisk kommunikation (skr. 2017/18:69 och skr. 2018/19:19). Enligt de brottsbekämpande myndigheterna beror det på att personer som är medvetna om att de kan komma att avlyssnas tenderar att övergå från vanliga telefonsamtal till att kommunicera på ett sådant sätt att vedertagen avlyssning inte är möjlig.

Utöver problemet med kryptering finns anonymisering (avsnitt 7.2). Det kan t.ex. handla om att en avlyssnad person övergår från att använda internetåtkomst via sitt mobilabonnemang till att använda ett wifi-nätverk. Även om syftet med det kan vara helt legitimt så omöjliggör det avlyssning

av kommunikationen. Andra förfaranden som medför anonymisering är särskilda tjänster som används just för att uppnå ett anonymt användande av internet, t.ex. genom att byta ut personens riktiga ip-adress mot en anonym sådan.

Utredningen drar slutsatsen att en metod som ger tillgång till krypterade och anonymiserade uppgifter i klartext skulle vara mycket värdefull för de brottsbekämpande myndigheterna. Regeringen delar, i likhet med flertalet remissinstanser, den bedömningen och menar att det föreligger ett påtagligt behov för de brottsbekämpande myndigheterna att med nya metoder kunna bereda sig tillgång till innehållet i och uppgifter om meddelanden som man i dag har en laglig, men inte praktisk, möjlighet att inhämta. Som *Säkerhets- och integritetsskyddsnämnden* påtalar rör det sig om en ny verkställighetsform som såvitt kan bedömas inte medför några möjligheter att få fram någon annan typ av information än vad hemlig avlyssning och övervakning av elektronisk kommunikation kan ge i dag.

Hemlig avlyssning och övervakning av elektronisk kommunikation är möjliga åtgärder både i underrättelseverksamhet och i brottsutredande verksamhet. De problem som gör sig gällande avseende kryptering och anonymisering skiljer sig inte åt beroende på om inhämtningen av uppgifter görs i underrättelse- eller förundersökningsverksamhet. Behovet är därför enligt regeringens mening lika starkt oavsett i vilket skede av brottsbekämpningen som inhämtningen görs. Detsamma gäller vid särskild utlänningskontroll.

Sammanfattningsvis anser regeringen i likhet med utredningen att kryptering och anonymisering medför stora negativa konsekvenser för de brottsbekämpande myndigheterna. Det kan till exempel innebära att utredningar läggs ned eller väljs bort i ett tidigt skede eftersom befintliga utredningsåtgärder inte är en framkomlig väg. En annan effekt är att utredningarna inte kommer åt ledare för organiserad brottslighet med hierarkiska strukturer eftersom de sällan kan kopplas till brotten, trots att de brottsbekämpande myndigheterna anser sig ha en god bild av vilka dessa personer är. Det finns således ett påtagligt behov av ett nytt hemligt tvångsmedel så att de brottsbekämpande myndigheterna återfår sin förmåga att inhämta innehåll i och uppgifter om meddelanden.

Uppgift om geografisk position

De brottsbekämpande myndigheterna har ett behov av att kunna ta reda på var en viss teknisk enhet, som har betydelse i en brottsutredning eller i underrättelseverksamhet, finns eller har funnits, även om den misstänkte är okänd. En sådan uppgift kan vara värdefull även i situationer där den misstänkte är känd för den brottsbekämpande myndigheten, för att få veta var den misstänkte befinner sig eller i vilka miljöer han eller hon rör sig.

Både i förundersökningsverksamhet och i underrättelseverksamhet har de brottsbekämpande myndigheterna möjlighet att få tillgång till lokaliseringsuppgifter avseende bl.a. mobiltelefoner. Det kan handla om uppgifter om vilken basstation en telefon eller annan elektronisk kommunikationsutrustning varit uppkopplad mot i samband med kommunikation.

Uppgifter om var en elektronisk kommunikationsutrustning befinner eller har befunnit sig finns inte bara hos teleoperatören utan också många gånger i utrustningen. Hemlig dataavläsning kan därför användas för att ta

del av sådana uppgifter, t.ex. uppgifter som finns sparade i en telefon med platsinformation eller genom aktivering av inbyggd positioneringsutrustning som exempelvis GPS.

Dessa uppgifter kan vara betydligt mer exakta än de som kan hämtas in från operatören om vilken mast telefonen kopplat upp sig mot. Säkerhetspolisen har i sin behovsbeskrivning (se bilaga 2 till utredningens betänkande s. 608) exempelvis anfört att i flera av myndighetens utredningar har positionsuppgifterna från operatörerna varit allt för oprecisa för att vara avgörande när det gäller att knyta en person till en viss plats. Ytterligare en aspekt är att lokaliseringsuppgifter förutsätter att telefonen är påslagen. Så är sällan fallet i direkt samband med att ett planerat brott utförs. Med en mer exakt geografisk positionering strax före avstängningen skulle möjligheterna öka att knyta telefonen eller gärningsmannen till brottet. Det skulle också vara möjligt att i realtid se när telefonens GPS-positionering stängs av.

Det angivna talar enligt regeringens mening med styrka för att det föreligger ett påtagligt behov av nya och bättre metoder för att samla in uppgifter om geografisk position. Ingenting har framkommit som talar för att behovet skiljer sig åt beroende på om åtgärden vidtas i underrättelseverksamhet, i förundersökningsverksamhet eller vid särskild utlänningskontroll.

Optisk personövervakning och avlyssning av ljud

Om teknisk utrustning har en kamerafunktion eller en mikrofonfunktion kan tekniska metoder användas för att på distans aktivera dessa funktioner i utrustningen. Sådana uppgifter (rörlig bild och tal) motsvarar vad som i dag får hämtas in efter tillstånd till hemlig kameraövervakning och hemlig rumsavlyssning.

Ingenting har framkommit i de behovsbeskrivningar som de brottsbekämpande myndigheterna har lämnat (se bilaga 2 till utredningens betänkande s. 603–689) som talar för att hemlig kameraövervakning eller hemlig rumsavlyssning i teknisk mening fungerar sämre i dag än de gjort tidigare, såsom beskrivs ovan beträffande hemlig avlyssning och övervakning av elektronisk kommunikation på grund av t.ex. kryptering. Inte heller utredningen redogör för att det finns sådana problem. Däremot har det framkommit att det i vissa fall inte är möjligt att verkställa åtgärderna på grund av att den verkställande myndigheten inte kan bereda sig tillgång till den plats ett tillstånd avser eller att det inte finns något lämpligt ställe på platsen att montera det tekniska hjälpmedlet på. Också en generell medvetenhet hos kriminella om under vilka förutsättningar de brottsbekämpande myndigheterna får använda befintliga hemliga tvångsmedel har lyfts fram som skäl för nya metoder. Det framgår av utredningen att kriminella bland annat utnyttjar att tillstånden måste vara knutna till viss förutbestämd plats och därför väljer att ha möten på platser som inte går att förutse från myndigheternas sida eller platser där tvångsmedlen inte fysiskt kan verkställas.

En vanlig förklaring när misstänkta personer konfronteras med att vissa meddelanden har skickats eller andra åtgärder vidtagits från deras telefon eller dator är nämligen att de lånat ut eller låtit någon annan använda utrustningen, alternativt att det inte är deras telefon eller dator. Med en

möjlighet att t.ex. använda kameran på en mobiltelefon som är riktad mot användaren kan det snabbt avgöras om det är den som åtgärden avser eller annan person som skickat ett meddelande. Sådan identifiering kan också göras genom röstigenkänning genom att aktivera mikrofonen i den tekniska utrustningen. Åtgärden skulle alltså kunna identifiera den misstänkte eller den som är av intresse i underrättelseverksamheten. Åtgärden kan även vara värdefull i situationer där den misstänkte är känd för den brottsbekämpande myndigheten, för att veta var den misstänkte befinner sig eller i vilka miljöer han eller hon rör sig.

Det är alltså inte utvecklingen av tekniken i sig utan endast andra förutsättningar för verkställighet som ligger till grund för behovet av nya metoder i denna del. Det finns inte skäl att ifrågasätta de uppgifter som de brottsbekämpande myndigheterna lämnat i sina behovsbeskrivningar och under remissbehandlingen. I Tullverkets behovsbeskrivning (se bilaga 2 till utredningens betänkande s. 632 och 643) anför myndigheten att det numera är välkänt för kriminella att de brottsbekämpande myndigheterna använder hemliga tvångsmedel, vilka dessa är och hur de används. De kriminella nätverken har anpassat sitt beteende efter denna kunskap. Vidare konstateras att hemlig kameraövervakning och hemlig rumsavlyssning är mycket kostsamma och tidskrävande åtgärder och att resultatet ofta brister i kvalitet. Dessutom tar det lång tid att granska materialet, vilket leder till längre förundersökningstider. Vidare har hemlig kameraövervakning vid ett flertal tillfällen inte kunnat verkställas eftersom det varit svårt att hitta ett lämpligt ställe att montera kamerautrustningen på. Eftersom tvångsmedlet framför allt ska användas på platser som är svårspanade går myndigheten miste om viktig information om det inte finns möjlighet att montera utrustningen. I Åklagarmyndighetens behovsbeskrivning (se bilaga 2 till utredningens betänkande s. 677–678) konstateras att hemlig kameraövervakning och hemlig rumsavlyssning är mycket resurskrävande metoder eftersom platsen för verkställighet ofta måste undersökas i förväg och säkras under tiden som avlyssnings- eller övervakningsutrustningen monteras. Det är inte alltid det går att uppnå fullgod ljud- eller bildkvalitet. Vidare är de platser som hemlig rumsavlyssning kan utföras på sådana platser där den misstänkte kan räkna med att bli föremål för avlyssning. Det är inte tillfredsställande att personer i kriminella miljöer i någon mening förfogar över möjligheterna för de brottsbekämpande myndigheterna att lyckas i sina utredningar. Mot denna bakgrund anser regeringen, till skillnad från *Säkerhets- och integritetsskyddsnämnden,* att det finns ett påtagligt behov av åtgärder som kompletterar de befintliga möjligheterna till hemlig kameraövervakning och hemlig rumsavlyssning.

Hemlig dataavläsning kan möjliggöra en löpande insamling av uppgifter oberoende av vilken plats personen som åtgärden avser befinner sig på. En sådan lösning skulle innebära en utvidgning av tillämpningsområdet för både hemlig kameraövervakning och hemlig rumsavlyssning, vilka båda kräver att det i tillståndet anges på vilken plats åtgärden får vidtas. Det kan antas att kriminella personer, åtminstone personer inom den organiserade brottsligheten, är väl införstådda med på vilka platser de löper störst risk för att utsättas för hemlig rumsavlyssning eller hemlig kameraövervakning och att dessa personer anpassar sitt beteende efter sådan kunskap i syfte att undgå avlyssning eller övervakning. Behovet måste därför anses vara

påtagligt inte bara för uppgifter som kan hämtas in enligt dagens förutsättningar utan också för uppgifter som kan hämtas in på andra platser än de där avlyssning eller övervakning i dag får förekomma. En annan fråga är om det är proportionerligt, vilket regeringen återkommer till i avsnitt 8.6.

Hemlig rumsavlyssning är inte en tillåten åtgärd i underrättelseverksamhet. Utöver att integritetsskäl talade emot att införa en möjlighet till sådan användning anförde regeringen, i samband med införandet av åtgärden i rättegångsbalken, att det på det tidiga stadium när preventiva tvångsmedel används mer sällan synes finnas konkreta uppgifter om t.ex. att möten ska ske på en viss plats för att avhandla viktiga frågor, se propositionen Hemliga tvångsmedel mot allvarliga brott (prop. 2013/14:237 s. 101). I likhet med utredningen gör regeringen inte någon annan bedömning nu. Det är alltså endast i förundersökningsfallen som det redovisade behovet av rumsavlyssningsuppgifter finns. När det däremot gäller hemlig kameraövervakning är åtgärden tillåten i underrättelseverksamhet under de förutsättningar som framgår av preventivlagen. Ingenting har framkommit som ger anledning att anta att det behov av kameraövervakningsuppgifter som redovisas ovan skiljer sig åt mellan förundersöknings- och preventivlagsfallen.

8.3 Behovet av hemlig dataavläsning som metod för att kunna samla in uppgifter som inte kan samlas in genom befintliga tvångsmedel

Regeringens bedömning: Det finns ett påtagligt behov av att i hemlighet kunna samla in elektroniskt lagrade uppgifter och uppgifter som visar hur ett avläsningsbart informationssystem används, som inte kan samlas in genom befintliga tvångsmedel.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Majoriteten av de remissinstanser som kommenterar behovet av hemlig dataavläsning instämmer i utredningens bedömning. De instämmer också i den problembild som utredningen redovisar. Bland andra *Riksdagens ombudsmän (JO), Stockholms tingsrätt, Göteborgs tingsrätt, Justitiekanslern, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Brottsförebyggande rådet*, *Tullverket*, *Myndigheten för samhällsskydd och beredskap, Svenska kyrkan* och *Sveriges kristna råd* delar bedömningen att det finns ett klart behov av hemlig dataavläsning. Ekobrottsmyndigheten tillägger att dagens ordinarie utredningsmetoder såsom spaning oftast inte räcker för att driva förundersökningen framåt. Beslag av datorer räcker inte för bevissäkring i komplexa ärenden, eftersom kryptering eller lösenordsskydd försvårar eller omöjliggör att i efterhand ta fram information från datorn. Myndigheten antar att hemlig dataavläsning kommer att kunna effektivisera det brottsutredande arbetet. Även *Sveriges advokatsamfund* anser att ett sådant behov finns genom att den information som på laglig väg kan hämtas in har reducerats kraftigt. *Säkerhetspolisen* framför att de senaste årens tekniska utveckling, liksom brotts- och samhällsutveckling i övrigt, inneburit att de brottsbekämpande myndigheterna inte längre kan ta del av

många av de uppgifter som man tidigare fick del av genom användande av straffprocessuella tvångsmedel.

Stockholms universitet (Juridiska fakulteten) ifrågasätter inte myndigheternas upplevda behov men anför att utredningen inte har redovisat statistik eller någon övergripande bild av behovets omfattning och anser därför att det inte kommit fram ett tillräckligt starkt behov av att införa hemlig dataavläsning.

Skälen för regeringens bedömning

Den tekniska och samhälleliga utvecklingen har inte bara lett till att hemliga tvångsmedel har förlorat i effektivitet. Även beslag av elektroniska informationsbärare ger allt mindre information för de brottsbekämpande myndigheterna. Det beror dels på den alltmer använda krypteringen (se avsnitt 7.1), dels på att vissa uppgifter över huvud taget inte lagras, t.ex. uppgifter i dokument som inte sparas. Härtill kommer att digitaliseringen har medfört att alltmer information finns i elektronisk form. Att upprätthålla en brottsbekämpande förmåga i den digitala miljön har således blivit allt viktigare. Det finns därför skäl att överväga om hemlig dataavläsning bör införas som hemligt tvångsmedel för att komma åt uppgifter som lagras i ett informationssystem och uppgifter om hur ett informationssystem används. Genom ett sådant tvångsmedel skulle de brottsbekämpande myndigheterna få möjlighet att ta del av elektronisk information som de har rätt, men inte praktisk möjlighet, att inhämta.

Insamling av elektroniskt lagrade uppgifter under förundersökning

Det finns inga särskilda regler om husrannsakan i eller undersökning av elektroniska uppgifter i datorer eller andra informationsbärare. Det finns inte heller några regler i rättegångsbalken som särskilt tar sikte på beslag av elektroniskt lagrade uppgifter. Den allmänna uppfattningen är dock att det inte finns något hinder mot att innehållet i en informationsbärare genomsöks under en husrannsakan. Det krävs då inte något särskilt beslut om husrannsakan för informationsbäraren (betänkandena Tvångsmedel enligt 27 och 28 kap. RB samt polislagen, SOU 1995:47 s. 184 samt Förundersökning – objektivitet, beslag, dokumentation m.m., SOU 2011:45 s. 295 och 296). Ett föremål som har tagits i beslag får undersökas. Den allmänna uppfattningen är att det innefattar en möjlighet att genomsöka det lagrade innehållet i t.ex. en dator eller en mobiltelefon. Genom husrannsakan och beslag av elektroniska informationsbärare får de brottsutredande myndigheterna således tillgång till elektroniskt lagrade uppgifter.

Vid införandet av tvångsmedlen beslag och husrannsakan gjordes bedömningen att det fanns ett behov för de brottsbekämpande myndigheterna att få tillgång till de uppgifter som beslag och husrannsakan ger. liksom vid hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning har det inte framkommit något som tyder på annat än att det behovet alltjämt är gällande.

Husrannsakan och beslag är till skillnad från t.ex. hemlig avlyssning av elektronisk kommunikation inte hemliga tvångsmedel, även om underrättelse till enskild om utförd husrannsakan (men inte beslag) kan skjutas

upp till dess den inte längre är till men för utredningen (28 kap. 7 § rättegångsbalken, jfr dock förslagen om en sorts hemliga beslag i SOU 2017:100). Frågan blir därför om det påtagliga behovet av insamling av elektroniskt lagrade uppgifter även omfattar en metod som i hemlighet kan förse brottsbekämpande myndigheter med sådana uppgifter som beslag och husrannsakan kan ge. Som framgår i avsnitt 8.4 anser regeringen, till skillnad från *Stockholms universitet (Juridiska fakulteten)*, att denna analys kan utföras även utan ett fullständigt statistiskt underlag.

Behovet av nya metoder för insamling av elektroniskt lagrade uppgifter

Flera olika omständigheter gör att uppgifter som tidigare varit möjliga att få ut från teknisk utrustning många gånger inte längre kan samlas in.

En första omständighet är den ökade krypteringsgraden (se avsnitt 7.1). Utredningen redogör för att de brottsbekämpande myndigheterna betraktar krypterade enheter som ett stort problem. För ägaren öppnas enheterna med enkla handgrepp men för utomstående är det närmast omöjligt, t.ex. vid undersökning efter beslag. Flertalet mobiltelefoner är skyddade av lösenkod eller biometriskt skydd (t.ex. upplåsning genom avläsning av fingeravtryck). Även om det skulle gå att komma in i mobiltelefonen kan det vara så att innehållet i appar därefter inte går att komma åt på grund av lösenordsskydd och ytterligare kryptering. De metoder som i dag används av brottsbekämpande myndigheter är att gissa lösenordet genom särskilda program (s.k. brute force), att den misstänkte frivilligt lämnar lösenordet eller att lösenordet hittas nedskrivet någonstans eller erhålls på annat sätt. Att gissa svårare lösenord bedöms vara närmast omöjligt, även med teknisk hjälp.

En annan omständighet som lyfts fram som problem vid undersökningar av teknisk utrustning är förekomsten av raderingsprogram. Sådan programvara kan radera allt eller visst innehåll på teknisk utrustning på en given signal. Sedan sådana program använts finns mycket sällan möjlighet för de brottsutredande myndigheternas it-forensiker att återskapa något av det raderade innehållet. Det innebär att uppgifterna kan vara förlorade redan innan ett beslag hunnit göras och uppgifter i en informationsbärare hunnit säkras. Det är inte enbart särskilda raderingsprogram utan också inbyggda funktioner i modern teknisk utrustning som utgör problem för de brottsbekämpande myndigheterna. I takt med att ny teknik blir allt mer utbredd försvåras således möjligheten att återskapa raderade uppgifter för de brottsbekämpande myndigheterna. Förekomsten av raderingsprogram gör att det finns ett stort behov av att komma åt uppgifterna i hemlighet. Dessutom kan kunskapen om att ett beslag har gjorts medföra kollusions- och flyktfara (SOU 2017:100 s. 612–613). Det gör behovet av hemliga åtgärder än mer påtagligt. Det kan också vara viktigt att få del av lagrad information löpande under ett ärende, eftersom det med hjälp av informationen skulle gå att t.ex. avstyra ett terroristattentat, förhindra annan brottslig verksamhet eller få spaningsuppslag.

Som *Ekobrottsmyndigheten* anför är dagens ordinarie utredningsmetoder såsom spaning oftast inte tillräckliga för att driva förundersökningen framåt. Beslag av datorer räcker inte för bevissäkring i komplexa ärenden, eftersom kryptering eller lösenordsskydd försvårar eller omöjlig-

gör att i efterhand ta fram information från datorn. Förekomsten av raderingsprogram och instruktioner på internet om s.k. antiforensiska metoder talar för att det finns behov av att kunna samla in uppgifter i hemlighet, löpande och i realtid. För detta talar också de fördelar det skulle innebära för de brottsbekämpande myndigheterna, t.ex. att under pågående tvångsmedelsanvändning kunna identifiera brottsplaner, förhindra att brott fullbordas, avvärja överhängande fara och säkra bevis.

Vid en samlad bedömning anser regeringen, i likhet med utredningen, att åtgärder bör vidtas för att ge de brottsbekämpande myndigheterna inte bara rättslig utan också faktisk tillgång till uppgifter som finns elektroniskt lagrade.

Insamling av elektroniskt lagrade uppgifter utanför förundersökning

Till skillnad från vad som gäller under en förundersökning finns det inga regler som tillåter beslag i den brottsförhindrande verksamheten. Det gäller såväl enligt reglerna i preventivlagen som reglerna i lagen (1991:572) om särskild utlänningskontroll, vilka – i nu relevant hänseende – endast tillåter hemlig övervakning och avlyssning av elektronisk kommunikation. Det finns således inte någon möjlighet för de brottsbekämpande myndigheterna att i underrättelseverksamhet komma åt information som finns lagrad i en kommunikationsutrustning, utan det är först när uppgifterna sänds från enheten i t.ex. ett e-brev som de blir åtkomliga genom hemlig avlyssning av elektronisk kommunikation. Det innebär att i den här delen måste en analys göras av i vilken utsträckning det finns ett påtagligt behov av att i underrättelseverksamhet eller vid särskild utlänningskontroll kunna samla in elektroniskt lagrade uppgifter i hemlighet.

I samband med införandet av preventivlagen angav regeringen bl.a. att reglerna om användning av hemliga tvångsmedel, som förutsatte att förundersökning hade inletts och att det fanns någon som var skäligen misstänkt för brott, innebar en begränsning i Säkerhetspolisens möjligheter att ingripa mot och förhindra terroristbrott, spioneribrott och författningshotande brottslighet. Mot denna bakgrund bedömde regeringen i propositionen Åtgärder för att förhindra vissa särskilt allvarliga brott att det på det område där Säkerhetspolisen har ett ansvar för att förhindra att brott begås fanns ett påtagligt behov av att använda tvångsmedel innan förundersökning ännu har inletts och att behovet var särskilt påtagligt inom Säkerhetspolisens verksamhetsgrenar författningsskydd, kontraspionage och kontraterrorism (prop. 2005/06:177 s. 39–40).

När det gällde Polismyndighetens behov av hemliga tvångsmedel gjorde regeringen bedömningen att det fanns ett påtagligt sådant behov för att förhindra vissa särskilt allvarliga brott som kan anses utgöra ett hot mot vårt demokratiska samhällssystem. Det stod enligt regeringen klart att en del av den systemhotande brottsligheten härrörde från vissa kriminella grupperingar vilka, på grund av den ofta mycket starka lojaliteten mellan medlemmarna är svår att bedriva traditionell yttre spaning mot och också mycket svår att infiltrera. Mot den bakgrunden konstaterade regeringen att det inte kunde råda någon tvekan om att en möjlighet för polisen att använda sig av hemliga tvångsmedel för att få information om befarad systemhotande brottslighet skulle vara av betydande värde för brottsbekämpningen och att det förelåg ett påtagligt behov av sådana åtgärder

för att förhindra viss annan systemhotande brottslighet än den som huvudsakligen Säkerhetspolisen ska bekämpa (prop. 2005/06:177 s. 40–41).

Utredningen om vissa hemliga tvångsmedel som bl.a. hade till uppgift att utvärdera preventivlagen konstaterade i sitt betänkande år 2012 att lagen nästan uteslutande hade använts inom Säkerhetspolisens område. De situationer den användes i var när det befarades att allvarliga brott skulle begås och information för att komma vidare i utredningsarbetet inte kunde erhållas på annat sätt men där tillräckligt med information inte fanns för att inleda en förundersökning. Utredningen bedömde att det fanns ett påtagligt behov för Säkerhetspolisen att även utanför en förundersökning kunna använda vissa hemliga tvångsmedel för att förhindra brott. Trots att den öppna polisen inte använde hemliga tvångsmedel i underrättelseverksamhet enligt lagen konstaterade utredningen att en del brott inom den organiserade brottsligheten är av särskild natur, t.ex. brott som i påverkanssyfte riktar sig mot befattningshavare inom rättssystemet, politiker eller företrädare för massmedia. I betänkandet Hemliga tvångsmedel mot allvarliga brott (SOU 2012:44 s. 38) bedömde Utredningen om vissa hemliga tvångsmedel att det fanns ett påtagligt behov även för den öppna polisen att utom en förundersökning kunna använda vissa hemliga tvångsmedel för att förhindra systemhotande brott, en uppfattning som delades av regeringen i propositionen med samma namn (prop. 2013/14:237 s. 69).

I samband med införandet av lagen om särskild utlänningskontroll övervägde regeringen behovet av hemliga tvångsmedel vid särskild utlänningskontroll. Som skäl för behovet av att kunna få tillgång till hemliga tvångsmedel utanför en förundersökning angavs att rättegångsbalkens krav på en specificerad och grundad misstanke innebär en högst betydande skillnad i förhållande till vad som föreskrevs enligt den då gällande terrorismlagstiftningen. Ett exempel på när denna skillnad blir högst påtaglig är när det finns vissa indikationer på att en organisation förbereder ett terrordåd men ingenting som pekar på att en viss bestämd medlem ur organisationen är inblandad. Det är då inte rättsligt möjligt att tillgripa hemliga tvångsmedel mot någon medlem i organisationen enligt rättegångsbalken för att ta reda på om han eller hon t.ex. genom telefonsamtal får information som kan ge underlag för förebyggande skyddsåtgärder. Utan möjlighet till hemliga tvångsmedel vid särskild utlänningskontroll skulle regleringen förlora i effektivitet på ett sätt som inte skulle vara försvarligt av hänsyn till den allmänna hotbild som man för närvarande och under överskådlig tid har att räkna med, se propositionen med förslag till lag om särskild kontroll av vissa utlänningar, m.m. (prop. 1990/91:118 s. 48).

Som Säkerhetspolisen redogör för i sin behovsbeskrivning (se bilaga 2 till utredningens betänkande s. 606–607) ligger det i sakens natur att möjligheten att få tillgång till elektroniskt lagrade uppgifter löpande, alltså utan att invänta att ett beslag genomsökts, många gånger kan vara helt avgörande för att identifiera brottsplaner och förhindra att brott fullbordas. I den brottsförhindrande verksamheten skulle de brottsbekämpande myndigheterna genom hemlig dataavläsning kunna få tillgång till uppgifter som antecknade brottsplaner, fotografier över tänkta brottsplatser och annan lagrad information. Detta skulle redan vid ett tidigt skede kunna ge bättre förutsättningar att hindra t.ex. planerade terrordåd. Det framstår därför som närmast självklart att de elektroniskt lagrade uppgifter som kan hämtas in genom hemlig dataavläsning skulle ha lika stort värde i den

brottsförhindrande verksamheten som i den brottsutredande. Sådana uppgifter är inte möjliga att få tillgång till i dag i den brottsförhindrande verksamheten. De skäl som regeringen anförde i lagstiftningsarbetet med preventivlagen och som redovisas ovan beträffande vikten av att förhindra de brott som Säkerhetspolisen ansvarar för och för annan systemhotande brottslighet gör sig fortfarande gällande. Detsamma gäller de skäl som anfördes för att förhindra terrordåd som anfördes i samband med att lagen om särskild utlänningskontroll infördes. Attentatet på Drottninggatan i Stockholm den 7 april 2017 där en gärningsman med en lastbil körde ihjäl fem personer och skadade många, liksom bombdådet där en ensam gärningsman sprängde sig själv i närheten av Drottninggatan den 11 december 2010 visar hur svårt det är att förhindra sådan brottslighet. Det anförda visar att det finns behov av nya metoder för att kunna förhindra den typen av brottslighet. Med hänsyn till den omfattande digitalisering som samhället genomgått är det dessutom svårt att se att det finns alternativa metoder för att komma åt samma information.

Vid en samlad bedömning anser således regeringen att det föreligger ett påtagligt behov av att kunna samla in elektroniskt lagrade uppgifter i en kommunikationsutrustning även i underrättelseverksamhet och vid särskild utlänningskontroll.

Insamling av uppgifter som inte lagras

Nära frågan om att kunna samla in lagrade uppgifter ligger frågan om att kunna ta del av uppgifter som inte lagras. Vad som här avses är främst uppgifter om hur teknisk utrustning används i olika avseenden. Det kan också t.ex. vara antecknade uppgifter i ett elektroniskt dokument som inte sparas av användaren och angivande av vissa inloggningsuppgifter. I somliga fall förekommer det att uppgifter av det slaget lagras tillfälligt medan de i andra situationer inte lagras alls. Samma sak gäller för exempelvis öppnande av filer, uppstart eller stängning av program och anslutning av externa lagringsmedier till en dator. Hemlig dataavläsning kan användas för att i hemlighet i realtid ta del av vad som sker på den tekniska utrustning som åtgärden avser och alltså fånga upp både uppgifter som lagras och som inte lagras.

Det kan vara en slump vilka uppgifter som lagras och vilka som inte gör det och det skulle vara stötande om de brottsbekämpande myndigheternas förmåga till brottsbekämpning skulle bero på en teknisk slump. Det medför att det ligger nära till hands att bedöma uppgifter som inte lagras på samma vis som sådana som lagras. Säkerhetspolisen har i sin behovsbeskrivning (se bilaga 2 till utredningens betänkande s. 608) framhållit att det är ett problem i den brottsbekämpande verksamheten att de befintliga tvångsmedlen inte ger tillgång till uppgifter som varken kommuniceras till eller från utrustningen eller lagras i denna och att en möjlighet att få del av dessa uppgifter löpande i realtid många gånger kan vara helt avgörande för en framgångsrik brottsbekämpning.

De uppgifter som varken kommuniceras eller lagras kan behövas före, under och efter verkställighet av olika tvångsmedel. De kan t.ex. ge information om vilka lagringsmedia som ska eftersökas. Uppgifterna kan också behövas för att visa minnesanteckningar eller annan tillfälligt upprättad dokumentation och för att se att en person öppnar ett dokument eller ett

program vid ett visst tillfälle samt vad denne har för inloggningsuppgifter till programmen.

Enligt regeringen är behovet av att ta del av uppgifter som inte lagras lika stort som det är för uppgifter som lagras. På samma sätt som för lagrade uppgifter finns ett behov av att kunna utföra åtgärden i hemlighet. I likhet med utredningen anser därför regeringen att åtgärden bör vara tillåten under en förundersökning.

Liksom utredningen bedömer regeringen att det även utanför en förundersökning bör vara tillåtet att läsa av eller ta upp uppgifter om hur ett avläsningsbart informationssystem används. På så sätt skulle de brottsbekämpande myndigheterna i ett tidigt skede kunna övervaka uppgifter som kan komma att användas vid sådan mycket allvarlig brottslighet som preventivlagen och lagen om särskild utlänningskontroll syftar till att förebygga. Tillgång till dessa uppgifter redan i ett tidigt skede kan ge bättre förutsättningar att upptäcka och hindra t.ex. planerade terrordåd.

8.4 Hemlig dataavläsning förväntas vara en effektiv åtgärd

Regeringens bedömning: Hemlig dataavläsning bör kunna användas som metod för att komma åt uppgifter som de brottsbekämpande myndigheterna har ett påtagligt behov av. Åtgärden kommer dock att kunna genomföras i färre ärenden än där det finns behov av den. När hemlig dataavläsning kan genomföras förväntas åtgärden leda till betydligt bättre tillgång till information än vad dagens metoder ger tillgång till.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte bedömningen. *Åklagarmyndigheten* anser att förslagen kommer att innebära en påtaglig effektivisering i det brottsbekämpande arbetet i de fall där hemlig dataavläsning kan verkställas. Några remissinstanser ifrågasätter dock hur effektiv hemlig dataavläsning kommer att bli. *Stockholms universitet (Juridiska fakulteten)* anför att lagförslaget brister i redogörelsen för dess effektivitet. Eftersom det inte finns någon initial statistik (kontrolldata) kommer det att bli omöjligt att utvärdera lagens verkan och effektivitet. Detta strider mot rekommendationer från EU och OECD som menar att ny lagstiftning bör vara evidensbaserad och möjlig att utvärdera såväl ekonomiskt som kvalitativt. Universitetet anser vidare att den tekniska beskrivningen bör kompletteras och att utvecklingen av ny teknik som t.ex. framväxten av sakernas internet (Internet of things) ger en annan bild av den potentiella nyttan än den utredningen gör.

Sveriges advokatsamfund godtar utredningens analys när det gäller tvångsmedlets effektivitet, men anför att det finns risk för att de personer och miljöer som skulle komma att bli föremål för hemlig dataavläsning snabbt skulle utveckla tekniker för att förhindra informationsinhämtningen genom dataavläsning, på samma sätt som skett med traditionell avlyssning.

Skälen för regeringens bedömning

Utgångspunkter för analysen

Att analysera effektiviteten av en ny åtgärd på tvångsmedelsområdet är förenat med svårigheter eftersom flera faktorer som kan antas påverka effektiviteten inte blir kända förrän åtgärden har införts och prövats, samtidigt som åtgärden inte ska införas om den inte kan anses tillräckligt effektiv. Någon bedömning av effektiviteten måste dock göras. Till skillnad från *Stockholms universitet* (*Juridiska fakulteten*) anser regeringen inte att det behövs statistiska data för att kunna göra denna bedömning, eftersom frågornas komplexitet gör att de i allmänhet inte lämpar sig särskild bra för att mätas i siffror (jfr SOU 2012:44 s. 481). Analysen bör i stället vara så bred som möjlig.

Kvantitativ effektivitet

Det kommer att krävas ett omfattande förberedelsearbete och förmåga att möta tekniska svårigheter vid verkställighet av hemlig dataavläsning. Mot den bakgrunden bedömer regeringen i likhet med utredningen att hemlig dataavläsning endast kommer vara möjlig att använda i ett begränsat antal fall. Enligt utredningens experter skulle åtgärden räknat i antalet verkställigheter vara mer jämförbar med hemlig rumsavlyssning än med t.ex. hemlig avlyssning eller övervakning av elektronisk kommunikation. Det tyder på att åtgärden framstår som en i kvantitativ mening begränsat effektiv åtgärd i förhållande till föreliggande behov.

Kvalitativ effektivitet

En kvalitativt effektiv metod är en metod som när den används i ett enskilt fall kan förväntas ge de uppgifter den används för att hämta in.

När hemlig dataavläsning ska genomföras utan att den brottsbekämpande myndigheten har fysisk tillgång till den tekniska utrustningen måste myndigheten i stället utnyttja sårbarheter för att komma åt uppgifterna. Sådana sårbarheter kan vara av olika slag och därför i förlängningen ge tillgång till olika delar av viss teknisk utrustning. Beroende på karaktären på sårbarheten i det enskilda fallet kan det dock finnas begränsningar i vad som går att komma åt. Också andra tekniska faktorer, exempelvis hur säkerheten i form av brandväggar, virusprogram etc. är beskaffad, kan påverka vad som är möjligt att åstadkomma. Sättet att komma över uppgifter kan också variera över tid. Företag som utvecklar hårdvara, programvara eller appar arbetar kontinuerligt för att upptäcka och täppa igen sådana säkerhetsbrister som kan utnyttjas för att komma in i teknisk utrustning. De företag som utvecklar säkerhetssystem arbetar därtill löpande med att upptäcka sådan programvara som kan behöva användas av brottsbekämpande myndigheter vid verkställighet av hemlig dataavläsning.

När hårdvara används vid verkställighet torde det främst vara fråga om s.k. keyloggers eller chip, dvs. hjälpmedel som registrerar tangentnedslag på ett tangentbord och övrig aktivitet i en teknisk utrustning. Detta torde primärt vara möjligt att använda vid verkställighet som avser traditionella datorer. Det finns dock program som är utvecklade för att upptäcka dylika hårdvaror och dessutom kan det finnas risk för att den som utsätts för åtgärden upptäcker utrustningen just eftersom det är fråga om hårdvara.

Vid verkställighet genom användande av inloggningsuppgifter är de uppgifter som den brottsbekämpande myndigheten kan få del av begränsade till den tjänst eller det konto som inloggning sker på. Ett problem i sammanhanget är att det vid inloggning på användarkonton till många tjänster via annan utrustning än den som vanligtvis används förekommer att kontoinnehavaren får ett meddelande om inloggningen. När så sker finns risk för att framtida meddelanden inte kan hämtas in, såväl på grund av att inloggningsuppgifterna ändras som att den som åtgärden avser slutar att använda kontot.

Det synes mot bakgrund av det anförda finnas olika faktorer som kan påverka den kvalitativa effektiviteten av hemlig dataavläsning oavsett vilken teknik för att verkställa åtgärden som används. Även framväxten av ny teknik kan, som *Stockholms universitet (Juridiska fakulteten)* anför, påverka den kvalitativa effektiviteten. Det får dock förutsättas att den brottsbekämpande myndighet som ska verkställa åtgärden har gjort en noggrann kartläggning och analys för att säkerställa att verkställighetstekniken i det enskilda fallet ger tillgång till de uppgifter som eftersöks. Regeringen instämmer därför i utredningens bedömning att åtgärden, när den kan användas, kommer att vara mycket verkningsfull och att de svårigheter som redovisas ovan bör vara beaktade innan verkställighet påbörjas. Som *Åklagarmyndigheten* påtalar kan därför effektiviteten i kvalitativ mening förväntas bli hög.

Effektivitet i relation till resursåtgång

Vad sedan gäller vilka resurser som kommer att krävas för att genomföra hemlig dataavläsning kan först konstateras att resursåtgången i många fall kan jämföras med den resursåtgång som hemlig rumsavlyssning kräver. Det innebär att åtgärden kommer att kräva en hel del personalresurser från den brottsbekämpande myndighet vars ärende det är fråga om. När det gäller arbetet under verkställighet finns det inte skäl att tro att själva insamlingen av uppgifter kommer att kräva vare sig större eller mindre arbetsinsats från de brottsbekämpande myndigheterna än vad som krävs vid verkställighet av befintliga hemliga tvångsmedel. Däremot är sannolikheten stor att det i lyckade verkställighetsärenden, dvs. då de eftersökta uppgifterna kan samlas in, kommer att finnas mer information att ta om hand och analysera än vad som är fallet med befintliga hemliga tvångsmedel. Det innebär att arbetet för de som ska analysera de inhämtade uppgifterna blir mer omfattande än vad som är fallet i dag. En ökad uppgiftsmängd att bearbeta och analysera ställer även högre krav på ändamålsenliga verktyg och arbetsmetoder för analysen. Det kan också konstateras att kostnaderna för utveckling och implementering av den teknik som behövs för hemlig dataavläsning kommer att bli betydande (se avsnitt 15.1).

I förarbetena till hemlig rumsavlyssning anförde regeringen att hemlig rumsavlyssning otvivelaktigt är ett mycket resurskrävande tvångsmedel som kräver omfattande förberedande spaningsinsatser (prop. 2005/06:178 s. 41). Regeringen menade dock att detta inte är något som i sig innebär att man kan säga att hemlig rumsavlyssning är en ineffektiv arbetsmetod. De gånger hemlig rumsavlyssning kan verkställas på ett effektivt sätt får man tillgång till information som man inte hade kunnat skaffa fram på

något annat sätt, eftersom hemlig rumsavlyssning ibland är den enda framkomliga vägen i en utredning. Motsvarande resonemang gör sig gällande för hemlig dataavläsning.

Kriminellas agerande kan påverka effektiviteten

Som *Sveriges advokatsamfund* pekar på kan de kriminellas eget agerande påverka effektiviteten av hemlig dataavläsning. Det kan t.ex. handla om att det görs en uppdatering av den misstänktes dator för att täppa till en säkerhetsbrist. Om säkerhetsbristen är den som de brottsbekämpande myndigheterna tänkt använda vid verkställigheten kan således ett lyckosamt resultat omintetgöras genom en uppdatering. Det kan också handla om att den misstänkte uppmärksammar den teknik som de brottsbekämpande myndigheterna använder, t.ex. en keylogger. I fråga om verkställighet efter inloggning på en misstänkts användarkonto kan det finnas en risk för att den misstänkte får meddelande om att sådan inloggning skett. Nya metoder kan även innebära att kriminella söker efter motåtgärder för att undvika kontroll från de brottsbekämpande myndigheterna som t.ex. en minskad användning av teknisk utrustning för kommunikation. Det hämmar naturligtvis effektiviteten av hemlig dataavläsning men innebär samtidigt att andra, traditionella, spaningsmetoder eller tvångsmedel kan sättas in.

Sammanfattningsvis är det enligt regeringen möjligt att kriminellas beteenden, precis som gäller för de hemliga tvångsmedel som finns i dag, kan påverka möjligheterna till en effektiv verkställighet. Det kan dock inte förmodas att verkställigheten av hemlig dataavläsning på ett generellt plan skulle bli så lidande att den inte längre skulle kunna vara sakligt motiverad.

8.5 Hemlig dataavläsning innebär risker för den personliga integriteten

Regeringens bedömning: Hemlig dataavläsning innebär, vid en jämförelse med nuvarande användning av hemliga tvångsmedel, att riskerna för enskildas personliga integritet ökar.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Merparten av de remissinstanser som yttrar sig särskilt över bedömningen, bl.a. *Justitiekanslern* och *Riksdagens ombudsmän (JO),* instämmer i utredningens bedömning att hemlig dataavläsning i flera avseenden innebär att riskerna för enskildas personliga integritet ökar. Justitiekanslern anför att det därför är av stor vikt att användningen av tvångsmedlet utformas på ett sådant sätt att missbruk omöjliggörs och gränsförskjutningar inte förekommer. *Säkerhets- och integritetsskyddsnämnden* förordar en ingående analys av både de juridiska frågeställningarna och de praktiska möjligheterna att verkställa tvångsmedlet på ett rättssäkert sätt. *Datainspektionen* anser att utredningen undervärderar riskerna för enskilda personers integritet eftersom redan möjligheten för myndigheter att ta del av uppgifter som en person valt att ha krypterade har en direkt påverkan på den personliga integriteten och att detta måste värderas betydligt högre än vad utredningen gör. *Stockholms universitet*

(Juridiska fakulteten) anser att utredningen inte på ett tillräckligt tydligt sätt har belyst de risker som finns med förslaget. Mycket stora resurser kommer att bindas till enstaka fall och om de visar sig vara oriktiga betyder det stora förluster och ett avsevärt integritetsintrång. *Svenska Journalistförbundet* anser att förslaget innebär ett paradigmskifte för användningen av hemliga tvångsmedel i Sverige. Hemlig dataavläsning skulle enligt förbundet innebära att polisen i princip kan göra en husrannsakan i en persons dator och ta del av information som personen valt att inte kommunicera med någon utomstående och detta utan att personen får reda på att polisen har varit där. Även *Civil Rights Defenders*, *Dataskydd.net, Föreningen för digitala fri- och rättigheter, Stiftelsen för Internetinfrastruktur (Internetstiftelsen)* och *Google Sweden AB (Google)* anser att förslaget riskerar att utgöra ett mycket stort intrång i den personliga integriteten.

Skälen för regeringens bedömning

Personlig integritet som begrepp

Som framgår i avsnitt 4.2 finns ett grundlagsstadgat skydd för den enskildes privatliv – den personliga integriteten. Det har i flera statliga utredningar gjorts försök att definiera begreppet personlig integritet (se bl.a. betänkandena Skyddet för den personliga integriteten, Del 1, SOU 2007:22, s. 53–62, Integritet och straffskydd, SOU 2016:7 s. 63–75 och Hur står det till med den personliga integriteten?, SOU 2016:41 s. 136–147). Det är svårt att ge en positiv bestämning av den personliga integriteten, dvs. att formulera en beskrivning som pekar ut alla de situationer i vilka individen har rätt att få sin integritet respekterad och skyddad. Trots svårigheterna är det nödvändigt att veta vad som avses när begreppet används. Integritetskommittén uttryckte detta som att innebörden måste vara tillräckligt tydlig för att det ska vara möjligt att avgöra vad som innebär en kränkning eller ett otillbörligt intrång (SOU 2016:41 s. 148). När det gäller hemliga tvångsmedel uttryckte Utredningen om vissa hemliga tvångsmedel att den personliga integritetens kärnområden, dvs. sådant som rör individen och dennes personlighet, var det relevanta för den analys utredningen hade att göra. Inom den personliga integritetens kärnområden omfattas information om den enskilde inklusive identifieringsdata avseende den enskildes bild, namn och liknande. Utredningen konstaterade också att varje befogenhet för staten att bereda sig tillgång till personlig information om den enskilde och varje nyttjande av sådan information leder till ingrepp i den personliga integriteten. Graden av integritetsintrång varierar med tvångsmedlets utformning och tillämpning (SOU 2012:44 s. 480).

Dagens regler utgör utgångspunkten

Vid bedömningen av om hemlig dataavläsning utgör en ökad risk för enskildas personliga integritet utgår utredningen från nuläget, dvs. utredningen gör sin bedömning utifrån en jämförelse med vad som gäller i dag. Utredningen utgår även från att befintliga tvångsmedel alltjämt är nödvändiga och godtagbara ur integritetssynpunkt. *Datainspektionen* anser att

utredningen undervärderar riskerna för enskilda personers integritet och att man inte borde utgå ifrån nuvarande regler som en normerande nivå.

Regeringen delar inledningsvis utredningens bedömning att de avvägningar mellan en effektiv brottsbekämpning och de risker för den personliga integriteten som ligger till grund för befintliga tvångsmedel alltjämt är gällande. Som *Stockholms universitet (Juridiska fakulteten)* anför innebär hemlig dataavläsning att stora resurser kommer att bindas till enstaka fall. Utredningarna kan, i synnerhet om de avser oskyldiga, leda till betydande integritetsintrång. Sådana risker finns dock redan enligt dagens regler om bl.a. hemlig rumsavlyssning. Någon principiell skillnad mellan olika metoder för inhämtning av information föreligger alltså inte enligt regeringen, även om själva verkställighetsmetoden i sig kan vara integritetskränkande (se mer om det nedan). Regeringen anser därför, i likhet med utredningen, att bedömningen om hemlig dataavläsning innebär ökade risker för den personliga integriteten bör göras med utgångspunkt i dagens regler. För att minimera riskerna för den personliga integriteten är det som *Justitiekanslern* framhåller av stor vikt att regleringen av ett nytt tvångsmedel utformas på ett sådant sätt att missbruk omöjliggörs och gränsförskjutningar inte förekommer.

Hemlig dataavläsning för att ta del av innehåll i och uppgifter om meddelanden

Datainspektionen anser att redan möjligheten för myndigheter att ta del av uppgifter som en person valt att ha krypterade har en direkt påverkan på den personliga integriteten och att det måste värderas betydligt högre än vad utredningen gör. Med dagens regler är det emellertid tillåtet för de brottsbekämpande myndigheterna att försöka dekryptera krypterade uppgifter som de fått in vid hemlig avlyssning av elektronisk kommunikation. Om hemlig dataavläsning används för att läsa av innehållsuppgifter eller uppgifter om meddelanden är metoden närmast att jämföra med sådan dekryptering. Hemlig dataavläsning utgör då ett sätt att komma runt vissa av de tekniska problem som finns i dag. Utredningen anser därför att det inte uppstår någon ökad risk för den personliga integriteten om hemlig dataavläsning används för att läsa av innehåll i och uppgifter om meddelanden. I sammanhanget ska nämnas att det förhållandet att kryptering ökar inte enbart är ett val som den enskilde gör utan beror till stor del på att kommunikation överlag krypteras i större omfattning än tidigare. Sammantaget innebär hemlig dataavläsning för att läsa av innehållet i meddelanden enligt regeringens mening inte någon beaktansvärd ökad risk för den personliga integriteten.

Hemlig dataavläsning för att ta del av uppgifter om geografisk position

I den befintliga lagstiftningen avseende inhämtning av lokaliseringsuppgifter görs ingen skillnad på hur detaljerade uppgifter som kan erhållas. Det finns t.ex. fler master som en mobiltelefon kan koppla upp sig mot i stadsmiljö än på landsbygden. Med hemlig dataavläsning skulle uppgifterna kunna bli mer detaljerade än i stadsmiljö och det skulle dessutom inte krävas att mobiltelefonen kopplar upp sig mot en mast för att myndigheterna ska kunna hämta in uppgifter om geografisk position. Det innebär

enligt regeringens mening att hemlig dataavläsning för att ta del av uppgifter om geografisk position medför en viss ökad risk för den personliga integriteten jämfört med dagens ordning.

Hemlig dataavläsning för att ta del av kameraövervaknings- och rumsavlyssningsuppgifter

Hemlig dataavläsning kan ge tillgång till samma uppgifter som i dag kan samlas in med hemlig kameraövervakning eller hemlig rumsavlyssning, t.ex. genom att en mobiltelefons kamera eller mikrofon aktiveras och att uppgifterna därefter läses av. Om åtgärden skulle användas med de begränsningar som gäller för hemlig kameraövervakning eller hemlig rumsavlyssning skulle det inte medföra någon ökad risk för den personliga integriteten eftersom uppgifter som kan läsas av med hemlig dataavläsning skulle motsvaras av dem som får hämtas in i dag.

Bedömningen skulle dock bli annorlunda om motsvarande begränsningar avseende plats som gäller för hemlig kameraövervakning och hemlig rumsavlyssning inte skulle gälla för hemlig dataavläsning. Hemlig dataavläsning kan användas för att t.ex. aktivera en mikrofonfunktion i en mobiltelefon och göra det möjligt att höra varje ord på alla de platser som den misstänkte befinner sig. Detta innebär risker för den personliga integriteten för såväl den som utsätts för åtgärden som för andra som befinner sig i närheten. Samma risker gäller vid aktivering av en kamera i t.ex. en mobiltelefon.

Om hemlig dataavläsning skulle tillåtas utan krav på precisering av plats för att läsa av kameraövervaknings- eller rumsavlyssningsuppgifter skulle det vara nästintill omöjligt att ta ställning till vilka integritetsintrång som åtgärden skulle kunna medföra i det enskilda fallet. Dessutom får det antas att myndigheterna skulle få tillgång till en mycket stor mängd uppgifter utan betydelse för ärendet. Regeringen delar därför utredningens uppfattning att en sådan ordning skulle innebära allvarligt ökade risker för den personliga integriteten både för den som utsätts för åtgärden och för personer som befinner sig i dennes närhet. Åtgärden bör därför inte tillåtas utan platskrav (se avsnitt 10.1.4). Med denna begränsning innebär enligt regeringens bedömning hemlig dataavläsning för att ta del av kameraövervakningsuppgifter och rumsavlyssningsuppgifter inte någon beaktansvärd ökad risk för den personliga integriteten.

Hemlig dataavläsning för att ta del av elektroniskt lagrade uppgifter och uppgifter som visar hur viss teknisk utrustning används

Svenska Journalistförbundet anser att hemlig dataavläsning innebär ett paradigmskifte för användningen av hemliga tvångsmedel i Sverige och att hemlig dataavläsning skulle innebära att polisen i princip kan göra husrannsakan i en persons dator och ta del av information som personen valt att inte kommunicera med någon utomstående och detta utan att personen i fråga får reda på att polisen varit där. Även *Civil Rights Defenders, Dataskydd.net, Föreningen för digitala fri- och rättigheter, Internetstiftelsen* och *Google* är kritiska och anser att förslaget riskerar att utgöra ett mycket stort intrång i den personliga integriteten. Å ena sidan är det uppenbart att en fullständig avläsning av t.ex. någons mobiltelefon utgör ett mycket stort intrång i den drabbades personliga sfär då en mobiltelefon

eller annan liknande utrustning kan innehålla mycket känsliga och personliga uppgifter. Å andra sidan måste beaktas att risken för ett sådant intrång finns redan i dag vid beslag av en mobiltelefon under en förundersökning. Denna risk finns dock enbart under en förundersökning då det enligt dagens regler inte är möjligt att beslagta en mobiltelefon i underrättelseverksamhet. Det går således redan i vissa situationer att få tag på uppgifterna i fråga, men vid ett senare skede än vad som kan bli fallet med hemlig dataavläsning. Det kan hävdas att integritetsintrånget vid genomsökning av en teknisk utrustning efter ett beslag är högre än om åtgärden vidtas utan att den tekniska utrustningen fråntas den som åtgärden gäller, även om integritetsintrånget av att vid ett visst givet tillfälle inte få disponera elektronisk utrustning generellt sett får sägas vara begränsat. Samtidigt ökar integritetsintrånget genom att åtgärden vidtas i hemlighet. Vid en samlad bedömning delar regeringen utredningens uppfattning att insamling av elektroniskt lagrade uppgifter innebär en ökad risk för den personliga integriteten jämfört med dagens förhållanden.

Utredningen föreslår att hemlig dataavläsning även ska kunna användas för att samla in uppgifter som visar hur teknisk utrustning används. Det kan t.ex. röra sig om övervakning av hur en enskild använder utrustningen, alltså vilka program som används och vilka inloggningsuppgifter som anges. Sådana uppgifter är typiskt sett integritetskänsliga. Ibland finns sådana uppgifter lagrade, eller i vart fall är möjliga att återskapa vid t.ex. en undersökning av ett beslag. I sådana fall kan de brottsbekämpande myndigheterna alltså samla in uppgifterna. I och med att hemlig dataavläsning utförs i hemlighet och ger tillgång till fler och mer fullständiga uppgifter skulle åtgärden, i synnerhet om den genomförs utanför en förundersökning, innebära en ökad risk för den personliga integriteten jämfört med dagens förhållanden.

Intrång i samband med verkställighet

För att kunna verkställa ett beslut om hemlig dataavläsning kommer det i vissa fall att vara nödvändigt att skaffa sig tillgång till den fysiska utrustningen som åtgärden ska avse. Det kan t.ex. röra sig om intrång i annars skyddade utrymmen som bostäder. Sådana intrång är i dag möjliga efter särskilt tillstånd vid hemlig rumsavlyssning och vid husrannsakan. Om det för att hemlig dataavläsning ska kunna verkställas krävs att brottsbekämpande myndigheter ges tillstånd att tränga in i annars skyddade utrymmen ökar således risken för integritetsintrång jämfört med nuvarande reglering. Regeringen bedömer i likhet med utredningen att det rör sig om en viss ökad risk för den personliga integriteten.

Vid verkställighet av hemlig dataavläsning kan olika tekniker aktualiseras, t.ex. utnyttjande av kända inloggningsuppgifter eller av sårbarheter i teknisk utrustning. Dessutom kräver hemlig dataavläsning många gånger att den verkställande myndigheten installerar något slags program- eller hårdvara i en annan persons dator, mobiltelefon eller liknande för att åtgärden ska fungera. Att utan lov från innehavaren ta sig in i dennes tekniska utrustning eller installera programvara i den, alternativt fästa hårdvara på den, kan i sig vara ett allvarligt intrång i den drabbade personens skyddade sfär. Själva intrånget och installation av program eller hårdvara i utrust-

ningen måste dock ses som en mindre integritetsrisk än den risk det innebär att staten i hemlighet kan ta del av personlig information som finns i utrustningen. Redan intrånget i utrustningen och installationen av program eller hårdvara innebär dock enligt regeringens mening en ökad risk från integritetssynpunkt. En förutsättning för att ett sådant intrång ska tillåtas bör vara att det omgärdas av tydliga regler med högt ställda krav på rättssäkerhet. När det är fråga om intrång i skyddade utrymmen, t.ex. bostäder, bör det krävas att den tekniska utrustning som hemlig dataavläsning ska avse finns tillgänglig på eller genom den plats där intrånget ska ske (se vidare avsnitt 10.4).

8.6 Det är proportionerligt att införa regler om hemlig dataavläsning

Regeringens bedömning: Det är proportionerligt att införa regler om hemlig dataavläsning under förutsättning att dessa balanseras med rättssäkerhetsgarantier och regler för att minska riskerna för informationssäkerheten.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Remissutfallet är blandat. Majoriteten av remissinstanserna instämmer i bedömningen eller lämnar den utan kommentarer.

Bland andra *Riksdagens ombudsmän (JO), Svea hovrätt, Stockholms tingsrätt, Göteborgs tingsrätt, Luleå tingsrätt, Justitiekanslern, Åklagarmyndigheten, Ekobrottsmyndigheten, Migrationsverket, Tullverket, Myndigheten för samhällsskydd och beredskap, Sveriges läkarförbund, Svenska kyrkan* och *Sveriges kristna råd* anför att utredningens avvägning mellan den personliga integriteten och effektiviteten i brottsbekämpningen framstår som rimlig och att förslaget försetts med tillräckliga rättssäkerhetsgarantier. *Säkerhets- och integritetsskyddsnämnden* delar denna bedömning såvitt avser hemlig dataavläsning för att få del av uppgifter avseende elektronisk kommunikation, uppgifter om geografisk position och elektroniskt lagrade uppgifter samt uppgifter som visar hur ett informationssystem används.

Ett antal remissinstanser, bl.a. *Datainspektionen, Sveriges advokatsamfund, Svenska Journalistförbundet, Föreningen för digitala fri- och rättigheter, Stiftelsen för Internetinfrastruktur (Internetstiftelsen)* och *Google Sweden AB (Google)*, anser inte att det är proportionerligt att införa regler om hemlig dataavläsning och avstyrker förslaget. Google menar att hemlig dataavläsning i den omfattning som beskrivs i förslaget skulle innebära ett mycket stort ingrepp i den personliga integriteten utöver vad som tillåts inom befintliga hemliga tvångsmedel. Om lagen införs i enlighet med förslaget kommer detta, enligt Google, att innebära att myndigheter får möjlighet att fullständigt kartlägga en persons liv.

Säkerhets- och integritetsskyddsnämnden avstyrker att hemlig dataavläsning införs för uppgifter som innebär optisk personövervakning och rumsavlyssningsuppgifter, eftersom den föreslagna tillämpningen enligt nämnden kommer att innebära en väsentlig utökning av myndigheternas möjlighet att i hemlighet kartlägga enskildas liv. Eftersom verkställighet i

dessa delar endast får äga rum på i förhand beslutade platser är det nödvändigt att den brottsbekämpande myndigheten känner till exakt var en elektronisk utrustning finns under hela verkställighetstiden. Nämnden anför vidare att utredningen inte närmare analyserar vilka konsekvenser det får att regleringen om hemlig dataavläsning i sin helhet utformas som ett nytt tvångsmedel när den till större delen behandlar en särskild verkställighetsform av befintliga tvångsmedel. Förslaget innebär även en viss dubbelreglering i förhållande till vad som gäller för de hemliga tvångsmedlen i rättegångsbalken.

Internetstiftelsen vill att alla ska vilja, våga och kunna använda internet och stiftelsen är angelägen om att användningen av internet omgärdas med transparenta förfaranden och adekvata skyddsmekanismer samt att tvångsmedel som syftar till brottsbekämpning begränsas till vad som är nödvändigt och proportionerligt. Stiftelsen anför vidare att det finns en uppenbar risk att de åtgärder som de brottsbekämpande myndigheterna ska få vidta för att kunna genomföra hemlig dataavläsning bidrar till en osäkrare digitaliserad tillvaro för alla genom att säkerhetshål i verktyg och tjänster inte täpps till så snabbt som de skulle kunna.

Civil Rights Defenders avstyrker att hemlig dataavläsning ska få användas för att läsa av eller ta upp uppgifter som visar hur ett informationssystem används. Om Sverige ska leva upp till sina internationella åtaganden anser Civil Rights Defenders att förslaget måste kompletteras med mer effektiva rättsmedel för den enskilde, att kraven för hemlig dataavläsning behöver sättas högre än de krav som ställs för hemlig avlyssning av elektronisk kommunikation och att hemlig dataavläsning i underrättelseverksamhet endast bör kunna användas av Säkerhetspolisen vid misstanke om mycket allvarlig brottslighet som utgör brott mot rikets säkerhet. *Sveriges advokatsamfund*, *Internetstiftelsen* och *Svenska stadsnätsföreningen* har samma uppfattning som Civil Rights Defenders.

Myndigheten för samhällsskydd och beredskap stödjer utredningens slutsats att det inte är lämpligt att kräva att teknikföretag och tjänstetillhandahållare ska tillhandahålla bakdörrar in i systemen för brottsbekämpande myndigheter och att det inte heller är lämpligt att försvaga krypteringsmöjligheterna. Myndigheten vill dock betona att det är olyckligt att den kunskap som byggs upp kring informationssäkerhetsbrister i samband med hemlig dataavläsning inte i något skede och inte på något sätt ska kunna nyttjas för att stärka skyddet för sådana system som samhällsviktig verksamhet är beroende av. Det finns ett behov av en fördjupad analys om möjlig informationsdelning som tillgodoser både brottsbekämpande myndigheters behov av att genomföra hemlig dataavläsning och myndighetens möjligheter att stödja och säkra informations- och cybersäkerheten, särskilt i samhällsviktig verksamhet. *Stockholms universitet (Juridiska fakulteten)* framför att det finns en risk att allmänt spridd kunskap om att de brottsbekämpande myndigheterna använder sig av en viss teknik kan få till effekt att systemet avsiktligt kommer att överbelastas eller missbrukas. Systematiskt missbruk kommer enligt universitetet inte bara att binda stora resurser utan även vara komplicerade att utreda och utredningarna kommer i sig att utgöra avsevärda integritetsintrång för de oriktigt utpekade. *Dataskydd.net* framför att sanktionerade dataintrång orsakar risker och skador för civila verksamheter och att förfarandet därför av säkerhetsskäl bör begränsas.

Föreningen för digitala fri- och rättigheter anser att de eventuella effektivitetsvinster som finns för brottsbekämpande myndigheter inte är tillräckligt stora för att motivera användandet av hemlig dataavläsning. Föreningen anför att säkra och effektiva sätt att kommunicera digitalt är en förutsättning för ett demokratiskt samhälle och att medborgarna och även institutioner har rätt att slippa avlyssnas av staten.

Svenska Journalistförbundet anser inte att utredningen har beaktat de negativa konsekvenser som förslaget medför för medborgare som inte begår brott. Förbundet anser att de positiva effekter som går att vinna i brottsbekämpande verksamhet inte uppväger förslagets förmodade integritetskränkningar och att förslaget därför inte är proportionerligt. Enligt förbundet innebär hemlig dataavläsning helt nya problem när det gäller möjligheten att skydda källor. Tidigare har journalister kunnat ha material som omfattas av källskyddet på sina datorer utan att riskera att någon annan kan ta del av det. Med det nya förslaget om hemlig dataavläsning finns det anledning att ifrågasätta om man som journalist kan ha material som omfattas av källskyddet på en dator som är möjlig att gå in i med hjälp av hemlig dataavläsning. *Internetstiftelsen* anför att trots att polisen är skyldig att upphöra med avlyssningen om det kommer fram uppgifter som omfattas av källskydd så är skadan redan skedd och källan får anses vara röjd.

Telia Company AB anser att ett kraftfullt tvångsmedel som hemlig dataavläsning medför risker som är svåra att bedöma art och omfattning av, bland annat vad gäller upprätthållandet av krav på driftsäkerhet och integritet i telenäten.

Kungliga tekniska högskolan (KTH) anför att det är viktigt att hemlig dataavläsning endast brukas för avsett ändamål och att inte exempelvis teknikens utveckling tillåts utöka användningen utan att nya politiska beslut fattas. Liknande synpunkter framförs av *Sveriges advokatsamfund* och *Svenska stadsnätsföreningen*.

Skälen för regeringens bedömning

En förutsättning för att införa bestämmelser om hemlig dataavläsning är att tvångsmedlet är proportionerligt i förhållande till behov, effektivitet och integritet. Utredningens sammantagna slutsats är att hemlig dataavläsning uppfyller detta krav. I de föregående avsnitten konstaterar regeringen att det finns ett påtagligt behov av hemlig dataavläsning och att det är ett effektivt tvångsmedel. Regeringen konstaterar också att hemlig dataavläsning är förenad med vissa ökade integritetsrisker. I det följande redovisar regeringen sina bedömningar och de avgränsningar som krävs för att hemlig dataavläsning ska vara en proportionerlig åtgärd.

Informationssäkerhet och hemlig dataavläsning

Informationssäkerhet har en central plats i informationssamhället. Vikten av en fungerande informationssäkerhet för samhället och dess medborgare måste vägas mot vikten av en effektiv brottsbekämpning. Proportionalitetsbedömningen måste därför göras inte enbart i förhållande till de integritetsrisker som hemlig dataavläsning för med sig utan också i förhållande till informationssäkerheten. I sammanhanget kan noteras att

risker för informationssäkerheten kan, men behöver inte, påverka frågor om risker för den personliga integriteten.

Verkställighet av hemlig dataavläsning med programvara kommer kräva att de brottsbekämpande myndigheterna dels gör intrång i den tekniska utrustning som de relevanta uppgifterna finns i, dels installerar hård- eller mjukvara i systemet. *Föreningen för digitala fri- och rättigheter* anser att åtgärderna bidrar till en osäkrare digitaliserad tillvaro för alla. Liknande synpunkter framförs av *Internetstiftelsen* och *Telia Company AB*. De anför att allmänheten, genom att de brottsbekämpande myndigheterna aktivt söker sårbarheter i informationssystem och sedan bygger verktyg för att utnyttja dessa säkerhetsluckor, utsätts för stora risker eftersom säkerhetshål inte täpps igen så snabbt som de skulle kunna. *Dataskydd.net* anför att metoden utgör ett sanktionerat dataintrång och att förfarandet orsakar risker och skador för civila verksamheter och därför bör begränsas. *Stockholms universitet (Juridiska fakulteten)* framför att det finns en risk att allmänt spridd kunskap om att de brottsbekämpande myndigheterna använder sig av en viss teknik kan få till effekt att systemet avsiktligt kommer att överbelastas eller missbrukas. Systematiskt missbruk kommer enligt universitetet inte bara att binda stora resurser utan även vara komplicerade att utreda och utredningarna kommer i sig att utgöra avsevärda integritetsintrång för de oriktigt utpekade.

Stark informationssäkerhet är ett så viktigt samhällsintresse i dag att det som remissinstanserna och utredningen påpekar knappast kan accepteras att åtgärder vidtas av brottsbekämpande myndigheter som leder till minskad informationssäkerhet i någon annan utrustning än den som åtgärden avser. Detta innebär enligt regeringens mening att hemlig dataavläsning, trots de fördelar som åtgärden kan innebära för brottsbekämpningen, endast bör tillåtas om det vidtas nödvändiga åtgärder för att informationssäkerheten i system utanför utrustningen som åtgärden avser inte ska minska till följd av åtgärden. För detta behövs det en tydlig reglering som ålägger de brottsbekämpande myndigheterna att vidta aktiva åtgärder under hela den tid som verkställighet ska pågå (se avsnitt 11.2.3).

Det förhåller sig något annorlunda i frågan om det kan accepteras att hemlig dataavläsning innebär minskad informationssäkerhet i den tekniska utrustning som åtgärden avser. I den delen redogör utredningen för vilka alternativ det finns till hemlig dataavläsning och vilken påverkan de olika alternativen har för den personliga integriteten. Ett alternativ är att kräva av teknikföretag och tjänstetillhandahållare att de ska kunna gå förbi säkerheten i sina egna system och tjänster för att bistå brottsbekämpningen, t.ex. genom att använda bakdörrar. Riskerna med en sådan lösning är svåra att bedöma men det kan antas att så snart det är möjligt för någon att gå förbi säkerhetslösningar så torde likadana möjligheter öppnas även för andra, också kriminella, vilket kan medföra stora risker för såväl informationssäkerheten som för den personliga integriteten. Ett annat alternativ är att systematiskt arbeta med att försvaga krypteringslösningar eller standarder för kryptering. Att generellt eller systematiskt försvaga krypteringslösningar för att komma åt uppgifter kan få stora återverkningar på hela den legitima användningen av den moderna tekniken. Regeringen bedömer sammanfattningsvis, i likhet med utredningen och *Myndigheten för samhällsskydd och beredskap*, att alternativen till att införa regler om hemlig dataavläsning inte är tillfredsställande och riskerar

att ha ännu större negativ inverkan på både den personliga integriteten och informationssäkerheten generellt. De risker som kan uppstå till följd av minskad informationssäkerhet i den tekniska utrustning som hemlig dataavläsning avser kan enligt regeringen accepteras. Detta förutsätter dock att åtgärderna balanseras mot väl avvägda regleringar för att minimera riskerna. Det kräver också att det sedan åtgärden har avslutats inte finns några kvardröjande informationssäkerhetsrisker (se vidare avsnitt 11.2.3).

Risk för tillämpningsglidningar

Den lagstiftning som föreslås är teknikneutral. Även om syftet med en teknikneutral lagstiftning är att den ska kunna stå sig över tid kan sådan lagstiftning öka risken för tillämpningsglidningar. Det innebär att lagstiftningen i takt med en snabb teknisk utveckling får ett mer omfattande tillämpningsområde än vad som var tänkt från början. Problemet med en sådan utveckling är i detta sammanhang att riskerna för den personliga integriteten typiskt sett ökar om regler om tvångsmedel med tiden får ett vidare tillämpningsområde än vad de från början var tänkta att ha.

Det finns ingenting som tyder på att den tekniska utvecklingen kommer att avstanna. Den snabba tekniska utvecklingen kan som *Sveriges advokatsamfund* och *KTH* anför innebära en risk för att lagstiftningen i framtiden kan komma att tillämpas på ett sätt som inte var avsett när reglerna infördes. Det får till följd att det finns en viss ökad risk för den personliga integriteten om hemlig dataavläsning införs.

För att motverka tillämpningsglidningar bör det, som utredningen anför, framgå tydligt i lagstiftningen vilka förutsättningar som gäller för att en viss typ av uppgifter ska få samlas in med hemlig dataavläsning. Bland åtgärder som motverkar tillämpningsglidning kan nämnas domstolsprövning och användande av offentligt ombud (se vidare avsnitt 11.1.1 och 11.1.3). För att ytterligare motverka risken bör lagstiftningen ange vilken typ av utrustning åtgärden får avse och vilken typ av uppgifter som får samlas in. Också framtida utvärderingar av åtgärden inklusive kontroll av hur tillämpningen ser ut kan hjälpa till att motverka denna risk (se avsnitt 12.1.5).

Hemlig dataavläsning bör differentieras i varje enskilt fall

Hemlig dataavläsning skulle, som bl.a. *Google* framhåller, kunna innebära en omfattande kartläggning av en persons förehavanden och ge information om var den som blir föremål för åtgärden befinner sig, vem personen talar med, vad han eller hon säger och gör i princip dygnet runt. Använt på det sättet skulle tvångsmedlet bidra till en allvarligt ökad risk för integritetsintrång.

Redan dagens tvångsmedel kan emellertid ge tillgång till i stort sett alla de typer av uppgifter som hemlig dataavläsning skulle kunna ge tillgång till. Det saknas formella hinder mot att samtliga befintliga hemliga tvångsmedel samtidigt kan riktas mot en och samma person, förutsatt att det har bedömts vara proportionerligt. Vad som skulle vara unikt med hemlig dataavläsning vore om åtgärden alltid gav möjlighet till insamling av alla de typer av uppgifter som är möjliga att hämta in med den. Det skulle vara problematisk ur integritetssynpunkt. Befintliga tvångsmedel har olika

trösklar som bestämmer när de får användas. De skiljer sig åt bl.a. beträffande vilka brott som krävs för att tillstånd till tvångsmedlet ska kunna beviljas. Det är också reglerat på olika sätt vad som får samlas in i underrättelseverksamhet och när förundersökning pågår. Hemlig rumsavlyssning är t.ex. inte möjlig att använda i underrättelseverksamhet och det är vid inhämtning enligt inhämtningslagen endast möjligt att hämta in vissa typer av uppgifter. De överväganden som ligger till grund för sådana olikheter grundar sig framför allt i de skillnader i integritetsintrång som kan uppstå om brottsbekämpande myndigheter får tillgång till de olika uppgifterna. Dessa skillnader består även om uppgifterna hämtas in genom hemlig dataavläsning, vilket redovisas nedan i detta avsnitt.

Även om det är nödvändigt att införa hemlig dataavläsning för att komma åt många olika slags uppgifter bör behovet av uppgifter i varje enskilt fall vara styrande för vad hemlig dataavläsning får och ska kunna användas för i det enskilda fallet. Utredningen benämner detta som att åtgärden bör differentieras. Om en brottsbekämpande myndighet t.ex. behöver komma åt uppgifter från krypterad kommunikation i en mobiltelefon bör åtgärden inte också per automatik ge tillgång till alla bilder, filer och lösenord som finns sparade i telefonen. En lösning där åtgärden differentieras redan när tillstånd beviljas innebär enligt regeringens mening att riskerna för den personliga integriteten minskar jämfört med om hemlig dataavläsning alltid skulle tillåta att alla uppgifter samlas in på en och samma gång. Det innebär även enligt regeringens mening att den kartläggning av en persons liv som bl.a. *Google* befarar, undviks. För att hemlig dataavläsning bör differentieras i varje enskilt fall talar även de svårigheter som annars kan uppstå vid tillståndsprövningen. Utan en sådan differentiering är det nämligen svårt att se hur en proportionalitetsbedömning skulle kunna göras. Utgångspunkten bör i stället vara att hemlig dataavläsning ska kopplas till varje uppgiftstyp som åtgärden bedöms nödvändig för och därmed utgöra ett komplement till befintliga tvångsmedel.

Säkerhets- och integritetsskyddsnämnden saknar en analys av vilka konsekvenser det får att regleringen i sin helhet utformas som ett nytt tvångsmedel när den till större delen behandlar en särskild verkställighetsform av befintliga tvångsmedel. Att hemlig dataavläsning kopplas till varje uppgiftstyp kan som nämnden påpekar innebära en viss dubbelreglering eftersom de flesta av de uppgifter som kan samlas in med hemlig dataavläsning redan kan samlas in genom befintliga tvångsmedel. Eftersom hemlig dataavläsning föreslås regleras i en egen lag (se avsnitt 9.1) med egna tillståndsrekvisit är dock regeringens uppfattning att de otydligheter som nämnden pekar på är försumbara. Tvärtom kommer hemlig dataavläsning i första hand att användas när andra tvångsmedel inte är framkomliga alternativ (se avsnitt 9.4).

Hemlig dataavläsning för att ta del av innehåll i och uppgifter om meddelanden

Som konstateras i avsnitt 8.2 finns det ett påtagligt behov av en ny metod för att de brottsbekämpande myndigheterna i hemlighet ska kunna få tillgång till uppgifter i teknisk utrustning beträffande innehåll i och uppgifter om meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät. Dessa uppgifter kan i dag hämtas in genom hemlig

avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation eller inhämtning enligt inhämtningslagen. Hemlig dataavläsning kan vara en effektiv metod för att få tillgång till sådana uppgifter.

Eftersom uppgifterna kan hämtas in i hemlighet redan i dag uppstår det enligt regeringens bedömning inga påtagligt ökade risker för den personliga integriteten om hemlig dataavläsning införs. Den enda skillnaden jämfört med dagens tvångsmedel är att de brottsbekämpande myndigheterna med hjälp av hemlig dataavläsning kan genombryta anonymisering och kryptering och därmed återfå den förmåga som det ursprungligen var tänkt att de skulle ha. Hemlig dataavläsning bör i denna del endast få användas vid sådana brott som kan föranleda användning av hemlig avlyssning av elektronisk kommunikation (se vidare avsnitt 10.1.1 och 10.2.1).

Hemlig dataavläsning för att ta del av uppgifter om geografisk position

Det finns, som anges i avsnitt 8.2, ett påtagligt behov av nya och bättre metoder för att samla in uppgifter om var en viss teknisk utrustning befinner sig, dvs. en uppgiftstyp som kan hämtas in genom hemlig övervakning av elektronisk kommunikation och inhämtning enligt inhämtningslagen. Hemlig dataavläsning kan ge tillgång till mer precisa uppgifter än de som enligt gällande regler får samlas in, t.ex. om det vore tillåtet att aktivera en GPS-utrustning i en mobiltelefon och sedan läsa av uppgifterna. Utöver de integritetsrisker som följer av själva metoden för hemlig dataavläsning, finns en viss ökad risk om hemlig dataavläsning får användas på detta sätt jämfört med dagens förhållanden.

Den ökade integritetsrisken är dock, i jämförelse med behovet, inte så stor att den bör hindra ett införande av metoden. En viss ökad risk för den personliga integriteten får alltså enligt regeringens mening accepteras för att ge de brottsbekämpande myndigheterna mer effektiva åtgärder. Hemlig dataavläsning bör således få användas för att ta del av uppgifter om geografisk position. Sådana uppgifter bör inte få läsas av med hemlig dataavläsning för mindre allvarliga brott än sådana som kan föranleda användning av hemlig avlyssning av elektronisk kommunikation (se vidare avsnitt 10.1.1 och 10.2.1).

Hemlig dataavläsning för att ta del av kameraövervaknings- och rumsavlyssningsuppgifter

Som anges i avsnitt 8.2 föreligger det ett påtagligt behov av nya metoder för att samla in sådana uppgifter som i dag får samlas in efter tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning. Regeringen delar inte *Säkerhets- och integritetsskyddsnämndens* bedömning att åtgärden inte bör införas. Regeringen anser i stället, mot bakgrund av vad som konstateras i avsnitt 8.5 om risker för den personliga integriteten, att hemlig dataavläsning bör få användas för att läsa av kameraövervakningseller rumsavlyssningsuppgifter under motsvarande förhållanden som gäller för hemlig kameraövervakning och hemlig rumsavlyssning i dag. I likhet med utredningen och *Säkerhets- och integritetsskyddsnämnden* anser regeringen dock att det är nödvändigt att de brottsbekämpande myndigheterna känner till var den utrustning som ska verkställa åtgärden, t.ex. en mobiltelefon, befinner sig under verkställighetstiden för att säkerställa

att verkställigheten enbart sker på den plats som tillståndet avser (se vidare om regeringens förslag till platskrav i avsnitt 10.1.4). Trots det påtagliga behovet och de fördelar som skulle kunna uppnås utan ett platskrav (avsnitt 9.2) delar alltså regeringen utredningens bedömning att det bör införas ett sådant när hemlig dataavläsning används för att hämta in kameraövervaknings- och rumsavlyssningsuppgifter.

Regleringen bör även, som utredningen och *Säkerhets- och integritetsskyddsnämnden* föreslår, kompletteras med bl.a. regler om förbud att läsa av eller ta del av uppgifter som används i verksamhet där tystnadsplikt gäller för att säkerställa att sådana uppgifter skyddas (se vidare avsnitt 10.3.2–10.3.4). Utan sådana regler skulle riskerna för den personliga integriteten bli allt för stora.

Hemlig dataavläsning för att ta del av lagrade uppgifter och uppgifter som visar hur teknisk utrustning används

Som redogörs för i avsnitt 8.2 och 8.3 finns det ett påtagligt behov av att samla in uppgifter som lagras i kommunikationsutrustning och uppgifter som visar hur teknisk utrustning används. Dessa uppgifter får inte samlas in med befintliga hemliga tvångsmedel om de inte överförs från ett informationssystem till ett annat via ett elektroniskt kommunikationsnät och skiljer sig därför från de uppgifter som redogörs för tidigare i detta avsnitt. Behovet finns såväl under en förundersökning som i underrättelseverksamhet. Det finns också goda skäl att tro att åtgärden kommer att vara effektiv (avsnitt 8.4).

Husrannsakan och beslag kan genomföras när en förundersökning inletts, om det finns ett tillräckligt behov och åtgärden är proportionerlig. För beslag krävs inte någon särskild svårhetsgrad hos brottet för att åtgärden ska få vidtas medan husrannsakan kräver att det misstänkta brottet har fängelse i straffskalan. Båda åtgärderna kan alltså användas av brottsbekämpande myndigheter för att ta del av uppgifter som finns lagrade i teknisk utrustning redan vid misstanke om mindre allvarlig brottslighet. Skillnaden mot de hemliga tvångsmedlen är huvudsakligen att husrannsakan och beslag typiskt sett sker öppet för den som utsätts för åtgärderna. Under alla förhållanden underrättas den misstänkte i ett tidigare skede än vid användning av hemliga tvångsmedel. I sammanhanget ska dock nämnas att det i Regeringskansliet bereds förslag på att i vissa fall skjuta på underrättelse till den som blivit föremål för beslag (SOU 2017:100 s. 608). I underrättelseverksamhet finns inte möjlighet till beslag.

Om hemlig dataavläsning tillåts för att samla in elektroniskt lagrade uppgifter och uppgifter som visar hur teknisk utrustning används kan de brottsbekämpande myndigheterna få del av ungefär samma slags uppgifter som efter husrannsakan eller beslag. Hemlig dataavläsning kan dock innebära en hemlig och löpande realtidsövervakning eller realtidskontroll av den tekniska utrustning som åtgärden avser.

Svenska Journalistförbundet och *Internetstiftelsen* anför att åtgärden innebär problem avseende möjligheten att skydda källor. *Civil Rights Defenders* avstyrker att hemlig dataavläsning ska få användas för att läsa av eller ta upp uppgifter som visar hur ett informationssystem används eftersom integritetsintrånget är för stort.

För att balansera de ökade riskerna för den personliga integriteten bör lagrade uppgifter och uppgifter som visar hur teknisk utrustning används inte få läsas av med hemlig dataavläsning för mindre allvarliga brott än sådana som kan föranleda användning av hemlig avlyssning av elektronisk kommunikation (se vidare avsnitt 10.1.1 och 10.2.1). För att journalister och andra yrkesgrupper som omfattas av tystnadsplikt ska kunna ha material som omfattas av källskyddet eller tystnadsplikten på sina datorer utan att riskera att någon annan kan ta del av innehållet bör till hemlig dataavläsning knytas regler om förbud att läsa av eller ta del av uppgifter som används i verksamhet som tystnadsplikt gäller för (se vidare avsnitt 10.3.2 och 10.3.4).

Det är proportionerligt att införa hemlig dataavläsning

Hemlig dataavläsning kommer i det enskilda fallet att innebära en inskränkning av de rättigheter och det skydd som tillkommer enskilda enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga. De skäl som föreligger för att begränsa dessa rättigheter är hänförliga till intresset av att förebygga och beivra brott. Detta är sådana intressen som får ligga till grund för begränsningar av rättigheterna, se 2 kap. 21 § regeringsformen och artikel 8.2 Europakonventionen.

Den bortre gränsen för i vilken grad skyddet för den personliga integriteten i Sverige får inskränkas framgår av 2 kap. 21 § regeringsformen. Där anges bland annat att en begränsning får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Alltför långtgående möjligheter för staten att använda hemlig dataavläsning, i meningen att löpande i realtid läsa av allt innehåll på datorer, telefoner och i annan teknisk utrustning, kan leda till såväl misstro som ryktesspridning och därmed i förlängningen utgöra ett hot mot den fria åsiktsbildningen. Några av de remissinstanser som avstyrker förslaget att införa hemlig dataavläsning, t.ex. *Sveriges advokatsamfund, Svenska Journalistförbundet* och *Föreningen för digitala fri- och rättigheter,* anser att det intrång i den personliga integriteten som hemlig dataavläsning innebär inte ryms inom statens handlingsutrymme. Regeringen kan i och för sig instämma i att hemlig dataavläsning är en ingripande åtgärd men delar inte remissinstansernas bedömning att det skulle gå utöver vad som är tillåtet enligt regeringsformen och Europakonventionen. En alltmer tilltagande kryptering och anonymisering på nätet skulle dessutom utan hemlig dataavläsning kraftigt försvåra eller till och med omöjliggöra bekämpandet av vissa brott. Att på detta sätt lämna en del av den digitala arenan oåtkomlig för de brottsbekämpande myndigheterna är enligt regeringen inte ett realistiskt alternativ. Det saknas mindre ingripande alternativ till åtgärden för att komma åt de uppgifter som det finns behov av. Frågan är då om det är proportionerligt att införa hemlig dataavläsning Det är av allra största vikt att en reglering om hemlig dataavläsning förses med tydliga ramar och begränsningar av de situationer där åtgärden får vidtas. Det är som *Internetstiftelsen* anför viktigt att alla ska vilja, våga och kunna använda

internet. Redan genom att åtgärden aldrig får användas vid lindrig brottslighet, varken i eller utanför förundersökningsverksamhet, gör att det finns sådana ramar och begränsningar. Regleringen skulle i och för sig kunna, som bl.a. *Sveriges advokatsamfund* föreslår, begränsas till att enbart avse brott som utreds av Säkerhetspolisen. Regeringen menar dock att den behovs- och riskbedömning som görs i föregående avsnitt visar att även den öppna polisen bör få använda hemlig dataavläsning i begränsade fall. Det får således enligt regeringens mening anses proportionerligt att hemlig dataavläsning, med undantag för rumsavlyssningsuppgifter, ska få användas för sådan brottslighet som kan föranleda hemlig avlyssning av elektronisk kommunikation (se vidare avsnitt 10.1.1 och 10.2.1). Regeringen anser, till skillnad från *Säkerhets- och integritetsskyddsnämnden*, att det är proportionerligt att införa hemlig dataavläsning även för kameraövervaknings- och rumsavlyssningsuppgifter. Som nämnden påpekar innebär åtgärderna en utökning av myndigheternas möjligheter att i hemlighet få uppgifter om enskildas liv. För att det ska vara acceptabelt krävs att regleringen om hemlig dataavläsning kringgärdas av starka rättssäkerhetsgarantier och innehåller tydliga och strikta ramar som tillämparen har att hålla sig inom. Regleringen måste även i övrigt utformas på ett sådant sätt att metoden kan accepteras av allmänheten som ett nödvändigt och godtagbart verktyg för de brottsbekämpande myndigheterna i kampen mot den allra allvarligaste kriminaliteten. Regeringen återkommer till dessa frågor i kapitel 12. Ytterligare en rättssäkerhetsgaranti är att lagen som ska möjliggöra tvångsmedlet tidsbegränsas (se vidare avsnitt 9.1).

Civil Rights Defenders anser att förslaget måste kompletteras med effektivare rättsmedel för den enskilde för att det ska vara proportionerligt. Enligt artikel 13 i Europakonventionen ska var och en, vars i konventionen angivna fri- och rättigheter kränkts, ha tillgång till ett effektivt rättsmedel inför en nationell myndighet och detta även om kränkningen förövats av någon under utövning av offentlig myndighet. Den ordning som föreslås för hemlig dataavläsning innehåller bl.a. domstolsprövning (avsnitt 11.1.1), offentliga ombud (avsnitt 11.1.3) och tillsyn (avsnitt 12.2.1) samt extraordinär tillsyn som utförs av JO och Justitiekanslern. Till det kommer den parlamentariska efterhandskontroll som föreslås utövas av riksdagen (avsnitt 12.1.5) och den underrättelseskyldighet till enskild som föreslås (avsnitt 12.1.4). För enskilda innebär en sådan underrättelseskyldighet en möjlighet att själv reagera genom att t.ex. kräva ersättning för skada på grund av fel eller försummelse vid myndighetsutövning. Regeringens mening är sammantaget att det krav på effektiva rättsmedel som uppställs i artikel 13 är tillgodosett.

Sammanfattningsvis menar regeringen att de positiva effekter som förslaget får i form av att försvåra de kriminellas verksamhet klart överväger de negativa effekter som förslaget får i form av integritetsinskränkningar mot den som blir föremål för åtgärden. Det är alltså proportionerligt att införa hemlig dataavläsning.

Hemlig dataavläsning är proportionerligt även i förhållande till egendomsskyddet

Av 2 kap. 15 § regeringsformen följer bl.a. att varje medborgares egendom är tryggad genom att ingen kan tvingas avstå sin egendom till det allmänna

eller till någon enskild genom expropriation eller annat sådant förfogande eller tåla att det allmänna inskränker användningen av mark eller byggnad utom när det krävs för att tillgodose angelägna allmänna intressen. Regeringsformens regler skyddar alltså inte mot inskränkningar i användningen av egendom annat än när det gäller mark eller byggnad.

Det finns mera allmänna regler om egendomsskydd i artikel 1 i första tilläggsprotokollet till Europakonventionen. Av artikeln följer att varje fysisk eller juridisk person ska ha rätt till respekt för sin egendom. Ingen får berövas sin egendom annat än i det allmännas intresse och under de förutsättningar som anges i lag och i folkrättens allmänna grundsatser. Det följer dock av artikeln att skyddet inte inskränker en stats rätt att genomföra sådan lagstiftning som staten finner nödvändig för att bl.a. reglera nyttjandet av viss egendom i överensstämmelse med det allmännas intresse.

Bedömningen av om en åtgärd är i det allmännas intresse ska i första hand göras av de nationella organen (t.ex. regering, riksdag och domstolar). Organen har en viss bedömningsmarginal (eng. margin of appreciation) att vidta åtgärder, men det krävs att samtliga begränsningar är proportionerliga.

Hemlig dataavläsning kan innebära en inskränkning i lagringsutrymme och kapacitet på ett tekniskt hjälpmedel. Detta gäller dock typiskt sett under en begränsad tid och avser inte egendomen i sin helhet.

Genomförandet av hemlig dataavläsning vilar på intresset av att förbättra förutsättningarna att kunna utreda och förhindra allvarlig brottslighet. Vid bedömningen av om den åtgärden kan anses proportionerlig bör det beaktas att lagstiftningen innehåller krav på såväl misstankegrad eller annars en viss grad av risk som en kvalificering av vilka brott som kan föranleda åtgärden. Dessutom kommer inskränkningarna i den enskildes egendom och det ekonomiska värdet av inskränkningen att vara av mycket begränsad omfattning, framför allt i relation till vad som står att vinna med åtgärden. Åtgärderna kommer också, som framgår i bl.a. avsnitt 12, att förses med åtskilliga rättssäkerhetsgarantier. Vid en samlad bedömning anser regeringen att de begränsningar som hemlig dataavläsning skulle kunna innebära avseende lagringsutrymme och kapacitetsutnyttjande är förenliga med bestämmelserna om skyddet för äganderätten. Detsamma gäller inskränkningar i äganderätten som uppstår genom att ett tillträdestillstånd verkställs (se avsnitt 10.4).

9 Hemlig dataavläsning – en ny lag

9.1 En ny lag om hemlig dataavläsning införs

Regeringens förslag: En ny lag ska införas med bestämmelser om hemlig dataavläsning. Lagen ska tidsbegränsas till att gälla i fem år efter införandet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna, t.ex. *Åklagarmyndigheten, Polismyndigheten* och *Säkerhetspolisen*, ställer sig positiva till eller lämnar inte några synpunkter på att en ny lag införs eller att lagen tidsbegränsas. De remissinstanser som motsätter sig förslaget, bl.a. *Sveriges advokatsamfund* och *Datainspektionen*, framför synpunkter av huvudsakligen principiell karaktär, vilka redovisas i föregående avsnitt. Sveriges advokatsamfund tillägger att det finns risker med att införa försökslagstiftning på tvångsmedelsområdet eftersom den regelmässigt görs permanent. Risken för ändamålsglidning är därmed enligt samfundet uppenbar och det är jämförelsevis enkelt att utvidga tvångsmedlets tillämpningsområde.

Svea hovrätt anser att lösningen att införa en ny lag i stället för att reglerna förs samman med befintliga bestämmelser om hemliga tvångsmedel leder till ökad fragmentisering och minskad överskådlighet. Om bestämmelserna görs permanenta anser hovrätten att de borde sammanföras med övriga bestämmelser om hemliga tvångsmedel. *Stockholms tingsrätt* och *Göteborgs tingsrätt* anser att utredningens lagförslag är svårläst och väcker frågan om det är bättre att lagen, till skillnad från utredningens förslag, består av huvudregler och undantag från dem. Göteborgs tingsrätt tillägger att det visserligen framstår som lämpligt med en särskild lag på området eftersom lagstiftningen ska vara tidsbegränsad, men att detta minskar överskådligheten av regelverket.

Säkerhets- och integritetsskyddsnämnden anser att lagförslaget är svårt att överblicka och att det inte uppfyller grundläggande krav på förutsebarhet och tydlighet. Det är otydligt vad som faktiskt ska gälla när rättegångsbalkens tvångsmedel ska verkställas med stöd av beslut om hemlig dataavläsning. Som alternativ anför nämnden att en reglering på området skulle kunna utformas med en lag som bara innehåller de från rättegångsbalken avvikande reglerna och att specialbestämmelser regleras direkt i lagen om internationell rättslig hjälp i brottmål, preventivlagen och lagen om särskild utlänningskontroll. *Stockholms universitet (Juridiska fakulteten)* anser att lagen är svåröverskådlig med hänsyn till det stora antalet hänvisningar som den innehåller.

Justitiekanslern tillstyrker att lagen införs och tidsbegränsas men anser att effekterna och tillämpningen av lagen måste utvärderas innan den kan göras permanent.

Stiftelsen för internetinfrastruktur (Internetstiftelsen) och *Svenska Journalistförbundet* är tveksamma till att stifta tillfälliga lagar eftersom det sedan tidigare finns en obenägenhet att protestera när tillfälliga lagar ska göras permanenta. Om lagen ska införas anser förbundet att den måste utvärderas ordentligt ur ett bredare samhällsperspektiv än endast det brottsbekämpande.

Skälen för regeringens förslag: Det finns regler om hemliga tvångsmedel i både rättegångsbalken och i vissa speciallagar. Det är i och för sig möjligt att införa regler om hemlig dataavläsning i dessa. En fördel med att placera reglerna i existerande lagar är att det då går att använda den redan befintliga lagtekniska strukturen. Dessutom blir det mer lättillgängligt med hänvisningar till bestämmelser i samma lag än med motsvarande hänvisningar till andra lagar. Härtill kommer synpunkten, som framförs av bland andra *Svea hovrätt,* att överskådligheten av systemet för hemliga tvångsmedel minskar om ett tvångsmedel regleras i en separat lag.

Som regeringen återkommer till nedan är emellertid ambitionen att tidsbegränsa reglerna om hemlig dataavläsning. Dessutom föreslår regeringen att reglerna ska gälla både under förundersökning och i underrättelseverksamhet. Det blir därmed svårt att införa reglerna i befintliga lagar utan att behöva upprepa många bestämmelser. Sammantaget innebär det att, i vart fall så länge lagen är tidsbegränsad, övervägande skäl talar för att införa reglerna om hemlig dataavläsning i en ny lag.

Hemlig dataavläsning kan i det närmaste användas som ett verktyg för att verkställa flera olika tvångsmedel som alla i princip regleras på olika sätt. För att reglera hur dessa tvångsmedel kan verkställas genom hemlig dataavläsning kommer lagen behöva förses med ett större antal hänvisningar, både inom lagen och till andra lagar, vilket bl.a. *Stockholms universitet (Juridiska fakulteten)*, *Stockholms tingsrätt* och *Säkerhets- och integritetsskyddsnämnden* är kritiska till. Regeringen har förståelse för kritiken och använder därför en delvis annan lagstiftningsteknik än utredningen i syfte att försöka minska antalet hänvisningar.

Hemlig dataavläsning kan på goda grunder förväntas vara ett effektivt tvångsmedel i den brottsbekämpande verksamheten, vilket talar för att åtgärden borde införas i permanent lagstiftning. Mot att lagstiftningen görs permanent kan anföras att det rör sig om en ny utredningsmetod som dessutom innebär vissa risker för den personliga integriteten. Många lagar och bestämmelser som rör hemliga tvångsmedel har inledningsvis begränsats i tiden. Sådan tidsbegränsning föreslogs t.ex. i förarbetena till lagen om hemlig rumsavlyssning (prop. 2005/06:178) och lagen om hemlig kameraövervakning (prop. 1995/96:85). Skälet till att lagarna tidsbegränsats har huvudsakligen varit att nya tvångsmedel ger upphov till risker för otillbörliga integritetsintrång, varför ett fördjupat underlag kan behövas inför ett ställningstagande till om lagen i fråga bör permanentas (prop. 2005/06:178 s. 47). Av samma skäl bör därför även den nu föreslagna lagen tidsbegränsas.

Det kan antas att hemlig dataavläsning till en början endast kommer att kunna användas i ett begränsat antal fall. När lagen om hemlig rumsavlyssning infördes begränsades dess giltighetstid till tre år. Vid utvärderingen av buggning och preventiva tvångsmedel (SOU 2009:70) konstaterades att antalet fall av hemlig rumsavlyssning var så få att det inte utifrån dessa gick att dra några säkra slutsatser om tvångsmedlets effektivitet eller praktiska värde. Regeringen bedömer att det finns risk för att tre års giltighetstid för lagen om hemlig dataavläsning skulle leda till samma resultat. Lagen bör därför, som utredningen föreslår, gälla i fem år från dess införande. En senare utvärdering av den tidsbegränsade lagen minimerar enligt regeringens mening risken för att lagen görs permanent utan ett fullgott underlag, vilket är en farhåga som framförs av *Svenska advokatsamfundet, Internetstiftelsen* och *Svenska Journalistförbundet*. Vid en framtida utvärdering och beredning kommer nyttan, behovet och proportionaliteten av hemlig dataavläsning återigen att analyseras och bedömas.

9.2 Innebörden av hemlig dataavläsning

Regeringens förslag: Genom hemlig dataavläsning ska uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel få läsas av eller tas upp i ett avläsningsbart informationssystem. Med avläsningsbart informationssystem avses antingen en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att begreppet informationssystem används utan preciseringen att det ska vara avläsningsbart men med preciseringen att det ska vara identifierbart.

Remissinstanserna: *Svea hovrätt* ifrågasätter innebörden av tillägget liknande tjänst och föreslår att det stryks. *Säkerhets- och integritetsskyddsnämnden* anför att begreppet ”uppgifterna ska vara avsedda för automatiserad behandling i ett informationssystem” innebär att uppgifterna ännu inte finns i informationssystemet, vilket är problematiskt och knappast kan ha varit avsikten med förslaget. Vidare anser nämnden att begreppet informationssystem inte avgränsar lagens tillämpningsområde tillräckligt tydligt eftersom termen används på ett annat sätt i annan lagstiftning, t.ex. registerlagstiftning. Slutligen anser nämnden att utredningens krav på att ett informationssystem ska vara identifierbart är felaktigt eftersom alla system potentiellt är identifierbara. I stället föreslår nämnden att begreppet identifierat informationssystem, eller något liknande uttryck, används. Även *Datainspektionen* anser att objektet för åtgärden måste preciseras och att begreppet informationssystem inte är tillräckligt tydligt, vilket leder till att det är osäkert vad som omfattas av förslaget. *Myndigheten för samhällsskydd och beredskap* avråder också från att använda begreppet informationssystem och förordar i stället avläsningsbart informationssystem. Begreppet informationssystem har nämligen i betänkandet fått en annan och snävare innebörd än vad som gäller för begreppet i stort och hur det har använts i andra sammanhang. *Lunds universitet (Juridiska fakulteten)* anser att det borde finnas tydligare hållpunkter när det gäller bedömningen av vilken utrustning som kan bli föremål för hemlig dataavläsning. *Svenska Journalistförbundet* anser att begreppet avläsning och upptagning inte beskriver vilken uppgift de brottsbekämpande myndigheterna får ägna sig åt utan tycker i stället att det bör framgå i lagtext att myndigheterna faktiskt får lov att gå in i en dator eller annat tekniskt hjälpmedel.

Skälen för regeringens förslag

Hemlig dataavläsning behöver definieras

Lagen bör inledas med en definition som beskriver och avgränsar vad hemlig dataavläsning är. Definitionen bör lämpligen ta sin utgångspunkt i definitioner av andra hemliga tvångsmedel samt knyta an till straffbestämmelsen om dataintrång, enligt vilken möjligheterna att i dag använda tekniker för hemlig dataavläsning begränsas.

Ett gemensamt drag i definitionerna av befintliga hemliga tvångsmedel är att samtliga slår fast objektet för åtgärden, alltså klargör vilka uppgifter som får hämtas in genom användning av åtgärden. Hemlig dataavläsning

ska vara en metod för att hämta in olika typer av uppgifter och begreppet som ska beskriva objektet måste därför täcka in samtliga dessa uppgifter.

I brottsbalkens bestämmelse om dataintrång används begreppet ”uppgift som är avsedd för automatiserad behandling” för att beskriva vilka uppgifter som omfattas av bestämmelsen. Begreppet infördes för att förtydliga att alla uppgifter, dvs. fakta, program, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form omfattas av bestämmelsen. Det är för tillämpningen av begreppet utan betydelse var uppgifterna finns eller förvaras i systemet, varför uppgifterna omfattas oavsett på vilket datamedium de finns. Därmed innefattas också uppgifter som finns i en dators temporära minne. Vidare omfattar begreppet uppgifter som är under befordran, oavsett på vilket sätt befordran sker, se propositionen Angrepp mot informationssystem (prop. 2006/07:66 s. 49).

Uttrycket ”uppgift som är avsedd för automatiserad behandling” kritiseras av *Säkerhets- och integritetsskyddsnämnden* som anser att uttryckssättet enligt sin ordalydelse innebär att uppgifterna ännu inte finns i informationssystemet. Fördelen med begreppet är dock att det täcker alla uppgiftstyper som kan aktualiseras vid hemlig dataavläsning. Det visar också kopplingen mellan hemlig dataavläsning och straffbestämmelsen om dataintrång. Det tydliggör dessutom på ett teknikneutralt och ändamålsenligt vis vilka uppgifter åtgärden får användas för att hämta in. Begreppet innebär dock som nämnden påpekar inget krav på att uppgifterna måste finnas i informationssystemet vid tidpunkten för tillståndsprövningen. Uppgifter som den enskilda inte har avsett att behandla automatisk kan ändå bli avsedda för automatiserad behandling. Det kan vara fallet när den verkställande myndigheten, efter beviljat tillstånd till hemlig dataavläsning, t.ex. aktiverar en mobiltelefons inspelningsfunktion för att få tillgång till tal mellan flera personer (s.k. rumsavlyssningsuppgifter, se avsnitt 9.3). Vid en samlad bedömning framstår det enligt regeringen som lämpligt att använda detta begrepp i lagen.

Det bör också av definitionen framgå hur uppgifterna får hämtas in. Hemlig dataavläsning kommer att kunna innebära avläsning och upptagning av flera olika slags uppgifter och på olika sätt. Det bör därför anges att uppgifterna läses av. Det bör också anges att uppgifterna får tas upp för att tydliggöra att uppgifterna får granskas såväl i realtid som i efterhand. Redan i definitionen av hemlig dataavläsning bör det anges vilken metod för avläsningen eller upptagningen som får användas. Eftersom de tekniska metoderna för detta kan se olika ut och förändras över tid bör begreppet vara teknikneutralt. Därför bör det framgå att den brottsbekämpande myndigheten får läsa av eller ta upp uppgifterna med ett tekniskt hjälpmedel. Begreppet tekniskt hjälpmedel avser såväl hårdvara som programvara (se prop. 1994/95:227 s. 29). Regeringen anser, till skillnad från *Svenska Journalistförbundet*, att definitionen är tillräckligt tydlig och täcker såväl att ett elektroniskt program installeras i t.ex. en dator som att ett fysiskt föremål, t.ex. ett chip installeras i densamma.

Det bör vidare framgå av definitionen att hemlig dataavläsning är en åtgärd som utförs i hemlighet utan att den enskilde, mot vilken den riktas, känner till den.

Åtgärden ska avse uppgifter i ett avläsningsbart informationssystem

Av definitionen av hemlig dataavläsning bör även framgå var de uppgifter som ska läsas av ska finnas. I många fall är föremålet för åtgärden uppgifter i fysisk utrustning, t.ex. en dator eller en mobiltelefon, men även icke-fysisk utrustning, t.ex. ett användarkonto till en kommunikations- eller lagringstjänst på internet, kan vara av stort intresse i den brottsbekämpande verksamheten. Eftersom behovet är lika stort oavsett var uppgifterna finns och integritetsintrånget typiskt sett är detsamma oberoende av hur och var informationen lagras saknas det skäl att inte tillåta avläsning av uppgifter som finns tillgängliga via användarkonton. En annan sak är att integritetsintrånget kan variera högst väsentligt beroende på vad för slags information det är fråga om (se vidare avsnitt 9.4 om proportionalitet). Regeringens förslag innebär därför, i likhet med utredningens, att hemlig dataavläsning ska få användas även beträffande sådana uppgifter, varför beskrivningen av åtgärden måste inbegripa även dem.

Några remissinstanser, bl.a. *Myndigheten för samhällsskydd och beredskap*, är kritiska till begreppet informationssystem som utredningen föreslår eftersom det redan används i andra sammanhang på ett sätt som inte stämmer överens med hur det används i den nu föreslagna lagen. Myndigheten förordar i stället begreppet avläsningsbart informationssystem. Regeringen instämmer i att ett avläsningsbart informationssystem bättre beskriver vad som avses. Genom begreppet anser regeringen att det inte finns något behov av att ange att informationssystemet ska vara vare sig identifierbart, som utredningen föreslår, eller identifierat, vilket *Säkerhets- och integritetsskyddsnämnden* föreslår. Nedan redovisas vad som omfattas av begreppet avläsningsbart informationssystem.

Ett avläsningsbart informationssystem kan vara antingen elektronisk kommunikationsutrustning eller användarkonton till vissa tjänster

Avläsningsbara informationssystem av fysisk karaktär kan vara t.ex. datorer, mobiltelefoner, surfplattor, smarta armbandsur och servrar. Utredningen föreslår att det ska beskrivas med begreppet elektronisk kommunikationsutrustning. Fördelen med det är att det redan används i bestämmelserna om hemliga tvångsmedel (se t.ex. 27 kap. 19 § RB och 1 § inhämtningslagen) och i förundersökningssammanhang (se t.ex. 23 kap. 9 a § RB). Regeringen har i propositionen Förstärkt rättssäkerhet och effektivitet i förundersökningsförfarandet (prop. 2015/16:68 s. 74) förtydligat att begreppet anses omfatta all slags utrustning som kan användas för att kommunicera elektroniskt. Det framstår sammantaget som lämpligt att använda begreppet elektronisk kommunikationsutrustning för att beskriva vad ett informationssystem i lagens mening kan vara, när det är fråga om fysisk utrustning. En tydligare definition av vilken utrustning hemlig dataavläsning kan riktas mot, som *Lunds universitet (Juridiska fakulteten)* efterfrågar, är enligt regeringens bedömning inte möjlig att utforma då det är angeläget att lagstiftningen hålls så teknikneutral som möjligt för att kunna omfatta såväl dagens som framtidens teknik.

Som anges i det föregående bör det finnas en möjlighet att tillåta hemlig dataavläsning även för uppgifter i informationssystem som inte i sig utgör elektronisk kommunikationsutrustning. De informationssystem som det då

är fråga om är främst internetbaserade kommunikations- eller lagringstjänster. De är visserligen uppbyggda genom fysisk utrustning och infrastruktur som den som tillhandahåller tjänsterna förfogar över. Det relevanta i sammanhanget är dock den enskildes användning av själva tjänsterna. De brottsbekämpande myndigheternas tillgång till uppgifter i sådana tjänster måste därför begränsas till de delar av informationssystemet som den som utsätts för åtgärden har behörighet till. I Norge, som har regler motsvarande hemlig dataavläsning, har detta hanterats genom att de brottsbekämpande myndigheterna enligt en uttrycklig bestämmelse kan få tillstånd att rikta hemlig dataavläsning mot ett specifikt användarkonto ”brukerkonto” till en kommunikations- eller lagringstjänst.

När de relevanta uppgifterna finns i ett avläsningsbart informationssystem, bör hemlig dataavläsning endast få avse det som är avgränsat till den enskilde användaren. Med ett avläsningsbart informationssystem ska alltså också kunna avses ett användarkonto eller en på motsvarande sätt avgränsad del av en viss tjänst. Med användarkonto avses typiskt sett en egen personlig sida på ett socialt medium, en applikation för snabbmeddelanden eller på ett internetforum. En på motsvarande sätt avgränsad del av en viss tjänst är ett teknikneutralt begrepp som bör täcka sådana fall där den enskilde använder en tjänst med inloggningsuppgifter som flera har tillgång till, utan ett bestämt användarkonto (t.ex. inloggning till tjänster som företag erbjuder sina anställda eller som högskolor erbjuder sina studerande).

De tjänster som kan vara relevanta vid hemlig dataavläsning bör avgränsas till kommunikations- och lagringstjänster och liknande tjänster. Kommunikationstjänster innefattar t.ex. tjänster för samtal och sms-meddelanden. Även andra liknande tjänster som t.ex. webbmejl och andra typer av samtals- och meddelandetjänster bör kunna bli föremål för hemlig dataavläsning. Lagringstjänster kan t.ex. vara sådana tjänster som möjliggör lagring av data på annan plats än i den egna elektroniska kommunikationsutrustningen, s.k. molntjänster.

Det torde också finnas andra tjänster som innefattar kommunikations- eller lagringsmöjligheter även om det inte är det primära syftet med tjänsten. Detta kan t.ex. avse en chatt- eller meddelandefunktion i en applikation som huvudsakligen har ett annat syfte, t.ex. spel. Om ett användarkonto på en sådan tjänst är av intresse för de brottsbekämpande myndigheterna i ett särskilt ärende bör det inte vara uteslutet att läsa av eller ta upp uppgifter som finns i tjänsten. Således bör även tjänster som liknar lagringstjänster, utan att primärt vara det, omfattas av möjligheterna till hemlig dataavläsning. Till skillnad från bl.a. *Svea hovrätt* och *Datainspektionen* anser regeringen att definitionerna är tillräckligt tydliga och förutsebara.

9.3 Vilka uppgiftstyper ska hemlig dataavläsning få omfatta?

Regeringens förslag: Tillstånd till hemlig dataavläsning ska få beviljas för att läsa av eller ta upp

1. uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress (kommunikationsavlyssningsuppgifter),
2. uppgifter om annat än innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress (kommunikationsövervakningsuppgifter),
3. uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits (platsuppgifter),
4. uppgifter som framkommer genom optisk personövervakning (kameraövervakningsuppgifter),
5. uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till (rumsavlyssningsuppgifter),
6. uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i 1–5, eller
7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i 1–6.

Vid hemlig dataavläsning som gäller kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät även hindras från att nå fram.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: De remissinstanser som ställer sig bakom den föreslagna lagen ställer sig också i huvudsak bakom hur hemlig dataavläsning ska få användas. Bland andra *Åklagarmyndigheten*, *Polismyndigheten* och *Säkerhetspolisen* noterar att de uppgifter det är fråga om redan nu får hämtas in med öppna eller hemliga tvångsmedel men att det i dagsläget inte går att göra det på teknisk väg.

Datainspektionen, *Sveriges advokatsamfund* och *Stiftelsen för Internetinfrastruktur (Internetstiftelsen)* anser att de tvångsåtgärder som föreslås är alltför ingripande och ger mycket stora möjligheter att övervaka och kartlägga människors liv. Sveriges advokatsamfund anser dessutom att de åtgärder som kan bli aktuella måste förtydligas genom att lagtexten uttryckligen hänvisar till de lagbestämmelser som reglerar vilka tvångsmedel det är fråga om.

Säkerhets- och integritetsskyddsnämnden avstyrker förslaget om att hemlig dataavläsning ska få användas för att läsa av eller ta upp uppgifter som avser optisk personövervakning samt uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster dit allmänheten inte har tillträde. Nämnden anför att det för att säkerställa verkställighet enbart på den plats som anges i tillståndet är nödvändigt att den brottsbekämpande myndigheten känner till exakt var en telefon finns under hela verkställighetstiden. Likaså får verkställigheten inte komma i konflikt med bestämmelserna om avlyssningsförbud. Nämnden anser inte att utredningen visar hur detta ska gå till. I övrigt godtar nämnden förslagen när det gäller vilka typer av uppgifter som ska få

avläsas. Nämnden anser dock att definitionen av kommunikationsövervaknings- och kameraövervakningsuppgifter skiljer sig från terminologin i övriga författningar om hemliga tvångsmedel och att definitionen av uppgifter som finns lagrade i ett informationssystem är oklar. Det är också, enligt nämnden, oklart hur myndigheterna ska förhålla sig till omständigheten att det är okänt var dessa uppgifter finns lagrade.

Civil Rights Defenders och *Sveriges advokatsamfund* är kritiska till det integritetsintrång det innebär att myndigheterna får lov att läsa av eller ta upp uppgifter som visar hur ett informationssystem används samt möjlighet att hindra meddelanden från att nå fram. Även *Internetstiftelsen* är tveksam till den åtgärden och anser att det är oklart vad som avses med att myndigheterna får hindra meddelanden från att komma fram och vilka konsekvenser detta kan få.

Malmö tingsrätt noterar att det i 27 kap. 25 § RB anges att det vid verkställighet av hemlig avlyssning och övervakning av elektronisk kommunikation får användas de tekniska hjälpmedel som behövs. Eftersom hemlig dataavläsning inte ska få användas för att verkställa dessa tvångsmedel utan särskilt beslut anser tingsrätten att det finns skäl att förtydliga 27 kap. 25 § RB så att den teknik som avses där inte kan användas för hemlig dataavläsning.

Lunds universitet (Juridiska fakulteten) anser att definitionen av kommunikationsövervakningsuppgifter är otydlig och bör förtydligas.

Skälen för regeringens förslag

Utgångspunkter

Eftersom hemlig dataavläsning kan användas för att läsa av eller ta upp flera olika typer av uppgifter bör det införas en uttrycklig regel i den nya lagen som klargör vilka uppgifter det kan röra sig om. Bestämmelsen blir utgångspunkt i varje enskilt fall när det ska avgöras vilka uppgifter som ska få läsas av eller tas upp inom ramen för hemlig dataavläsning. Ett tillstånd till hemlig dataavläsning innebär inte per automatik tillgång till alla slags uppgiftstyper utan det bör bestämmas i det enskilda fallet vilka uppgiftstyper som kan bli aktuella. Genom att tillståndet för hemlig dataavläsning kan och ska differentieras på detta sätt och tillståndet ska ges med restriktivitet är de risker för övervakning av människors liv som framförs av *Datainspektionen*, *Sveriges advokatsamfund* och *Internetstiftelsen* inte särskilt framträdande.

Hemlig dataavläsning för att verkställa andra hemliga tvångsmedel

Hemlig dataavläsning bör få användas för att läsa av eller ta upp motsvarande uppgifter som kan hämtas in med de befintliga tvångsmedlen. Definitionerna av uppgifterna bör, som utredningen föreslår, så långt som möjligt överensstämma med hur uppgifterna definieras i regleringen av de befintliga tvångsmedlen. Det är inte lämpligt att, som *Lunds universitet (Juridiska fakulteten)* är inne på, introducera nya definitioner i detta lagstiftningsarbete. Även om definitionerna av uppgifterna huvudsakligen motsvarar de uppgifter som kan inhämtas med befintliga tvångsmedel råder inte fullständig överensstämmelse, t.ex. omfattar hemlig dataav-

läsning inte s.k. basstationstömningar som vanligtvis används efter tillstånd till hemlig övervakning av elektronisk kommunikation. Det blir därför inte heller, som *Sveriges advokatsamfund* föreslår, rättvisande att hänvisa till befintliga tvångsmedelsbestämmelser. De uppgifter som ska kunna hämtas in med hemlig dataavläsning kan ge tillgång till följande information:

1. Historiskt innehåll och realtidsinnehåll i meddelanden. Detta motsvarar uppgifter som kan hämtas in genom hemlig avlyssning av elektronisk kommunikation (kommunikationsavlyssningsuppgifter).

2. Historiska uppgifter och realtidsuppgifter om sådana meddelanden som avses i punkt 1. Detta motsvarar uppgifter som kan hämtas in genom hemlig övervakning av elektronisk kommunikation och till viss del genom inhämtning enligt inhämtningslagen (kommunikationsövervakningsuppgifter).

3. Uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Detta motsvarar huvudsakligen uppgifter som kan hämtas in genom hemlig övervakning av elektronisk kommunikation och inhämtning enligt inhämtningslagen (platsuppgifter). Innebörden av begreppet platsuppgifter ska inte sammanblandas med begreppet lokaliseringsuppgifter som är uppgifter som behandlas i ett elektroniskt kommunikationsnät eller av en elektronisk kommunikationstjänst och som visar den geografiska positionen för terminalutrustningen för en användare (1 kap. 7 § lagen om elektronisk kommunikation). Utredningen föreslår att begreppet lokaliseringsuppgifter ska användas även vid hemlig dataavläsning. Regeringen väljer dock begreppet platsuppgifter för att denna uppgiftstyp inte ska sammanblandas med det redan etablerade begreppet lokaliseringsuppgifter som används i andra sammanhang.

4. Uppgifter som framkommer genom optisk personövervakning. Detta motsvarar uppgifter som kan hämtas in genom hemlig kameraövervakning (kameraövervakningsuppgifter). Det kan noteras att uttrycket kameraövervakning numera ersatts av kamerabevakning i kamerabevakningslagen (2018:1200). Eftersom termen hemlig kameraövervakning används i rättegångsbalken används termen kameraövervakningsuppgifter här.

5. Uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till. Detta motsvarar uppgifter som kan hämtas in genom hemlig rumsavlyssning (rumsavlyssningsuppgifter).

Att i hemlighet läsa av eller ta upp någon av de nämnda uppgifterna är att jämställa med en metod för att verkställa befintliga hemliga tvångsmedel, vilket poängteras av bl.a. *Åklagarmyndigheten.* De uppgiftstyper som hemlig dataavläsning föreslås kunna ge tillgång till motsvarar ett verkligt behov och det är enligt regeringen proportionerligt att ge de brotts-

bekämpande myndigheterna möjlighet att få tillgång till dem för att möta

den alltmer digitaliserade brottsligheten (se avsnitt 8.2, 8.3 och 8.6). Regeringen gör därmed en annan bedömning än *Säkerhets- och integritetsskyddsnämnden* avseende vilka uppgiftstyper som bör omfattas av tvångsmedlet. Regeringen anser också att det genom definitionerna är tydligt vilka uppgifter som avses, inte minst eftersom de huvudsakligen stämmer överens med bakomliggande tvångsmedel.

När ett tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation har beviljats får åtgärderna användas för att hindra meddelanden från att nå fram (27 kap. 19 § andra stycket RB). Möjligheten att hindra meddelanden från att nå fram är en viktig åtgärd som kan användas i kritiska lägen för att t.ex. hindra brottslingar från att ta kontakt med varandra eller nås av varnande samtal. När hemlig dataavläsning används för att läsa av eller ta upp kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter bör denna rätt finnas, i synnerhet då det närmast är en verkställighetsmetod av redan befintliga regler. Regeringen gör därmed en annan bedömning än *Civil Rights Defenders, Internetstiftelsen* och *Sveriges advokatsamfund* i denna del.

Hemlig dataavläsning för avläsning eller upptagning av andra uppgifter

Som framgår i avsnitt 8.2 ovan finns det ett behov för de brottsbekämpande myndigheterna att kunna avläsa uppgifter som finns lagrade i ett informationssystem och uppgifter som visar hur ett informationssystem används. Regeringen gör även i avsnitt 8.6 bedömningen att åtgärden är proportionerlig. Regeringens uppfattning är därför, till skillnad från bl.a. *Civil Rights Defenders*, att även sådana uppgifter ska få läsas av. Vid avläsning eller upptagning av lagrade uppgifter finns, som *Säkerhets- och integritetsskyddsnämnden* påpekar, en risk att uppgifterna inte kan hämtas in eftersom det är oklart var de är lagrade. Detta behandlas i avsnitt 13.4.

Hemlig dataavläsning ska få användas endast efter tillstånd

Som utvecklas i avsnitt 11.1.1 föreslår regeringen att hemlig dataavläsning endast ska få användas efter tillstånd av domstol. Det bör framgå av lagen. Genom att hemlig dataavläsning kräver ett uttryckligt tillstånd finns ingen risk för sammanblandning av hemlig dataavläsning och hemlig avlyssning av elektronisk kommunikation, varför ett sådant förtydligande som *Malmö tingsrätt* föreslår inte är nödvändigt.

9.4 Proportionalitet

Regeringens förslag: Ett tillstånd till hemlig dataavläsning ska få beviljas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Svea hovrätt*, *Säkerhets- och integritetsskyddsnämnden* och *Dataskydd.net* anser att det bör tydliggöras att proportionalitetsbedömningen ska omfatta samtliga åtgärder som begärts inom ramen för ett beslut om hemlig dataavläsning. *Stockholms universitet*

(Juridiska fakulteten) och *Sveriges advokatsamfund* anser att det är nödvändigt att föra in en bestämmelse om proportionalitet men att en sådan bestämmelse behöver omfatta även behovsprincipen och ändamålsprincipen. Tvångsmedlet hemlig dataavläsning borde därmed vara sekundärt till andra tvångsmedel för att balansera intresset av effektiv brottsbekämpning mot identifierade integritetsrisker. *Google Sweden AB (Google)* noterar att risken för att företagshemligheter kommer att samlas in ska beaktas inom ramen för proportionalitetsbedömningen men skulle önska tydligare begränsningar kring sådan insamling och hur den ska hanteras.

Skälen för regeringens förslag: Vid all tvångsmedelsanvändning gäller legalitetsprincipen, ändamålsprincipen, behovsprincipen och proportionalitetsprincipen som allmänna principer. Legalitetsprincipen innebär att en åtgärd måste ha stöd i lag. Ändamålsprincipen innebär att en myndighets befogenhet ska vara bunden till det ändamål för vilket tvångsmedlet har beslutats. Behovsprincipen innebär att en myndighet får använda ett tvångsmedel endast när det finns ett påtagligt behov av detta och en mindre ingripande åtgärd inte är tillräcklig. Slutligen innebär proportionalitetsprincipen att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden (Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas?, 4 uppl. 2018 s. 20–28). Även om proportionalitetsprincipen alltså redan gäller vid all tvångsmedelsanvändning utan att återges i lagtext är det vanligt att principen lagfästs (se t.ex. 27 kap. 1 § tredje stycket RB). Med hänsyn till remissinstansernas synpunkter och med beaktande av att hemlig dataavläsning innebär ett ökat integritetsintrång för den enskilde finns det starka skäl som talar för att principen bör tydliggöras i lagen om hemlig dataavläsning. Regeringen instämmer därför i utredningens förslag i denna del.

I proportionalitetsavvägningen är det särskilt viktigt att noggrant pröva samtliga omständigheter och väga dem som talar för mot dem som talar mot att tillåta hemlig dataavläsning i det enskilda fallet. Prövningen kan leda till att en åtgärd inte tillåts trots att de krav som lagen i övrigt uppställer är uppfyllda. En utgångspunkt för proportionalitetsprövningen bör vara att hemlig dataavläsning för en viss uppgiftstyp endast är proportionerlig om andra åtgärder för att komma åt uppgifterna inte är tillräckliga, skulle vara väsentligt svårare att genomföra än hemlig dataavläsning eller kan förväntas leda till större integritetsintrång än hemlig dataavläsning. Till skillnad från *Stockholms universitet (Juridiska fakulteten)* och *Sveriges advokatsamfund* anser regeringen att det är tillräckligt att det i proportionalitetsprövningen beaktas att hemlig dataavläsning bör vara sekundärt till andra tvångsmedel.

Proportionalitetsprincipen kan få särskild betydelse när en ansökan om hemlig dataavläsning avser flera uppgiftstyper och tvångsmedelsåtgärder eftersom integritetsriskerna då blir större för den enskilde. Vid tillståndsprövning av hemlig dataavläsning måste domstolen alltså, utöver att beakta samtliga omständigheter som åberopas i det enskilda fallet, också ställa sig frågan om det är proportionerligt att tillåta avläsning eller upptagning av flera olika uppgiftstyper. Det bör endast undantagsvis och endast i de allra allvarligaste fallen, t.ex. vid terroristbrottslighet eller annan mycket allvarlig brottslighet, vara möjligt att få tillstånd till avläsning eller upptagning av samtliga uppgiftstyper samtidigt.

Vid proportionalitetsprövningen kan det också väckas frågor om informationssäkerhet och företagshemligheter. Det är en naturlig del av rättens prövning att bedöma t.ex. om det finns risk för att den brottsbekämpande myndigheten kan få del av uppgifter som helt saknar betydelse för det ärende åtgärden ska vidtas i och som dessutom är av särskilt känslig karaktär. Det är inte formellt uteslutet med hemlig dataavläsning avseende sådana uppgifter men en viss åtgärd kan behöva uteslutas eller begränsas till sin omfattning. I och med att proportionalitetsprövningen kommer att inrymma dessa frågor och många andra behöver det inte, till skillnad från vad *Google* anser, anges uttryckligen i lagstiftningen.

Regeringen gör bedömningen att det, på samma sätt som för övriga hemliga tvångsmedel, inte finns något behov av att i lagen införa uttryckliga principer om legalitet eller åtgärdens ändamål och behov eftersom de kommer till uttryck i lagens materiella bestämmelser genom avgränsningar som tydliggör i vilka fall hemlig dataavläsning får användas för olika ändamål. Till skillnad från *Sveriges advokatsamfund* och *Stockholms universitet (Juridiska fakulteten)* anser regeringen alltså att det är tillräckligt att endast proportionalitetsprincipen uttryckligen anges i lagen.

Några remissinstanser, bl.a. *Svea hovrätt*, lyfter fram att proportionalitetsprincipen bör förtydligas att gälla även under den tid som tvångsmedlet består. Regeringen instämmer i att det är angeläget att principen respekteras under hela förfarandet. Det är emellertid klart att principen gäller både vid beslut och verkställighet (se SOU 1995:47 s. 324 och prop. 2005/06:178 s. 101). Om en situation uppstår där integritetsintrånget blir för stort kan åtgärden även utan att det uttryckligt anges i lagtexten, med hänvisning till proportionalitetsprincipen, behöva avbrytas eller beslutet omprövas (Gunnel Lindberg, samma bok s. 32). Med hänsyn härtill saknas det skäl att lagfästa att proportionalitetsprincipen gäller även under verkställighet.

10 Tillämpningsområdet för hemlig dataavläsning

10.1 Hemlig dataavläsning under en förundersökning

10.1.1 Utgångspunkter

Regeringens bedömning: Vid hemlig dataavläsning i syfte att läsa av eller ta upp uppgifter som får hämtas in med befintliga hemliga tvångsmedel bör som utgångspunkt motsvarande krav gälla som gäller för de bakomliggande tvångsmedlen. Vid hemlig dataavläsning för att läsa av eller ta upp uppgifter som i dag inte är möjliga att hämta in med hemliga tvångsmedel bör kravet för hemlig dataavläsning motsvara vad som gäller för hemlig avlyssning av elektronisk kommunikation.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte bedömningen. Några remissinstanser, t.ex. *Åklagarmyndigheten* och *Ekobrottsmyndigheten*, delar uttryckligen utredningens bedömning. *Malmö tingsrätt* anser att det är en naturlig och rimlig utgångspunkt att som huvudregel använda motsvarande krav för tillstånd till hemlig dataavläsning som gäller för tillstånd till hemlig avlyssning av elektronisk kommunikation.

Skälen för regeringens bedömning: Vid utformningen av reglerna om hemlig dataavläsning bör en jämförelse göras både med de krav som ställs för övriga hemliga tvångsmedel och med dagens möjligheter att komma åt uppgifterna på annat sätt och vilka krav som då ställs. Dessutom måste riskerna för den personliga integriteten beaktas.

De uppgiftstyper som föreslås ska kunna läsas av eller tas upp efter tillstånd till hemlig dataavläsning är dels uppgifter som får hämtas in enligt de nu gällande reglerna om hemliga tvångsmedel, dels uppgifter som hemliga tvångsmedel tidigare inte gett tillgång till. I den förstnämnda kategorin har hemlig dataavläsning närmast karaktären av en verkställighetsmetod för befintliga hemliga tvångsmedel. Det är därför, som utredningen föreslår och som *Malmö tingsrätt* instämmer i, rimligt att det som huvudregel ställs samma krav på hemlig dataavläsning som för de befintliga hemliga tvångsmedlen när hemlig dataavläsning motsvarar de befintliga tvångsmedlen. I avsnitt 10.1.2 redogörs för i vilka situationer den föreslagna regleringen om hemlig dataavläsning avviker från de befintliga tvångsmedlen.

Förslaget att hemlig dataavläsning ska få användas för att läsa av eller ta upp lagrade uppgifter samt uppgifter om hur ett informationssystem används innebär generellt sett en ökad integritetsrisk för den enskilde (se avsnitt 8.5). För att kunna avgöra hur regleringen bör utformas behöver därför göras en något mer ingående jämförelse mellan hemlig dataavläsning avseende dessa uppgiftstyper och andra hemliga tvångsmedel.

Det nuvarande hemliga tvångsmedel som det ställs högst krav på för att få använda är hemlig rumsavlyssning. Hemlig rumsavlyssning är generellt sett av särskilt ingripande karaktär och därför anförde regeringen i förarbetena till den lagen att det finns starka skäl att vara synnerligen restriktiv beträffande när åtgärden får användas, se propositionen Hemlig rumsavlyssning (prop. 2005/06:178 s. 51). Eftersom omständigheterna i det enskilda fallet styr hur stort integritetsintrång ett visst tvångsmedel utgör kan det dock finnas enskilda fall då hemlig rumsavlyssning utgör ett mindre integritetsintrång än andra tvångsmedel, se betänkandet Hemliga tvångsmedel mot allvarliga brott (SOU 2012:44 s. 516).

Hemlig övervakning av elektronisk kommunikation anses medföra ett klart mindre integritetsintrång än övriga hemliga tvångsmedel. I propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering jämförde regeringen hemlig övervakning av elektronisk kommunikation med hemlig avlyssning av elektronisk kommunikation och ansåg att övervakning var lindrigare eftersom övervakning inte ger uppgifter om innehållet i samtal eller meddelanden (prop. 2002/03:74 s. 23–24).

Hemlig kameraövervakning och hemlig avlyssning av elektronisk kommunikation har ansetts medföra integritetsintrång på likvärdiga nivåer och

användningen styrs därför av samma brottskatalog som reglerar när de får användas (se prop. 1995/96:85 s. 21–22).

Brottsbekämpande myndigheter kan redan i dag vid husrannsakan få rätt att ta del av elektroniskt lagrade uppgifter, t.ex. efter att en dator tas i beslag. Ett beslut om husrannsakan kräver endast att det finns anledning att anta att ett brott har begåtts på vilket fängelse kan följa. Beslag av ett föremål kräver endast att det skäligen kan antas ha betydelse för en utredning om brott eller vara avhänt någon genom ett brott eller förverkat på grund av brott. Till skillnad från husrannsakan och beslag kommer hemlig dataavläsning att utföras i hemlighet.

Hemlig dataavläsning som avser elektroniskt lagrade uppgifter och uppgifter om hur ett informationssystem används kan innebära en löpande realtidsövervakning av en persons förehavanden med ett informationssystem. Det kan ge tillgång till mycket känsliga uppgifter. Trots att uppgifterna i vissa fall är sådana som kan kommas åt genom husrannsakan och beslag kan integritetsintrånget anses tala för att kraven för att få använda åtgärden bör ställas lika högt som vid hemlig rumsavlyssning. Det kan nämligen hävdas att både hemlig rumsavlyssning och hemlig dataavläsning för att läsa av eller ta upp lagrade uppgifter och uppgifter om hur ett informationssystem används innebär en slags realtidsövervakning. Hemlig rumsavlyssning kan dock i större utsträckning än hemlig dataavläsning komma att avse förtroliga samtal med personer utan intresse för brottsutredningen eftersom rumsavlyssningen innefattar alla ljud och samtal i det avlyssnade rummet och är inte på samma sätt riktat mot användningen av ett enda informationssystem. På ett generellt plan anser regeringen därför att de nya åtgärder som föreslås inte kan anses vara lika ingripande för den enskilde som hemlig rumsavlyssning och bör därför inte jämställas med hemlig rumsavlyssning. Samtidigt är det uppenbart att hemlig dataavläsning för att få del av lagrade uppgifter och uppgifter om hur ett informationssystem används inte utgör ett så begränsat intrång som hemlig övervakning av elektronisk kommunikation.

Vid en samlad bedömning anser regeringen, i likhet med utredningen, att integritetsrisken vid hemlig dataavläsning för att läsa av eller ta upp lagrade uppgifter eller uppgifter som visar hur ett informationssystem används motsvarar vad som gäller vid hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. Det är därför rimligt att samma krav som gäller för dessa hemliga tvångsmedel även ska gälla för hemlig dataavläsning som avser lagrade uppgifter eller uppgifter som visar hur ett informationssystem används.

10.1.2 Vid vilka brott ska hemlig dataavläsning få användas?

Regeringens förslag: Ett tillstånd till hemlig dataavläsning ska få beviljas vid förundersökning om brott som kan leda till tillstånd till hemlig avlyssning av elektronisk kommunikation. Ett tillstånd till hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter ska få beviljas endast vid en förundersökning om brott som kan leda till tillstånd till hemlig rumsavlyssning.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget. *Åklagarmyndigheten* tillstyrker förslaget och anser att avgränsningen till vilka brott hemlig dataavläsning bör få användas är rimlig. *Datainspektionen* anser att förslaget omfattar möjlighet till tvångsmedel för brott som inte är tillräckligt allvarliga. Datainspektionen anser att utredningen borde ha prövat behovet och proportionaliteten för vart och ett av de brott som kan aktualisera hemlig dataavläsning. Vidare anser Datainspektionen att det som utgångspunkt endast bör bli aktuellt med hemlig dataavläsning för mycket allvarliga brott, t.ex. terroristbrott och mycket grov organiserad brottslighet, som kan påverka rikets säkerhet. *Svenska stadsnätsföreningen* och *Civil Rights Defenders* är av samma uppfattning och anser att tillämpningsområdet för hemlig dataavläsning bör begränsas och att det inte är tillräckligt att ange ett minimistraffvärde på två år för att få använda tvångsmedlet. *Sveriges advokatsamfund* och *Dataskydd.net* redovisar en liknande uppfattning. Sveriges advokatsamfund anser dessutom att hemlig dataavläsning bör vara förbehållet Säkerhetspolisen och komma i fråga endast vid mycket allvarlig brottslighet som utgör hot mot rikets säkerhet och som har som straffminimum eller förväntat straffvärde fängelse på fyra år eller mer. Även *Stiftelsen för Internetinfrastruktur (Internetstiftelsen)* och *Svenska stadsnätsföreningen* är av samma uppfattning.

Skälen för regeringens förslag: Som redogörs för i föregående avsnitt bör utgångspunkten för vilka krav som ska vara uppfyllda för att hemlig dataavläsning ska få användas för att läsa av eller ta upp uppgifter som får hämtas in med befintliga hemliga tvångsmedel motsvara de som gäller för de bakomliggande hemliga tvångsmedlen. I samma avsnitt görs också bedömningen att kraven för att få använda hemlig dataavläsning för att ta upp eller läsa av lagrade uppgifter och uppgifter om hur ett informationssystem används bör motsvara de som ställs för hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. Detta medför att de strafftrösklar som är föreskrivna för dessa tvångsmedel också som utgångspunkt ska tillämpas för hemlig dataavläsning.

Vissa remissinstanser, bl.a. *Datainspektionen* och *Sveriges advokatsamfund*, anser att de bakomliggande tvångsmedlens strafftrösklar inte bör bilda utgångspunkt för när hemlig dataavläsning ska kunna tillåtas utan att kravet för att få använda hemlig dataavläsning bör sättas högre så att tvångsmedlet endast kan användas vid mycket allvarlig brottslighet. De förordar en uppräkning, eller i vart fall en individuell prövning för vart och ett av de brott som kan bli aktuella att tillämpa hemlig dataavläsning för. Det kan hävdas att viss brottslighet, t.ex. terrorist- eller narkotikabrottslighet i allmänhet kräver mer kommunikation än annan allvarlig brottslighet, t.ex. en synnerligen grov misshandel utan föregående planering, och att behovet av åtgärder för att komma åt krypterad information i meddelanden därför är större i de förra fallen än i de senare. Emellertid avsätter en större andel av den totala brottsligheten i dag digitala spår. Det innebär att det kan vara av yttersta vikt att även vid ett brott som det senare kunna ta del av den misstänktes kommunikation eller annan information för att kunna knyta denne till brottet. Vikten av att kunna följa sådana spår kan inte anses mindre därför att det kan förväntas finnas färre uppgifter att hämta in. Mot den bakgrunden gör regeringen bedömningen att behovet

av hemlig dataavläsning inte i något avgörande avseende kan anses mindre för vissa brottskategorier än andra. Det är dessutom i enlighet med sedvanlig lagstiftningsteknik på det straffprocessuella tvångsmedelsområdet att ange en straffröskel för en viss tvångsåtgärd. Sådana trösklar finns vid en lång rad av möjliga åtgärder under en förundersökning; inte bara vid hemliga tvångsmedel utan också vid t.ex. häktning.

Eftersom verkställighet av hemlig dataavläsning i sig kan anses innebära en ökad risk för den personliga integriteten finns det dock skäl att i vissa delar höja kraven för när hemlig dataavläsning får användas. När det gäller avläsning eller upptagning av kommunikationsövervaknings- och platsuppgifter, dvs. uppgiftstyper som i dag får hämtas in genom hemlig övervakning av elektronisk kommunikation, bör kravet för hemlig dataavläsning sättas högre än vad som gäller för inhämtning av uppgifterna enligt nuvarande regler. Avläsning eller upptagning av sådana uppgifter bör, i enlighet med utredningens förslag, komma i fråga först vid sådana brott som kan föranleda tillstånd till hemlig avlyssning av elektronisk kommunikation. När det gäller kommunikationsavlyssningsuppgifter och kameraövervakningsuppgifter samt lagrade uppgifter och uppgifter som visar hur ett informationssystem används anser emellertid regeringen, i likhet med utredningen, att det inte finns skäl att göra avsteg från den ovan redovisade principen. Dessa åtgärder bör alltså kunna komma i fråga vid sådana brott som kan föranleda tillstånd till hemlig avlyssning av elektronisk kommunikation. Det ska noteras att de formella rekvisiten för hemlig avlyssning av elektronisk kommunikation avseende brottets allvar är desamma som för hemlig kameraövervakning.

Samma princip gör sig gällande när det gäller hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter. Åtgärden är i allt väsentligt är att jämställa med hemlig rumsavlyssning. Just när det gäller hemlig rumsavlyssning har det i förarbetena till införandet av tvångsmedlet ansetts att det med hänsyn till tvångsmedlets särskilt ingripande karaktär finns starka skäl för att vara synnerligen restriktiv med när tvångsmedlet ska få användas (prop. 2005/06:178 s. 51). Det finns inte skäl att avvika från denna hållning när rumsavlyssningen verkställs genom hemlig dataavläsning, varför kraven beträffande vilka brott som kan föranleda åtgärden bör sättas lika högt.

Vid hemlig avlyssning av elektronisk kommunikation finns en s.k. straffvärdeventil som anger att tillstånd får ges till tvångsmedlet om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år (27 kap. 18 § andra stycket RB). Det är enligt regeringen viktigt att det finns förutsättningar att använda hemlig dataavläsning även i dessa fall. Hemlig dataavläsning skulle då kunna aktualiseras vid misstanke om ett brott som inte har två års fängelse som minimistraff men som ändå i det enskilda fallet bedöms ha ett straffvärde på mer än fängelse i två år. Det kan t.ex. röra sig om mycket grova skattebrott, grova systematiska stölder, grov misshandel av allvarligt slag och rån som inte är att bedöma som grovt men med ett straffvärde över två år.

Vilka brott som bör kunna föranleda hemlig dataavläsning varierar således beroende på vilken åtgärd som tvångsmedlet avser. De straffnivåer som bestämmer när respektive tvångsmedel kan aktualiseras är enligt regeringens mening ändamålsenliga och tar hänsyn till tvångsmedlets ingripande karaktär samtidigt som kraven för användning av det inte ställs

för högt. Om lagstiftningen skulle utformas på så sätt att endast Säkerhetspolisen skulle ha möjlighet till hemlig dataavläsning eller att strafftröskeln skulle sättas lika högt som för hemlig rumsavlyssning, som bl.a. *Datainspektionen*, *Sveriges advokatsamfund* och *Civil Rights Defenders* anser, skulle tillämpningsområdet begränsas på ett sätt som inte stämmer med behovet av tvångsmedlet. Det skulle innebära att det vid mycket allvarliga brott som faller utanför Säkerhetspolisens verksamhetsområde fortfarande skulle saknas möjlighet att läsa av t.ex. krypterad trafik. Det skulle i förlängningen kunna leda till att vissa brott inte kan utredas. Det är inte acceptabelt.

Sammanfattningsvis föreslår regeringen, i likhet med utredningen, att hemlig dataavläsning ska få användas vid förundersökning om sådana brott som kan aktualisera hemlig avlyssning av elektronisk kommunikation. När det gäller hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter bör dock hemlig dataavläsning endast få användas vid förundersökning om sådana brott som kan föranleda hemlig rumsavlyssning.

10.1.3 Brottsmisstankens styrka och behovet av åtgärden

Regeringens förslag: Hemlig dataavläsning ska som utgångspunkt få användas endast om någon är skäligen misstänkt för brottet. Åtgärden ska vara av synnerlig vikt för utredningen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna lämnar förslaget utan kommentarer. *Svea hovrätt* och *Göteborgs* tingsrätt anser att hemlig dataavläsning innebär högre risker för den personliga integriteten och för informationssäkerheten än övriga hemliga tvångsmedel. Därför anser de att det bör övervägas att uttryckligen ange att hemlig dataavläsning är subsidiärt till andra tvångsmedel. Även *Sveriges advokatsamfund* anser att hemlig dataavläsning bör vara subsidiärt till övriga tvångsmedel och därför endast få användas efter att det visat sig att annat beslutat tvångsmedel inte gett avsett resultat.

Säkerhets- och integritetsskyddsnämnden anser att rekvisitet synnerlig vikt har getts delvis en annan innebörd än i nu gällande tvångsmedelsanvändning, eftersom utredningen anger att metoden för uppgiftsinhämtningen ska ges en särskilt framträdande roll vid bedömningen av tillståndsfrågan.

Skälen för regeringens förslag

Hemlig dataavläsning ska som huvudregel kräva en skäligen misstänkt

Användningen av nuvarande hemliga tvångsmedel under förundersökning förutsätter som huvudregel att det finns någon som är skäligen misstänkt för ett brott för vilket tvångsmedlet i fråga får användas. Hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning får dock under vissa förhållanden genomföras även utan att det finns en skäligen misstänkt person.

Att en person är skäligen misstänkt är ett högre ställt krav än att en person kan misstänkas för brott, men innebär ett lägre krav än att vederbörande är misstänkt på sannolika skäl. Om brottsmisstanken för att få använda hemliga tvångsmedel skulle bestämmas till sannolika skäl skulle det kunna leda till att åtgärderna blir utan betydelse i den brottsutredande verksamheten. Ett sådant krav innebär nämligen ofta att den mesta bevisningen redan är säkrad. Hemliga tvångsmedel används typiskt sett i ett tidigare skede, för att samla in uppgifter som kan leda till att misstankegraden når upp till sannolika skäl (se t.ex. Buggningsutredningens betänkande Om buggning och andra hemliga tvångsmedel, SOU 1998:46 s. 389–390). Att använda ett högre krav än skäligen misstänkt är därför inte lämpligt. Vidare framstår det som uteslutet att välja ett lägre krav än skäligen misstänkt med hänsyn till hur övrig reglering av hemliga tvångsmedel är utformad och den integritetsrisk som hemlig dataavläsning kan innebära, jfr propositionen om vissa tvångsmedelsfrågor (prop. 1988/89:124 s. 43–44) och prop. 1995/96:85 s. 28. Regeringens sammantagna bedömning är därför i likhet med utredningen att hemlig dataavläsning bör få användas endast om någon är skäligen misstänkt för ett brott som kan aktualisera åtgärden. Kravet bör gälla för samtliga uppgiftstyper som kan läsas av eller tas upp. Det ska dock noteras att regeringen föreslår att det under vissa förutsättningar bör finnas undantag från att det finns en skäligen misstänkt person (se avsnitt 10.1.5).

Åtgärden ska vara av synnerlig vikt för utredningen

Nuvarande hemliga tvångsmedel får endast användas om åtgärden är av synnerlig vikt för utredningen. I samband med införandet av det som då benämndes hemlig teleavlyssning och hemlig teleövervakning i rättegångsbalken uttalade departementschefen bl.a. att uttrycket synnerlig vikt för utredningen inte nödvändigtvis behöver avse att avlyssningen ska ge avgörande bevisning som omedelbart kan leda till fällande dom, utan kan ge uppslag till vidare spaning och för andra åtgärder. Vidare anförde hon att upplysningarna som kunde tänkas komma fram inte skulle inskränka sig till obetydliga detaljer, att avlyssningen bör vara nödvändig med hänsyn till utredningsläget och att vad som kan vinnas med åtgärden i princip inte får vara åtkomligt med andra, mindre ingripande metoder. Vad gäller det sist nämnda kan det ändå vara motiverat att använda tvångsmedlet om alternativen skulle kräva en orimligt hög personalinsats eller vara förenade med avsevärd risk att utredningen avslöjas. Utgångspunkten bör dock vara att i första hand pröva andra metoder, se propositionen Om vissa tvångsmedelsfrågor (prop. 1988/89:124 s. 44–45). Detta uttalande gör sig gällande även för hemlig dataavläsning och det är därför naturligt att kravet på synnerlig vikt för utredningen uppställs som villkor för användandet av hemlig dataavläsning. Regeringen anser därmed att kravet är väl avvägt i förhållande till både eventuella risker för integriteten eller andra intressen och det brottsbekämpande intresset.

Vid bedömningen av om det är av synnerlig vikt att hemlig dataavläsning ska få användas i ett enskilt fall är det viktigt att själva metoden för uppgiftsinhämtningen får en framträdande plats. Hemlig dataavläsning medför större risker för informationssäkerheten och i många fall även för integriteten än dagens tvångsmedel. Därför bör, som utredningen anför,

åtgärden endast användas när andra metoder inte är tillräckliga, är svårare att genomföra än hemlig dataavläsning eller förväntas leda till större integritetsintrång. I en förundersökning bör alltså mindre ingripande åtgärder vara överspelade eller inaktuella innan hemlig dataavläsning övervägs. Så kan vara fallet när det upptäcks att uppgifter eller enheter är krypterade. Vidare kan det vara väsentligt svårare att genomföra andra åtgärder än hemlig dataavläsning, t.ex. om hemlig rumsavlyssning ska genomföras på en plats som aldrig lämnas obevakad eller på en plats där hemlig kameraövervakning ska utföras men det inte är möjligt att fästa kamerautrustningen någonstans.

Regeringen anser dock inte, som bl.a. *Svea hovrätt* och *Göteborgs tingsrätt* föreslår, att det finns skäl att införa en bestämmelse om att hemlig dataavläsning ska vara subsidiär till andra tvångsmedel. Det bör således inte uppställas som krav för hemlig dataavläsning att de brottsbekämpande myndigheterna först måste begära tillstånd till andra hemliga tvångsmedel och konstatera att dessa är verkningslösa. Ett sådant förfarande skulle, framför allt när det är uppenbart att befintliga tvångsmedel inte skulle leda till resultat, endast fördröja och fördyra utredningen. Dessutom kan det i flera fall inte uteslutas att hemlig dataavläsning, vid en sammanvägd bedömning, faktiskt kan innebära ett förväntat mindre integritetsintrång än andra åtgärder. Rättens proportionalitetsbedömning vid domstolsprövningen är en garant för att hemlig dataavläsning inte används i onödan (avsnitt 9.4). Genom proportionalitetsprincipen anser regeringen, till skillnad från *Säkerhets- och integritetsskyddsnämnden,* även att det på ett tillräckligt sätt återspeglas i lagtext vilka överväganden som ska göras vid ett beslut om hemlig dataavläsning.

10.1.4 Krav på en bestämd plats vid avläsning eller upptagning av kameraövervaknings- eller rumsavlyssningsuppgifter

Regeringens förslag: Hemlig dataavläsning som används för att läsa av kameraövervakningsuppgifter ska få användas endast på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats ska dock inte få vara någons stadigvarande bostad.

Hemlig dataavläsning som används för att läsa av rumsavlyssningsuppgifter ska få användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Är platsen någon annan stadigvarande bostad än den misstänktes, ska avläsningen få utföras endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser kommenterar inte förslaget. *Svea hovrätt* anför att det utan ett platskrav skulle vara nästintill omöjligt att ta ställning till vilka integritetsintrång som en åtgärd kan medföra i det enskilda fallet. Platskravet medför dock vissa problem när åtgärden ska verkställas genom övervakning eller avlyssning av en mobiltelefon, eftersom den är i rörelse. Därför föreslår hovrätten att det borde vara möjligt att genom lämpliga villkor vid domstolsprövning avgränsa

tillståndet i det enskilda fallet på ett sådant sätt att åtgärden kan genomföras. Detta kan exempelvis ske genom att åtgärden får vidtas när den enskilde befinner sig i en viss situation, t.ex. på samma plats som en eller flera utpekade personer.

Polismyndigheten och *Tullverket* anser att det inte bör införas en bestämmelse som förutsätter anknytning till en plats utan i stället anknytning till en person. Polismyndigheten anför att regleringen riskerar att bli verkningslös med ett platskrav vid verkställighet eftersom elektronisk kommunikationsutrustning ofta förflyttas med personen. I så fall skulle det krävas ett omfattande spaningsarbete för att lokalisera personen innan hemlig dataavläsning kan verkställas. Detta riskerar att bli ännu mer integritetskränkande än förslaget som utredningen lämnar. Vidare kan det uppstå behov av att ompröva ett tidigare fattat beslut med mycket kort varsel om en misstänkt plötsligt ändrar mötesplats. Även hemlig kameraövervakning är problematiskt i det avseendet eftersom det inte går att tillämpa om man inte är säker på att den misstänkte finns i en bostad. Det kan uppstå situationer då myndigheterna behöver agera snabbt efter att ett tillfälle infunnit sig och det inte är möjligt att invänta ett tillträdestillstånd från domstol. Tullverket tillägger att det redan i dag finns en generell medvetenhet hos kriminella om lagstiftningens krav på plats för befintliga tvångsmedel och att detta utnyttjas.

Datainspektionen väcker frågan hur de brottsbekämpande myndigheterna ska kunna säkerställa att uppgifter läses av eller tas upp på en plats som omfattas av tillståndet om tillståndet avser den misstänktes mobiltelefon eftersom den är rörlig, till skillnad från fast avlyssnings- och övervakningsutrustning som används i dag.

Skälen för regeringens förslag: Platskravet för hemlig kameraövervakning innebär att åtgärden endast får avse en sådan plats där den misstänkte kan antas komma att uppehålla sig (27 kap. 20 b § RB). Motsvarande krav för hemlig rumsavlyssning är något strängare och innebär att åtgärden endast får avse en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig (27 kap. 20 e § RB). Som *Svea hovrätt* påpekar är platskravet viktigt för att kunna bedöma det förväntade integritetsintrånget. *Polismyndigheten* och *Tullverket* anser dock att principen om tvångsmedlets anknytning till en viss plats äventyrar tvångsmedlets effektivitet eftersom elektronisk kommunikationsutrustning ofta förflyttas med personen och att det då krävs ett omfattande spaningsarbete för att lokalisera personen innan hemlig dataavläsning kan verkställas.

I propositionen Hemlig kameraövervakning diskuterade regeringen frågan om tillståndet skulle knytas till person eller plats (prop. 1995/96:85 s. 29). Om tillståndet skulle avse en person konstaterade regeringen att ändamålsprincipen, behovsprincipen och proportionalitetsprincipen skulle bli svåra att tillämpa. Som exempel anfördes att det inte skulle gå att tillämpa proportionalitetsprincipen eftersom det på förhand inte är känt vilka eller hur många platser som skulle komma att övervakas. Vid en förundersökning som avser ett visst brott skulle, beroende på omständigheterna, övervakning av en allmän plats kanske anses vara godtagbar medan övervakning av en enskild plats, t.ex. genom att kameran riktades mot ett bostadsfönster, inte skulle kunna komma i fråga. Mot denna bakgrund och av praktiska skäl fann regeringen att tillstånd till hemlig

kameraövervakning skulle knytas till plats i stället för till person. Regeringen gör i detta lagstiftningsarbete samma principiella bedömning och föreslår att en verkställighet genom hemlig dataavläsning också ska vara underkastad ett platskrav. Att det kan krävas spaningsarbete eller liknande insatser för att säkerställa platsvillkoret utgör inte ett tillräckligt skäl att göra någon annan bedömning. Ställningstagandet ligger i linje med den slutsats som Utredningen om regeländringar för vissa hemliga tvångsmedel har kommit fram till i betänkandet Förenklat förfarande vid vissa beslut om hemlig avlyssning, nämligen att det inte finns tillräckliga skäl att knyta ett tvångsmedel till en person, bl.a. eftersom de integritetsintrång som annars kan befaras är för stora (SOU 2018:30 s. 53–59). Regeringen anser inte heller att den lösning som *Svea hovrätt* föreslår, att göra undantag från platskravet i vissa fall, är förenlig med de principer om ett generellt platskrav som nyss nämnts. Det är den brottsbekämpande myndigheten som ska verkställa åtgärden som har att se till att kravet angående plats efterlevs.

För hemlig kameraövervakning gäller vidare att det med hänsyn till risker för den personliga integriteten inte är tillåtet att övervaka någon som befinner sig i en stadigvarande bostad med en kamera som finns i den bostaden (se t.ex. prop. 1995/96:85 s. 30 och prop. 2013/14:237 s. 154–155). Det betyder att åtgärden endast får användas på en plats där den misstänkte kan antas komma att uppehålla sig och att en sådan plats inte får vara någons stadigvarande bostad. Utredningen föreslår att motsvarande krav ska gälla för hemlig dataavläsning av kameraövervakningsuppgifter. Ingen remissinstans invänder mot förslaget i denna del utom *Polismyndigheten* som bedömer att det kommer att bli svårt att verkställa hemlig dataavläsning av kameraövervakningsuppgifter vid osäkerhet om huruvida den misstänkte befinner sig i en stadigvarande bostad. Förbudet mot avläsning eller upptagning av kameraövervakningsuppgifter i någons bostad överensstämmer dock med bakomliggande reglering för hemlig kameraövervakning och har ansetts vara en nödvändig garant för den personliga integriteten (se prop. 2013/14:237 s. 154–155). Regeringen gör ingen annan bedömning och anser därför att utredningens förslag bör genomföras.

För hemlig rumsavlyssning gäller att åtgärden endast får användas på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig och, om platsen är någon annan stadigvarande bostad än den misstänktes, att det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. Utredningen föreslår att motsvarande begränsning ska gälla för avläsning av rumsavlyssningsuppgifter. Ingen remissinstans invänder mot det. Regeringen instämmer i utredningens förslag att motsvarande krav bör gälla vid hemlig dataavläsning när metoden används för att avläsa eller ta upp rumsavlyssningsuppgifter. I likhet med utredningen föreslår regeringen att hemlig dataavläsning som gäller rumsavlyssningsuppgifter inte får avse vissa platser (se vidare avsnitt 10.3.2).

10.1.5 Koppling mellan en enskild och ett informationssystem

Regeringens förslag: Hemlig dataavläsning ska få avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för ett brott.

Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter ska även få avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter ska även få beviljas för att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Avläsning eller upptagning av kommunikationsövervakningsuppgifter ska då endast få avse förfluten tid. En sådan åtgärd ska endast få avse ett avläsningsbart informationssystem som har använts vid ett brott eller i anslutning till en brottsplats vid brottstidpunkten eller som av någon annan anledning är av synnerlig vikt för utredningen.

Regeringens bedömning: Det behöver inte föreskrivas att hemlig dataavläsning, i syfte att utreda vem som skäligen kan misstänkas för brott, inte får avse informationssystem som tillhör någon som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för brott inte ska få avse informationssystem som tillhör någon som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Utredningen föreslår att ett tillstånd till hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för ett visst brott ska få beviljas om det är av synnerlig betydelse för att utreda vem som skäligen kan misstänkas för brottet.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget. *Datainspektionen* anser att utredningen inte på ett tillräckligt sätt har belyst svårigheten i att identifiera ett visst informationssystem och koppla det till en misstänkt. Svårigheten gör att de brottsbekämpande myndigheterna kommer att möta problem med att tillgodose rättssäkerheten. *Malmö tingsrätt* anför att utredningen utgår från att hemlig dataavläsning av ett informationssystem som tillhör någon annan än en misstänkt endast ska få ske vid mycket allvarlig brottslighet. Tingsrätten anser därför att det bör regleras särskilt att det inte ska vara möjligt att ge tillstånd till en sådan åtgärd vid mindre allvarlig brottslig verksamhet. *Civil Rights Defenders* motsätter sig att hemlig dataavläsning ska få användas i ett informationssystem som används av en annan person än den misstänkte. *Dataskydd.net* anser inte att tvångsmedel över huvud taget ska kunna användas mot en person som inte är misstänkt för brott och avstyrker därför att några åtgärder får användas för att utröna vem som kan vara skäligen misstänkt för brott. *Säkerhets- och integritetsskyddsnämnden* och

Säkerhetspolisen anser att utredningen inte har redovisat varför hemlig dataavläsning för att ta upp kameraövervakningsuppgifter inte ska få användas för att utröna vem som kan vara misstänkt för ett brott, vilket är möjligt enligt 27 kap. 20 c RB. Säkerhetspolisen anser också att det borde införas en bestämmelse som tillåter att en utrustnings kamera eller mikrofon används för att identifiera en misstänkt person.

Skälen för regeringens förslag och bedömning

Nuvarande regler i rättegångsbalken om koppling till en enskild

Hemlig avlyssning och hemlig övervakning av elektronisk kommunikation får avse 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. Åtgärderna får riktas mot 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 (27 kap. 20 § första och andra stycket RB). Synnerlig anledning att anta att det finns en sådan koppling betyder att man ska vara så gott som säker på att den misstänkte kommer att kontakta den aktuella adressen (prop. 2002/03:74 s. 38).

Reglerna om koppling mellan den enskilde och en teknisk utrustning finns till för att skydda integriteten och rättssäkerheten och ska minska risken för att personer som är ovidkommande för utredningen drabbas av åtgärderna (se t.ex. prop. 1988/89:124 s. 46).

Hemlig övervakning av elektronisk kommunikation får också genomföras i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen (27 kap. 20 § andra stycket RB). Uppgifter som då inhämtas om meddelanden får endast avse förfluten tid.

Det ska som huvudregel finnas en koppling mellan den misstänkte och informationssystemet

Hemlig dataavläsning föreslås få användas för att få tillgång till uppgifter i avläsningsbara informationssystem, såsom mobiltelefoner, datorer och läsplattor. Ett viktigt skydd för den personliga integriteten, framför allt för andra personer än den misstänkte, är att det ska finnas en koppling mellan den misstänkte och det informationssystem som det ska vidtas åtgärder i. En bestämmelse om en sådan koppling behövs därför i lagen om hemlig dataavläsning.

Det lämpligaste sättet att uttrycka en koppling mellan en enskild och ett informationssystem är, som utredningen föreslår, att informationssystemet används av den misstänkte. Det bör inte införas några regler om hur frekvent informationssystemet ska användas, eftersom det då skulle vara enkelt för kriminella att vidta motåtgärder genom att t.ex. administrera flera konton i sociala medier eller använda flera mobiltelefoner samtidigt. Det ingår dock i proportionalitetsprövningen att pröva om det är lämpligt att läsa av uppgifter i informationssystem som endast används tillfälligt (se vidare avsnitt 9.4).

Det behövs också regler om hur stark kopplingen ska vara mellan den enskilde och informationssystemet i fråga. För hemlig avlyssning av elektronisk kommunikation används det relativt låga beviskravet att ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning kan antas ha använts eller komma att användas av den misstänkte. Detta framstår som för lågt ställt för hemlig dataavläsning eftersom tvångsmedlet generellt sett innebär större risker för intrång i den personliga integriteten hos den enskilde. Inte heller är det lämpligt att sätta kravet så högt som synnerlig anledning att anta eftersom det innebär att man måste vara nästan säker på att den misstänkte kommer att kontakta adressen.

Utredningen föreslår att beviskravet för kopplingen sätts till särskild anledning att anta att informationssystemet har använts eller kommer att användas av den misstänkte. Ingen remissinstans invänder mot beviskravets styrka. Kravet innebär att utredningsläget måste visa någon faktisk omständighet som med viss styrka talar för att den misstänkte har använt eller kommer att använda informationssystemet under tillståndstiden. En sådan omständighet kan t.ex. vara att informationssystemet finns hemma hos den misstänkte eller på någon annan plats där han eller hon vistas regelbundet. Regeringen anser att det föreslagna kravet är väl avvägt. Huvudregeln bör därför vara att hemlig dataavläsning endast får avse ett avläsningsbart informationssystem som används, eller som det annars finns särskild anledning att anta har använts eller kommer att användas, av den misstänkte.

Regeringen har förståelse för *Datainspektionens* synpunkt att det kan vara svårt att identifiera ett informationssystem och koppla det till den enskilde. Det är dock en uppgift för de brottsbekämpande myndigheterna, som efter spaningsarbete eller på annat sätt måste kunna visa en sådan koppling. Eventuella svårigheter att nå upp till det föreslagna beviskravet för koppling mellan den som åtgärden riktar sig mot och informationssystemet får inte gå ut över rättssäkerheten, som Datainspektionen uttrycker en oro för. Om beviskravet inte uppnås får inte hemlig dataavläsning tillåtas.

Ett undantag från huvudregeln för informationssystem som den misstänkte kontaktar

Hemlig avlyssning och övervakning av elektronisk kommunikation får avse 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 (27 kap. 20 § första stycket 2 RB). Utredningen föreslår att motsvarande bör gälla för hemlig dataavläsning, vilket *Civil Rights Defenders* och *Dataskydd.net* invänder mot. Det är enligt regeringen av väsentlig betydelse att hemlig dataavläsning kan användas i motsvarande fall som de befintliga hemliga tvångsmedlen. Det finns annars risk för att vissa allvarliga brott inte kan utredas när det visar sig vara omöjligt att använda befintliga hemliga tvångsmedel. För hemlig dataavläsning bör det alltså finnas ett undantag från huvudregeln om att åtgärden endast får avse informationssystem som används av en misstänkt när det är fråga om avläsning eller upptagning av uppgifter som kan hämtas in genom hemlig

avlyssning och övervakning av elektronisk kommunikation. Undantaget bör dock endast kunna tillämpas i mycket särpräglade situationer och bör kräva att det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta informationssystemet. Det betyder att man måste vara nästan säker på att den misstänkte kommer att kontakta det aktuella informationssystemet. Det kan t.ex. ha kommit fram konkreta indikationer på att en misstänkt ska kontakta en annan persons mobiltelefon vid ett visst tillfälle. Även i dessa fall bör ställas krav på åtgärdens proportionalitet och att den är av synnerlig vikt för utredningen. Regeringen anser dock inte att det finns anledning att, som *Malmö tingsrätt* är inne på, ytterligare särreglera vad som gäller för hemlig dataavläsning när avläsningen eller upptagningen avser ett informationssystem som används av en person som inte är misstänkt för brott.

Ett ytterligare undantag för att utreda vem som skäligen kan misstänkas för brottet

Om det är av synnerlig vikt för utredningen får domstol lämna tillstånd till hemlig övervakning av elektronisk kommunikation för att utreda vem som skäligen kan misstänkas för brottet (27 kap. 20 § andra stycket RB). I dessa fall finns alltså inte någon misstänkt person. Eftersom det inte finns någon misstänkt person finns det inte heller någon koppling mellan en misstänkt och det informationssystem som åtgärderna ska vidtas i. De uppgifter som övervakningen kan ge tillgång till är samma slags uppgifter som får hämtas in enligt inhämtningslagen, dvs. historiska uppgifter om meddelanden samt historiska och realtidsbaserade platsuppgifter.

I likhet med vad som gäller för befintliga hemliga tvångsmedel bör det, som utredningen föreslår och till skillnad från vad *Dataskydd.net* anser, finnas en möjlighet att använda hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för ett visst brott. Det kan ge viktiga upplysningar när det har begåtts ett allvarligt brott men det inte går att hitta någon misstänkt. Utan en sådan möjlighet finns det risk för att brottsbekämpande myndigheter inte kan gå vidare i utredningar om allvarliga brott. Hemlig dataavläsning bör dock endast få tillgripas mot avläsningsbara informationssystem som funnits på eller i anslutning till en brottsplats eller om uppgifterna av något annat skäl är av synnerlig vikt för utredningen. Regeringen väljer därmed en formulering som närmare anknyter till 27 kap. 20 och 20 c §§ RB och inte utredningens förslag om att uppgifterna får läsas av eller tas upp om det är av synnerlig betydelse för att utreda vem som skäligen kan misstänkas för brottet. Skillnaden mellan uttrycken torde dock i praktiken vara närmast språklig och uttrycket synnerlig vikt för utredningen bör täcka samtliga fall som bedöms vara av synnerlig betydelse för att utreda vem som skäligen kan misstänkas för brottet.

Enligt gällande rätt får hemlig kameraövervakning användas för att fastställa vem som skäligen kan misstänkas för brottet (27 kap. 20 c § RB). Utredningen lämnar inte något förslag om att hemlig dataavläsning ska få användas i ett sådant syfte. *Säkerhets- och integritetsskyddsnämnden* och *Säkerhetspolisen* efterfrågar en analys i frågan. Det kan konstateras att sådan kameraövervakning som enligt rättegångsbalken får användas för att

identifiera en misstänkt endast får avse den plats där brottet har begåtts eller en nära omgivning till denna plats. Sådana fall kan t.ex. vara när ett parti narkotika hittas på en viss plats. Då kan en kamera monteras på platsen för att iaktta vilka som besöker den. Behovet av hemlig dataavläsning i ett sådant fall, eller andra fall där hemlig kameraövervakning får användas för att identifiera en misstänkt, framstår inte som särskilt stort. Regeringen har således svårt att se tillräckliga behov av åtgärden och lämnar därför, i likhet med utredningen, inget sådant förslag.

Vad gäller *Säkerhetspolisens* förslag om att de brottsbekämpande myndigheterna ska få använda hemlig dataavläsning för att ta upp rumsavlyssnings- och kameraövervakningsuppgifter för att kunna identifiera en person gör regeringen följande bedömning. Regeringen ifrågasätter inte att det finns fall där det skulle vara verksamhetsmässigt värdefullt att kunna ta upp sådana uppgifter som Säkerhetspolisen föreslår. En utgångspunkt för regeringen är emellertid att hemlig dataavläsning ska vara ett verktyg som ska återställa de brottsbekämpande myndigheternas förmåga. Säkerhetspolisens förslag får anses som en inte obetydlig utvidgning av vad som är rättsligt möjligt i dag. Förutom integritetsintrånget av ett sådant ingrepp ser regeringen svårigheter att säkerställa att åtgärden uppfyller det platskrav som ställs på rumsavlyssningsuppgifter (avsnitt 10.1.4). Regeringen lämnar därför inte något sådant förslag.

Hemlig dataavläsning bör inte vara förbjuden mot avläsningsbara informationssystem som tillhör en operatör

Utredningen föreslår ett förbud mot att i vissa fall använda hemlig dataavläsning mot operatörer som tillhandahåller elektroniska kommunikationsnät eller elektroniska kommunikationstjänster. Utredningen motiverar det med att det inte ska vara möjligt att ansöka om tillstånd till hemlig dataavläsning mot en operatör om operatören inte velat medverka vid verkställighet och på så sätt kringgå operatörens besked. Som framgår nedan gör regeringen en annan bedömning än utredningen i frågan om operatörernas medverkansskyldighet och bedömer att en sådan ska införas (avsnitt 12.2.2). Med hänsyn till detta finns det inte anledning genomföra utredningens förslag om att hemlig dataavläsning inte får riktas mot operatörer.

10.2 Hemlig dataavläsning utanför en förundersökning

10.2.1 Utgångspunkter

Regeringens bedömning: Hemlig dataavläsning bör få användas i underrättelseverksamhet och vid särskild utlänningskontroll.

Vid hemlig dataavläsning i syfte att läsa av eller ta upp uppgifter som får hämtas in genom befintliga hemliga tvångsmedel, bör som utgångspunkt motsvarande krav gälla som gäller för det bakomliggande tvångsmedlet.

Vid hemlig dataavläsning i underrättelseverksamhet och vid särskild utlänningskontroll för att läsa av eller ta upp lagrade uppgifter eller

uppgifter som visar hur ett informationssystem används bör kravet för hemlig dataavläsning motsvara vad som gäller för hemlig avlyssning av elektronisk kommunikation.

Hemlig dataavläsning utanför en förundersökning bör inte omfatta rumsavlyssningsuppgifter.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Endast ett fåtal remissinstanser kommenterar bedömningen. *Säkerhetspolisen* och *Tullverket* välkomnar att hemlig dataavläsning ska kunna användas i underrättelseverksamhet.

Civil Rights Defenders avstyrker att någon annan myndighet än Säkerhetspolisen ska kunna använda sig av hemlig dataavläsning utanför en förundersökning eftersom hemlig dataavläsning utgör ett stort integritetsintrång utan konkret brottsmisstanke. Det bör därför endast användas vid misstanke om mycket allvarlig brottslighet som utgör hot mot rikets säkerhet. Även *Sveriges advokatsamfund* anser att hemlig dataavläsning utanför en förundersökning endast bör tillåtas vid misstanke om mycket allvarlig brottslighet som utgör hot mot rikets säkerhet och som har ett straffminimum eller förväntat straffvärde på fängelse i minst fyra år. Sveriges advokatsamfund anser därför att frågan bör analyseras och beredas ytterligare. *Dataskydd.net* avstyrker att hemlig dataavläsning ska få användas utanför en förundersökning. *Säkerhets- och integritetsskyddsnämnden* avstyrker att hemlig dataavläsning införs utanför en förundersökning utöver tillämpningsområdet för preventivlagen och lagen om särskild utlänningskontroll.

Skälen för regeringens bedömning: Regler om hemlig tvångsmedelsanvändning utanför en förundersökning finns i preventivlagen, lagen om särskild utlänningskontroll och inhämtningslagen. Utredningen bedömer att även hemlig dataavläsning inom vissa ramar bör få användas utanför en förundersökning, något som välkomnas av *Säkerhetspolisen* och *Tullverket*. Några remissinstanser, bl.a. *Sveriges advokatsamfund*, är av uppfattningen att hemliga tvångsmedel inte bör få användas utanför en förundersökning eller enbart enligt vissa lagar eller att det bör krävas misstanke om mycket allvarlig brottslighet för att hemlig dataavläsning ska få komma i fråga.

Som skäl för sin bedömning att hemlig dataavläsning som syftar till att läsa av eller ta upp uppgifter som får hämtas in genom befintliga tvångsmedel bör tillåtas även utanför en förundersökning anför utredningen att behovet är lika tungt vägande där som i brottsutredande verksamhet. Genom ökade möjligheter till informationsinhämtning skulle de brottsbekämpande myndigheterna ges förutsättningar att på ett mer effektivt sätt förhindra terrordåd och annan systemhotande brottslighet. Utredningen bedömer därför att hemlig dataavläsning bör få användas utanför en förundersökning men begränsas till allvarlig brottslighet under vissa särskilda förhållanden. Som anförs i avsnitt 8.2 menar även regeringen att det finns ett påtagligt behov av hemlig dataavläsning utanför en förundersökning. Det kan också antas att åtgärden kommer att vara effektiv (se avsnitt 8.4). En förutsättning för att hemlig dataavläsning ska tillåtas utanför en förundersökning är dock att åtgärden, liksom under förundersökning, omgärdas av särskilda rättssäkerhetsgarantier. Eftersom sådana föreslås gälla både i och utanför en förundersökning (se avsnitt 12.1) delar regeringen

utredningens bedömning att hemlig dataavläsning i viss utsträckning bör tillåtas även utanför en förundersökning.

Eftersom införandet av hemlig dataavläsning till stor del syftar till att återställa de brottsbekämpande myndigheternas förmåga att förhindra och utreda brott bör utgångspunkten vara att kraven som gäller för det hemliga tvångsmedlet enligt respektive lag ska gälla även för hemlig dataavläsning.

Det finns också ett stort behov av att i underrättelseverksamhet och vid särskild utlänningskontroll få använda hemlig dataavläsning för att läsa av eller ta upp lagrade uppgifter eller uppgifter som visar hur ett informationssystem används (avsnitt 8.3). Det kan t.ex. vara fråga om bilder, filmer och ljudfiler som en potentiell gärningsperson har sparat på sin telefon eller anteckningar och påbörjade meddelanden som inte sparats på en telefon eller en dator. Med tillgång till sådan information i ett tidigt skede förbättras möjligheterna att stoppa planerad grov brottslighet. Som regeringen redogör för i avsnitt 8.3 kan åtgärden även i dessa delar antas vara effektiv. Även utanför en förundersökning bör krävas att åtgärden omgärdas av särskilda rättssäkerhetsgarantier (se avsnitt 12.1). Regeringen instämmer i utredningens bedömning att det bör införas en möjlighet till hemlig dataavläsning i underrättelseverksamhet och vid särskild utlänningskontroll såvitt avser lagrade uppgifter eller uppgifter som visar hur ett informationssystem används. För de uppgifter som får tas upp genom befintliga hemliga tvångsmedel konstateras ovan att de bakomliggande tvångsmedlen bildar en rimlig utgångspunkt för vilka krav som bör uppställas när samma uppgifter inhämtas genom hemlig dataavläsning. När hemlig dataavläsning däremot tillämpas för lagrade uppgifter och uppgifter som visar hur ett informationssystem används saknas befintliga hemliga tvångsmedel som kan bilda utgångspunkt för vilka krav som bör uppställas. Det finns dock enligt regeringens mening inte skäl att göra någon annan bedömning än vad som föreslås i förundersökningsverksamhet (se vidare avsnitt 10.1.1). De nu aktuella uppgifterna bör alltså få hämtas in under samma förutsättningar som gäller för hemlig avlyssning av elektronisk kommunikation.

Hemlig rumsavlyssning är inte tillåten enligt någon av de lagar som reglerar tvångsmedel i underrättelseverksamhet eller vid särskild utlänningskontroll. Mot bakgrund av det anser regeringen, i likhet med utredningen, att inte heller hemlig dataavläsning avseende rumsavlyssningsuppgifter bör få förekomma i dessa fall.

10.2.2 Hemlig dataavläsning i preventivlagsfallen

Regeringens förslag: Ett tillstånd till hemlig dataavläsning ska få beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva sådan brottslig verksamhet som anges i preventivlagen eller att sådan brottslig verksamhet kommer att utövas inom en organisation eller grupp och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Tillstånd ska få beviljas endast om åtgärden är av synnerlig vikt för att förhindra brottsligheten.

Hemlig dataavläsning av kameraövervakningsuppgifter ska få användas endast på en plats där den person som är föremål för åtgärden kan antas komma att uppehålla sig. En sådan plats ska dock inte få vara någons stadigvarande bostad.

Ett tillstånd ska inte få avse rumsavlyssningsuppgifter.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget. *Sveriges advokatsamfund* anser att det krav som ställs i preventivlagen på att det ska finnas påtaglig risk för att en person kommer att utöva brottslig verksamhet är för lågt och att det i stället bör krävas uppenbar risk vid hemlig dataavläsning. Vidare bör det enligt samfundet förtydligas att insatsen tar sikte på en viss namngiven person och inte en person som utredningen föreslår. *Stockholms universitet (Juridiska fakulteten)* anser att det inte bör införas en bestämmelse som innebär att tillstånd till hemlig dataavläsning kan avse en organisation eller grupp. Detta kan avse stora datamängder och med hänsyn till politiska förskjutningar kan det komma att avse mycket stora grupper av människor.

Skälen för regeringens förslag: Enligt preventivlagen finns möjlighet att få tillstånd till hemlig avlyssning och övervakning av elektronisk kommunikation samt hemlig kameraövervakning. När det gäller förutsättningarna för användning av hemliga tvångsmedel enligt preventivlagen (preventivlagsfallen) skiljer de sig åt jämfört med rättegångsbalkens bestämmelser.

Tillstånd till hemliga tvångsmedel enligt preventivlagen får beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva viss i lagen angiven särskilt allvarlig brottslighet (1 § första stycket). Tillstånd får också ges om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas sådan brottslig verksamhet och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet (1 § andra stycket). Den brottsliga verksamhet som kan föranleda hemliga tvångsmedel enligt preventivlagen består genomgående av mycket allvarliga brott. I preventivlagen uppställs motsvarande krav på plats som gäller enligt rättegångsbalken vid hemlig kameraövervakning. Dessutom krävs alltid att åtgärden ska vara av synnerlig vikt för att förhindra den brottsliga verksamheten som anges i lagen och att den är proportionerlig.

Som redogörs för i avsnitt 10.2.1 anser regeringen att hemlig dataavläsning bör få användas även i underrättelseverksamhet. Det gör sig särskilt starkt gällande i preventivlagsfallen som typiskt sett befinner sig tämligen nära en punkt då en förundersökning ska inledas. Regeringen anser, i likhet med utredningen, att hemlig dataavläsning bör få användas i samtliga fall när det föreligger omständigheter som kan leda till tvångsmedelsanvändning enligt preventivlagen. Regeringen gör därmed en annan bedömning än *Sveriges advokatsamfund* och *Stockholms universitet (Juridiska fakulteten),* som anser att det bör ställas högre krav för att hemlig dataavläsning ska få användas i preventivlagsfallen än vad som gäller för befintliga hemliga tvångsmedel enligt preventivlagen. Det kan tilläggas att det i dessa fall är fråga om mycket allvarlig brottslighet som

det finns ett stort behov av att kunna stoppa, t.ex. planerade terroristattentat. Det finns risk att uppgifterna inte kan tas upp eller läsas av om kraven för hemlig dataavläsning i dessa situationer är för höga. Alltför höga krav skulle inverka negativt på de brottsbekämpande myndigheternas förmåga att hindra allvarlig brottslighet på ett sätt som inte skulle vara försvarligt.

När hemlig dataavläsning används i preventivlagsfallen bör det på motsvarande sätt som enligt preventivlagen krävas att åtgärden ska vara av synnerlig vikt för att förhindra den brottsliga verksamheten (5 § preventivlagen). Även motsvarande platskrav som preventivlagen föreskriver för hemlig kameraövervakning bör gälla vid hemlig dataavläsning när det är fråga om avläsning eller upptagning av kameraövervakningsuppgifter (8 § tredje stycket preventivlagen). I likhet med vad som föreslås om hemlig dataavläsning som gäller kameraövervakningsuppgifter under en förundersökning bör sådana uppgifter inte få läsas av eller tas upp i någons stadigvarande bostad.

10.2.3 Kopplingen mellan en enskild och ett avläsningsbart informationssystem i preventivlagsfallen

Regeringens förslag: Hemlig dataavläsning ska få avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en person som kan omfattas av hemliga tvångsmedel enligt preventivlagen.

Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter ska även få avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den berörde personen under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag: Vid hemlig avlyssning och övervakning av elektronisk kommunikation enligt preventivlagen ska det finnas en koppling mellan en person som kan bli föremål för en åtgärd och det telefonnummer, adress eller kommunikationsutrustning som åtgärden ska avse (2 § första stycket 1). Preventivlagen har en motsvarande regel som i rättegångsbalken om att hemlig avlyssning eller övervakning av elektronisk kommunikation även får avse ett telefonnummer, en annan adress eller en elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att personen i fråga under den tid tillståndet avser har kontaktat eller kommer att kontakta (2 § första stycket 2 preventivlagen).

Eftersom hemlig dataavläsning så långt som möjligt bör anpassas till det bakomliggande tvångsmedlet bör samma förutsättningar som gäller enligt preventivlagen gälla även när hemlig dataavläsning används i sådana fall. Det innebär således att hemlig dataavläsning bör få avse ett avläsningsbart informationssystem som används av eller det finns särskild anledning att anta har använts eller kommer att användas av person som kan bli föremål för hemliga tvångsmedel enligt preventivlagen. Om det är fråga om ett

annat informationssystem än som nu sagts bör det krävas att uppgifterna finns i ett informationssystem som det finns synnerlig anledning att anta att en sådan person har kontaktat eller kommer att kontakta. Dessutom bör det i dessa fall endast kunna komma i fråga att läsa av kommunikationsavlyssnings-, kommunikationsövervaknings- och platsuppgifter.

Enligt gällande rätt får hemlig kameraövervakning enligt preventivlagen avse en plats där den person som är föremål för tvångsmedlet kan antas komma att uppehålla sig, eller på en plats där viss brottslig verksamhet kan antas komma att utövas eller en nära omgivning till denna plats (3 §). Utredningen lämnar inte något förslag om att hemlig dataavläsning ska få användas i preventivlagsfallen för att övervaka en viss plats eller nära omgivning till denna plats där brottslig verksamhet kan antas komma att utövas. I likhet med vad som anförs i avsnitt 10.1.5 anser regeringen att behovet av hemlig dataavläsning i sådana fall inte är särskilt stort och lämnar därför, i likhet med utredningen, inget sådant förslag.

10.2.4 Hemlig dataavläsning vid särskild utlänningskontroll

Regeringens förslag: Ett tillstånd till hemlig dataavläsning ska få beviljas i fråga om en utlänning som omfattas antingen av ett utvisningsbeslut enligt 1 § 2 lagen om särskild utlänningskontroll eller av ett avvisnings- eller utvisningsbeslut enligt 8 eller 8 a kap. utlänningslagen eller motsvarande äldre bestämmelser och det finns sådana omständigheter i fråga om utlänningen som avses i 1 § 2 lagen om särskild utlänningskontroll och som Migrationsverket, regeringen eller en domstol har beslutat att 19–22 §§ den lagen samt lagen om hemlig dataavläsning ska tillämpas på. Det förfarande och de förutsättningar som gäller för ett beslut om att 19–22 §§ lagen om särskild utlänningskontroll ska tillämpas i fråga om utlänningen ska också gälla för ett beslut om att hemlig dataavläsning ska få beviljas i fråga om utlänningen.

Ett tillstånd ska få beviljas endast om det finns synnerliga skäl och det är av betydelse för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott. Ett tillstånd till hemlig dataavläsning i samband med särskild utlänningskontroll ska dock inte få avse kameraövervaknings- eller rumsavlyssningsuppgifter.

I lagen om särskild utlänningskontroll ska det tas in en upplysning om att rätten kan bevilja Säkerhetspolisen eller Polismyndigheten tillstånd till hemlig dataavläsning.

Utredningens förslag överensstämmer med regeringens. Utredningen föreslår dock inte att det ska tas in en upplysning i lagen om särskild utlänningskontroll.

Remissinstanserna kommenterar inte förslaget särskilt. *Migrationsverket* anför dock att det behövs en översyn av lagen om särskild utlänningskontroll och att eventuella slutsatser från denna kan vara värdefulla även när det gäller hemlig dataavläsning.

Skälen för regeringens förslag: Åtgärder enligt lagen om särskild utlänningskontroll syftar bl.a. till att förebygga terroristbrott. De hemliga tvångsmedlen i den lagen har begränsats till hemlig avlyssning och hemlig övervakning av elektronisk kommunikation. Tvångsmedlen enligt lagen om särskild utlänningskontroll (LSU-fallen) får endast användas mot en utlänning som omfattas av ett utvisningsbeslut grundat på att det med hänsyn till vad som är känt om utlänningens tidigare verksamhet och övriga omständigheter kan befaras att han eller hon kommer att begå eller medverka till terroristbrott eller försök, förberedelse eller stämpling till sådant brott. Beslut om hemliga tvångsmedel kräver vidare att det är av betydelse för att utröna om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott. Det finns inte något krav på brottsmisstanke för att tvångsmedlen ska få användas. Det måste dock finnas synnerliga skäl för åtgärden (20 §).

Som anges i avsnitt 10.2.1 är en utgångspunkt för regeringen att hemlig dataavläsning ska få användas även i underrättelseverksamhet och i avsnitt 8.2 och 8.3 konstateras att det finns behov av att läsa av eller ta upp både uppgifter som i dag kan kommas åt med befintliga tvångsmedel och nya slags uppgifter. Hemlig dataavläsning bör av samma skäl få användas även vid särskild utlänningskontroll. Hemlig kameraövervakning och hemlig rumsavlyssning är inte tillåtet enligt lagen om särskild utlänningskontroll. Därför bör hemlig dataavläsning vid förhållanden som kan leda till tvångsmedelsanvändning enligt lagen om särskild utlänningskontroll inte omfatta kameraövervakning- eller rumsavlyssningsuppgifter.

Det sagda innebär att ett tillstånd till hemlig dataavläsning bör kunna ges när det har beviljats ett utvisningsbeslut med stöd av 1 § 2 LSU och Migrationsverket, regeringen eller en domstol har bestämt att reglerna om tvångsmedel och hemlig dataavläsning ska tillämpas på utlänningen (jfr 11, 14 och 15 §§ LSU). Även i de fall då en utlänning omfattas ett beslut om avvisning eller utvisning enligt 8 eller 8 a kap. utlänningslagen (2005:716) eller motsvarande äldre bestämmelser och det finns sådana omständigheter som avses i 1 § 2 LSU bör tillstånd till hemlig dataavläsning kunna beviljas om Migrationsverket, regeringen eller en domstol har bestämt att reglerna om tvångsmedel och hemlig dataavläsning ska tillämpas på utlänningen (jfr 11 a, 14 och 15 §§ LSU).

Det förfarande och de förutsättningar som gäller för ett beslut om att tvångsmedel enligt 19–22 §§ LSU ska tillämpas i fråga om utlänningen bör gälla också för ett beslut om hemlig dataavläsning.

En upplysning om att rätten kan bevilja Säkerhetspolisen eller Polismyndigheten tillstånd till hemlig dataavläsning bör tas in i lagen om särskild utlänningskontroll.

Det bör ställas höga krav på när åtgärden ska få användas. Åtgärden bör, precis som enligt lagen om särskild utlänningskontroll, förbehållas utredningar om potentiella terroristbrott. Regeringen anser därför att ett tillstånd till hemlig dataavläsning i LSU-fallen bör få beviljas endast om det finns synnerliga skäl och det är av betydelse för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott. Utredningen om utlänningsärenden med säkerhetsaspek-

ter (Ju 2018:08) har i uppdrag att göra en sådan översyn som *Migrationsverket* efterfrågar. Utredningen ska redovisa sitt uppdrag senast den 31 mars 2020.

10.2.5 Kopplingen mellan en enskild och ett informationssystem vid särskild utlänningskontroll

Regeringens förslag: Hemlig dataavläsning ska vid särskild utlänningskontroll få avse avläsning eller upptagning av uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som kan bli föremål för hemliga tvångsmedel vid särskild utlänningskontroll.

Hemlig dataavläsning ska också få avse avläsning eller upptagning av uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna kommenterar inte förslaget.

Skälen för regeringens förslag: I lagen om särskild utlänningskontroll finns inget uttryckligt krav på koppling mellan person och det telefonnummer, adress eller kommunikationsutrustning som de hemliga tvångsmedlen ska användas för att avlyssna eller övervaka. Hänvisningen i 20 § LSU till 27 kap. RB innebär dock att tvångsmedelsanvändningen ska följa samma systematik och är underkastad samma krav som tvångsmedelsanvändningen enligt rättegångsbalken, där krav på en sådan koppling finns. Eftersom hemlig dataavläsning så långt som möjligt bör anpassas till det bakomliggande tvångsmedlet bör samma förutsättningar som gäller enligt lagen om särskild utlänningskontroll gälla även när hemlig dataavläsning används i sådana fall. Det innebär således att hemlig dataavläsning bör få avse uppgifter i ett avläsningsbart informationssystem som används av eller det finns särskild anledning att anta har använts eller kommer att användas av person som kan bli föremål för hemliga tvångsmedel enligt lagen om särskild utlänningskontroll. Om det är fråga om ett annat informationssystem än som nu sagts bör det krävas att uppgifterna finns i ett informationssystem som det finns synnerlig anledning att anta att en sådan person har kontaktat eller kommer att kontakta.

För att åstadkomma enlighet med gällande bestämmelser bör det också föras in en möjlighet att bevilja tillstånd till hemlig dataavläsning för att läsa av eller ta upp uppgifter i ett avläsningsbart informationssystem det finns synnerlig anledning att anta att utlänningen, under den tid som tillståndet avser, har kontaktat eller avser att kontakta. Sådan möjlighet finns i lagen om särskild utlänningskontroll (jfr 20 § och 27 kap. rättegångsbalken). Även utredningen föreslår en sådan möjlighet – dock anser regeringen, till skillnad från utredningen, att det bör föras in en särskild bestämmelse som reglerar den situationen.

10.2.6 Hemlig dataavläsning i inhämtningslagsfallen

Regeringens förslag: Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter ska få beviljas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som anges i inhämtningslagen. Vid sådan hemlig dataavläsning ska meddelanden inte få hindras att nå fram. Ett tillstånd till hemlig dataavläsning för kommunikationsövervakningsuppgifter ska endast få avse uppgifter i förfluten tid.

Regeringens bedömning: Det behöver inte anges att en åtgärd för att förebygga, förhindra eller upptäcka brottslig verksamhet inte får avse ett avläsningsbart informationssystem som tillhör någon som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att hemlig dataavläsning för att förebygga, förhindra eller upptäcka brottslig verksamhet inte får avse ett informationssystem som tillhör någon som tillhandahåller elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget eller lämnar det utan invändning. *Polismyndigheten* och *Säkerhetspolisen* är kritiska till kravet på att åtgärden ska vara av synnerlig vikt för att förebygga, förhindra eller upptäcka den brottsliga verksamheten och anser att kravet bör vara detsamma som enligt inhämtningslagen, nämligen särskild vikt. *Ekobrottsmyndigheten* konstaterar att hemlig dataavläsning inte kommer att kunna användas i myndighetens underrättelseverksamhet och påtalar vikten av att det införs en straffvärdeventil i inhämtningslagen för att det ska bli möjligt. *Säkerhets- och integritetsskyddsnämnden* och *Civil Rights Defenders* avstyrker förslaget eftersom det saknar krav på koppling mellan informationssystemet och den enskilde. Nämnden anser att den bakomliggande regleringen i inhämtningslagen, som förvisso inte heller ställer krav på en sådan koppling, inte utan närmare analys kan läggas till grund för i vilka situationer hemlig dataavläsning ska få användas.

Skälen för regeringens förslag och bedömning: I inhämtningslagen regleras vilka uppgifter som de brottsbekämpande myndigheterna får hämta in från telekomoperatörer. Uppgifter som får hämtas in enligt inhämtningslagen (inhämtningslagsfallen) är samma sorts uppgifter som får hämtas in efter beslut om hemlig övervakning av elektronisk kommunikation under förundersökning för att utreda vem som skäligen kan misstänkas för brottet.

Inhämtningslagen uppställer som krav 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 får också ske om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar även viss annan i lagen uppräknad samhällsfarlig brottslighet, vars straffskalor föreskriver lindrigare straff än två års fängelse.

Regeringen gör i avsnitt 10.2.1 bedömningen att hemlig dataavläsning bör få användas i underrättelseverksamhet. Sådana uppgifter som faller

inom tillämpningsområdet för inhämtningslagen är inget undantag. Regeringen anser, i likhet med utredningen, att hemlig dataavläsning därför bör få användas för att hämta in sådana uppgifter. Eftersom kraven för hemlig dataavläsning enligt regeringen ska motsvara kraven för tillstånd för det bakomliggande tvångsmedlet, bör hemlig dataavläsning i inhämtningslagsfallen endast få avse avläsning eller upptagning av historiska kommunikationsövervakningsuppgifter och platsuppgifter, såväl historiska som realtidsuppgifter. Hemlig dataavläsning bör vidare endast få vidtas för sådant ändamål som anges i inhämtningslagen, dvs. för att förebygga, förhindra eller upptäcka viss allvarlig och samhällsfarlig brottslig verksamhet. Hemlig dataavläsning bör vidare följa samma systematik som inhämtningslagen varför det inte, som *Säkerhets- och integritetsskyddsnämnden* och *Civil Rights Defenders* anser, bör krävas en koppling mellan en enskild och ett informationssystem (se vidare nästa avsnitt).

Det bör krävas att åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka den brottsliga verksamheten. Liksom utredningen anser regeringen att det är lämpligt att införa detta strängare krav när hemlig dataavläsning ska användas i inhämtningslagsfallen, framför allt med hänsyn till att det kravet föreslås för hemlig dataavläsning i övrigt. Regeringen gör därmed en annan bedömning än *Polismyndigheten* och *Säkerhetspolisen*.

Regeringen ifrågasätter inte att en sådan ändring i inhämtningslagen som *Ekobrottsmyndigheten* efterfrågar, dvs. en straffvärdeventil, skulle kunna effektivisera myndighetens arbete i vissa underrättelsefall. Det finns dock en svårighet med en straffvärdeventil i underrättelseverksamhet eftersom det är svårt att bedöma straffvärdet av den brottsliga verksamheten i ett så tidigt skede. I vart fall är det en fråga som behöver ses över i ett större sammanhang och kan inte hanteras inom ramen för detta lagstiftningsarbete.

Slutligen bedömer regeringen, till skillnad från utredningen, att det inte behövs en bestämmelse om att hemlig dataavläsning ska vara förbjuden gentemot ett informationssystem som tillhör någon som tillhandahåller elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Övervägandena i denna del är desamma som redogörs för i avsnitt 10.1.5.

10.2.7 Kopplingen mellan en enskild och ett informationssystem i inhämtningslagsfallen

Regeringens bedömning: Det behövs inte några regler om koppling mellan den enskilde och det avläsningsbara informationssystem som hemlig dataavläsning ska avse i inhämtningslagsfallen.

Utredningens bedömning överensstämmer i huvudsak med regeringens. Utredningen lämnar dock inte någon uttrycklig bedömning i frågan.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte frågan. *Civil Rights Defenders* anser att det måste ställas ett krav på koppling mellan informationssystem och person för att Sverige ska anses

leva upp till sina internationella åtaganden. *Säkerhets- och integritetsskyddsnämnden* har liknande synpunkter.

Skälen för regeringens bedömning: Det finns inte några krav på att ett tvångsmedel enligt inhämtningslagen ska rikta sig mot en viss person. Det innebär att tvångsmedlet i princip kan riktas mot vem som helst, även personer utan anknytning till den brottsliga verksamheten (Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas?, 4 uppl. 2018 s. 753).

Regeringen bedömer mot den bakgrunden att det för hemlig dataavläsning inte heller bör införas ett uttryckligt krav på en koppling mellan informationssystemet och en enskild person. På samma sätt som övriga tvångsmedel i inhämtningslagen riskerar en sådan koppling att försvåra underrättelsearbetet väsentligt (prop. 2011/12:55 s. 84). Regeringen instämmer därför inte i den synpunkt som framförs av *Säkerhets- och integritetsskyddsnämnden* och *Civil Rights Defenders*. Vid tillståndsprövningen av hemlig dataavläsning i inhämtningslagsfallen sätter proportionalitetsbedömningen gränser för vilka uppgifter som får hämtas in och om inhämtning över huvud taget får äga rum.

10.3 Förbud mot hemlig dataavläsning

10.3.1 Gällande rätt om förbud mot användningen av hemliga tvångsmedel

Vissa yrkeskategorier bedriver verksamhet som omfattas av tystnadsplikt. Tystnadsplikten hindrar i många fall personerna i verksamheten från att vittna i en rättegång om angelägenheter som anförtrotts dem i deras yrkesutövning (36 kap. 5 § RB). Dessa bestämmelser har tillkommit av hänsyn till enskildas personliga integritet och privatliv eftersom det inte ansetts riktigt att yrkesgrupper som intar en förtroendeställning i förhållande till allmänheten ska behöva vittna mot en enskild. Den enskilde ska, utom när det är fråga om mycket allvarliga brott, och i vissa fall även då, kunna anförtro sig till vissa särskilda personer utan rädsla för att samtalet eller de uppgifter som lämnas kan komma att användas mot honom eller henne (se t.ex. Processlagsberedningens förslag till rättegångsbalk, SOU 1938:44 s. 39–40). Bestämmelserna begränsar möjligheten att inför domstol ställa frågor till ett vittne, och brukar därför beskrivas som frågeförbud. Det finns också regler som förbjuder användningen av hemlig rumsavlyssning i lokaler som används för viss verksamhet (27 kap. 20 e § tredje stycket RB). Förbudet mot hemlig rumsavlyssning gäller på följande platser:

1. en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet som tystnadsplikt gäller för enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen
2. en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453)

3. en plats som stadigvarande används eller är särskilt avsedd att användas av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, för bikt eller enskild själavård.

Det finns även särskilda regler om avlyssningsförbud för både hemlig avlyssning av elektronisk kommunikation och för rumsavlyssning (27 kap. 22 § RB och 11 § preventivlagen). Bestämmelserna är utformade så att avlyssning inte får avse samtal, annat tal eller meddelanden där någon som yttrar sig är undantagen från vittnesplikt enligt frågeförbudet.

I rättegångsbalken finns också skydd för uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § RB inte får höras som vittne om (27 kap. 2 § första stycket RB). Detta innebär förbud mot att ta en skriftlig handling i beslag om den kan antas innehålla sådana uppgifter och innehas av antingen en person som avses i 36 kap. 5 § RB eller av den som tystnadsplikten gäller till förmån för. Högsta domstolen har slagit fast att beslagsförbudet är ett informationsskydd som gäller oavsett informationsbärare och således inte enbart för information på ett papper (NJA 2015 s. 631 p. 25 och 26).

10.3.2 Hemlig dataavläsning får aldrig avse vissa avläsningsbara informationssystem eller vissa platser

Regeringens förslag: Ett tillstånd till hemlig dataavläsning ska inte få avse ett avläsningsbart informationssystem som stadigvarande används eller är särskilt avsett att användas

1. i verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen och 2 kap. 3 § yttrandefrihetsgrundlagen,
2. i verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare, eller
3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, i verksamhet för bikt eller enskild själavård.

Hemlig dataavläsning som gäller rumsavlyssningsuppgifter ska inte få avse en plats som stadigvarande används eller är särskilt avsedd att användas för sådan verksamhet som avses ovan.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Sveriges advokatsamfund*, *Svenska kyrkan* och *Sveriges kristna råd* anför att tystnadsplikten är en mycket viktig del i deras respektive verksamheter och att det behövs regler som respekterar detta. Svenska kyrkan anser dock att det kan uppstå tillämpningssvårigheter för kravet på att informationssystemet ska användas stadigvarande och anser att detta borde belysas närmare. Även *Svenska Journalistförbundet* välkomnar förslaget i denna del men anser att det finns en risk att frilansande journalister inte omfattas av förbudet eftersom det är svårt att avgöra om ett informationssystem som inte ingår i en redaktion används stadigvarande för journalistisk verksamhet. Svenska Journalistförbundet

anser därför att informationssystem som används av journalister i deras yrkesmässiga verksamhet bör undantas helt från ingrepp i form av hemlig dataavläsning. *Sveriges läkarförbund* anser att begreppet verksamhet som bedrivs av läkare ska tolkas så att det avser samtliga verksamheter där läkarverksamhet bedrivs och inte endast sådana som ägs av läkare. Dessutom anser förbundet att det bör förtydligas huruvida en wifi-uppkoppling för besökare och besöksdatorer omfattas av förbudet endast av den anledningen att de finns tillgängliga finns i lokalen. *Civil Rights Defenders* anser att förbudet mot hemlig dataavläsning även bör omfatta uppgifter i ett informationssystem som tillhör personer som nämns i 36 kap. 5 § första stycket RB (dvs. personer som omfattas av bl.a. försvarssekretess) då det annars riskerar att undergräva dessa personers integritetsskydd. *Säkerhets- och integritetsskyddsnämnden* påpekar att förbudet mot hemlig dataavläsning enligt utredningens förslag även träffar avläsning av uppgifter som kan inhämtas genom hemlig övervakning av elektronisk kommunikation, vilket regleringen i 27 kap. 22 § RB inte gör.

Skälen för regeringens förslag: Verkställighet av hemlig dataavläsning innebär användning av tekniker som skulle kunna ge tillgång till alla uppgifter som finns i ett visst avläsningsbart informationssystem. I informationssystem som används av t.ex. advokater, präster, läkare och journalister finns det en mängd känsliga uppgifter som är så skyddsvärda att sekretessen kring dem bör få företräde framför det brottsbekämpande intresset. Det finns behov av ett starkt skydd så att denna information inte kan spridas vidare till obehöriga. Därför bör det, som utredningen föreslår, införas ett förbud mot hemlig dataavläsning för informationssystem i sådana verksamheter. Förbudet bör gälla för alla uppgiftstyper. Det kan noteras att detta är ett avsteg från vad som gäller vid hemlig övervakning av elektronisk kommunikation enligt rättegångsbalken, vilket *Säkerhets- och integritetsskyddsnämnden* påpekar. Regeringen bedömer dock, med hänsyn till integritetsintrånget i själva verkställighetstekniken, att det finns skäl att reglera förbudet mot att läsa av eller ta upp de olika uppgiftstyperna från de aktuella informationssystemen på samma sätt, varför även kommunikationsövervakningsuppgifter bör omfattas av förbudet. Även proportionalitetsbedömningen kan sätta gränser för om det är tillåtet med hemlig dataavläsning för att läsa av uppgifter när det inte står helt klart att informationssystemet stadigvarande används i vissa skyddade verksamheter.

Förbudet bör utformas med regeln om förbud mot hemlig rumsavlyssning beträffande vissa platser som förebild (27 kap. 20 e § tredje stycket RB) och omfatta samma verksamheter som nämns där. I stället för en viss plats bör dock förbudet mot hemlig dataavläsning ta sikte på ett visst informationssystem.

Förbudet vid hemlig rumsavlyssning omfattar inte alla verksamheter som kan omfattas av frågeförbudet i 36 kap. 5 § RB. Det omfattar nämligen inte sådana personer som i paragrafens första stycke med hänsyn till t.ex. försvarssekretess och statsfinanssekretess inte får höras som vittne utan att berörd myndighet har gett sitt tillstånd. Detta frågeförbud fyller emellertid andra syften än det frågeförbud som även hindrar hemlig rumsavlyssning. Frågeförbudet i 36 kap. 5 § första stycket är nämligen uppställt till skydd för huvudsakligen statliga angelägenheter medan frågeförbudet i andra–sjunde styckena är uppställt till skydd för huvudsakligen enskilda.

Omfattningen av förbudet för hemlig dataavläsning bör ha samma omfattning som det för hemlig rumsavlyssning i 27 kap. 20 e § RB. Dock torde proportionalitetsprövningen i vissa fall hindra hemlig dataavläsning i informationssystem som innehåller information som skyddas av den sekretess som nämns i 36 kap. 5 § första stycket RB. Det finns mot bakgrund av det angivna inte anledning att, som *Civil Rights Defenders* föreslår, införa ett uttryckligt förbud mot hemlig dataavläsning även för sådan verksamhet som skyddas enligt 36 kap. 5 § första stycket RB. Se dock nedan om förslaget att en avläsning som omfattar sådana uppgifter genast ska avbrytas (avsnitt 10.3.3).

För att förbudet mot hemlig dataavläsning ska gälla och stämma överens med motsvarande förbud mot hemlig rumsavlyssning bör det krävas att informationssystemet stadigvarande används i sådan verksamhet där tystnadsplikt råder. Informationssystemet ska alltså vara beständigt och användas för något av verksamhetens syften. Det kan t.ex. röra sig om system för klientinformation i advokatverksamhet, system för journalföring på sjukhus eller samtalsanteckningar hos en psykolog. Syftet är inte, som *Sveriges läkarförbund* önskar ett förtydligande av, att skydda avläsning eller upptagning av informationssystem bara för att de ägs av någon som bedriver i och för sig skyddad verksamhet. Det innebär alltså att t.ex. besöksdatorer i en skyddad verksamhet, som inte kan sägas användas för ett sådant syfte som förbudet tar sikte på, inte omfattas av förbudet. Genom ett krav på att informationssystemet stadigvarande ska användas i den skyddade verksamheten torde risken för missbruk, t.ex. att kriminella kan anpassa sig efter undantaget i lagstiftningen, minska.

Frågan om ett informationssystem som används utanför en tidningsredaktion ska omfattas av förbud mot avläsning och upptagning – en frågeställning som *Svenska Journalistförbundet* aktualiserar – behandlades vid införandet av hemlig avlyssning av elektronisk kommunikation. Lagrådet påpekade i det sammanhanget att begreppet stadigvarande behandling inte behöver vara begränsad till att avse ett medieföretags redaktion utan kan omfatta också t.ex. en arbetsplats i en journalists hem, vilket regeringen instämde i (prop. 2013/14:237 s. 180). Motsvarande bör gälla även vid hemlig dataavläsning. Den fysiska arbetsplatsen är således inte avgörande för om informationssystemet kan bli föremål för hemlig dataavläsning. Inte heller är platsen av betydelse om det avläsningsbara informationssystemet befinner sig utanför arbetsplatsen. Det avgörande är huruvida informationssystemet stadigvarande används för vissa fredade verksamheter.

Det föreslagna förbudet mot hemlig dataavläsning i informationssystem som används i vissa skyddade verksamheter bör även gälla vid avläsning av rumsavlyssningsuppgifter för platser som stadigvarande används i sådana verksamheter. Därmed uppnås överensstämmelse med vad som gäller för hemlig rumsavlyssning (27 kap. 20 e § tredje stycket RB). För sådana platser får inte heller tillträdestillstånd ges (se avsnitt 10.4).

När det gäller det föreslagna förbudet mot hemlig dataavläsning avseende präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund samt i verksamhet för bikt eller enskild själavård är det självklart att det bör omfatta informationssystem som används i verksamhet som bedrivs i t.ex. kyrkor, synagogor och moskéer. Mer komplicerat blir det när en helt vanlig lokal med inga eller mycket få religiösa inslag

påstås användas för t.ex. själavård. Det kan till och med vara så att kriminella försöker freda platser från hemlig dataavläsning genom att påstå att de används i verksamhet för själavård. På en sådan plats bör inte förbudet mot hemlig dataavläsning gälla. Dessutom bör det fredade utrymmet endast vara det begränsade utrymme som är direkt avsett för bikt eller själavård. Det förhållandet att en präst kan hålla ett själavårdande samtal i en kyrkbänk bör inte innebära att platsen är fredad från hemlig dataavläsning. Däremot bör, som Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel konstaterat, självfallet aldrig ett biktbås eller ett rum särskilt inrättat för själavård kunna bli föremål för hemlig dataavläsning (jfr betänkandet Rättssäkerhetsgarantier och hemliga tvångsmedel, SOU 2018:61 s. 166). Samtidigt måste framhållas att även om en viss plats inte är fredad från hemlig dataavläsning så föreslår regeringen en skyldighet att omedelbart avbryta verkställigheten och förstöra upptagningarna om det framkommer uppgifter som är skyddade enligt 27 kap. 2 § första stycket RB, t.ex. uppgifter från bikt eller själavård (avsnitt 10.3.3). Ytterst blir det en fråga vid tillståndsprövningen och verkställigheten i varje enskilt fall att bedöma om hemlig dataavläsning bör utföras på den aktuella platsen eller om den innehar en skyddad ställning.

10.3.3 Förbud mot avläsning och upptagning av uppgifter som omfattas av beslagsförbudet

Regeringens förslag: Hemlig dataavläsning som avser uppgifter som finns lagrade i ett avläsningsbart informationssystem eller uppgifter om hur ett avläsningsbart informationssystem används ska inte få avse uppgifter som enligt 27 kap. 2 § första stycket RB hindrar beslag. Om det under verkställigheten kommer fram sådana uppgifter ska verkställigheten omedelbart avbrytas och upptagningarna och uppteckningarna omedelbart förstöras i de delar som omfattas av förbudet.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna tillstyrker förslaget eller lämnar det utan invändning.

Civil Rights Defenders anser att det i enlighet med EU:s rättighetsstadga och Europakonventionen behövs en bestämmelse om att de brottsbekämpande myndigheterna ska underrätta Säkerhets- och integritetsskyddsnämnden om uppgifter som omfattas av beslagsförbudet ändå läses av eller tas upp.

Skälen för regeringens förslag: Hemlig dataavläsning föreslås få användas för att läsa av eller ta upp lagrade uppgifter och uppgifter som visar hur ett avläsningsbart informationssystem används. Det kan förekomma att sådana uppgifter skulle ha omfattats av det s.k. beslagsförbudet (27 kap. 2 § första stycket RB). Enligt förbudet får en skriftlig handling inte tas i beslag om den kan antas innehålla uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § RB inte får höras som vittne om, och handlingen innehas av honom eller henne eller av den som tystnadsplikten gäller till förmån för. Som framgår av avsnitt 10.3.1 har Högsta domstolen slagit fast att det är själva uppgifterna som ska skyddas och inte den fysiska handlingen som sådan. Skyddet omfattar därför inte

bara uppgifter i skriftliga handlingar utan gäller alla uppgifter oavsett vilken informationsbärare dessa är präglade på (NJA 2015 s. 631). Det kan t.ex. förekomma att det vid hemlig avläsning upptäcks ett lagrat eller ännu inte lagrat brev till en advokat eller läkare, vilket inte får tas i beslag.

Skyddet bör vara detsamma vid hemlig dataavläsning som det hade varit vid ett beslag där uppgifterna förekommer, vilket innebär att om uppgifter som är skyddade av beslagsförbudet har lästs av eller tagits upp så ska verkställigheten avbrytas och upptagningen förstöras i de delar de är skyddade. Eftersom handlingar, och inte uppgifter, tas i beslag, bör bestämmelsen formuleras något annorlunda än utredningen föreslår.

Bestämmelsen bör gälla under pågående verkställighet. Det är den verkställande myndigheten som har att kontrollera att den efterlevs. I dagsläget finns det inte någon skyldighet att underrätta Säkerhets- och integritetsskyddsnämnden om beslagsförbudet skulle överträdas. Regeringen föreslår dock en reglering om underrättelseskyldighet till nämnden avseende själva beslutet om hemlig dataavläsning liksom om det förekommer otillåten tilläggsinformation (se vidare avsnitt 11.1.1 och 11.2.2). Genom dessa åtgärder uppfyller regleringen om hemlig dataavläsning de krav som *Civil Rights Defenders* efterfrågar. Någon ytterligare underrättelseskyldighet till nämnden är därmed inte nödvändig.

I 27 kap. 2 § andra stycket finns ytterligare bestämmelser om beslagsförbud, nämligen förbud mot att ta skriftligt meddelande mellan en misstänkt och en till denne närstående i beslag. Ett skriftligt meddelande får i sådana fall tas i beslag hos den misstänkte eller en närstående endast vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, vissa i bestämmelsen särskilt angivna brott eller försök, förberedelse eller stämpling till sådana brott. De angiva trösklarna för när beslagförbudet avseende meddelanden mellan närstående genombryts är samma som föreslås för att bevilja hemlig dataavläsning, förutom när det gäller möjligheten att bevilja hemlig dataavläsning genom den s.k. straffvärdeventilen (dvs. att brottet i det enskilda fallet kan antas ha ett straffvärde som överstiger två år, se avsnitt 10.1.2). Detta innebär att i förundersökningar om brott som inte är särskilt angivna och har ett lägre föreskrivet minimistraff än fängelse i två år finns det ett förbud mot beslag av skriftliga meddelanden mellan en misstänkt och en närstående, även om straffvärdet i det enskilda fallet bedöms överstiga två års fängelse. Frågan är om det bör införas ett förbud att genom hemlig dataavläsning läsa av eller ta upp sådana uppgifter. Utredningen lämnar inget sådant förslag. Ingen remissinstans uttalar sig i frågan. Inte heller regeringen ser tillräckliga skäl till ett sådant förbud. Det kommer nämligen endast i undantagsfall att bli aktuellt att läsa av eller ta upp uppgifter mellan närstående i en utredning där hemlig dataavläsning har aktiverats genom straffvärdeventilen (t.ex. grov misshandel) och vid så höga straffvärden är det rimligt att det brottsbekämpande intresset väger tyngre än de skäl som bär upp beslagsförbudet. Regleringen blir härmed i överensstämmelse med vad som gäller för hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och i viss mån hemlig rumsavlyssning (27 kap. 18, 20 a och 20 d §§ RB).

I sammanhanget bör noteras att en ändring av vissa av reglerna om beslagsförbud, genom Beslagsutredningens betänkande Beslag och husrannsakan – ett regelverk för dagens behov, är föremål för överväganden inom Regeringskansliet (SOU 2017:100).

10.3.4 Förbud mot avläsning och upptagning av vissa samtal och meddelanden

Regeringens förslag: Hemlig dataavläsning av kommunikationsavlyssnings- och rumsavlyssningsuppgifter ska inte få avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig inte skulle ha kunnat höras som vittne, på grund av tystnadsplikt enligt 36 kap. 5 § andra–sjätte styckena RB, om det som har sagts eller på annat sätt kommit fram. Om det under verkställigheten kommer fram sådana uppgifter ska verkställigheten omedelbart avbrytas och upptagningar och uppteckningar omedelbart förstöras i de delar som de omfattas av förbudet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Förutom *Åklagarmyndigheten* och *Ekobrottsmyndigheten*, som tillstyrker förslaget, kommenterar inte remissinstanserna förslaget. *Civil Rights Defenders* anser dock att det i enlighet med EU:s rättighetsstadga och Europakonventionen behövs en bestämmelse om att de brottsbekämpande myndigheterna ska underrätta Säkerhets- och integritetsskyddsnämnden om uppgifter som skyddas av avlyssningsförbudet läses av eller tas upp.

Skälen för regeringens förslag: I både rättegångsbalken (27 kap. 22 §) och preventivlagen (11 §) finns det bestämmelser om s.k. avlyssningsförbud. Enligt dessa får avlyssning inte avse samtal, annat tal eller meddelanden där någon som yttrar sig är undantagen från vittnesplikt (enligt 36 kap. 5 § andra–sjätte styckena RB). Om det under avlyssningen framkommer att uppgifterna inte får avlyssnas ska avlyssningen omedelbart avbrytas. Detta innebär ett absolut förbud mot att avlyssna dels samtal där en försvarare deltar vid utövandet av sitt uppdrag, dels samtal som avser bikt eller enskild själavård om en präst eller annan själasörjare deltar i samtalet, dels samtal med personer som tillhör vissa andra yrkeskategorier, om samtalet har samband med deras yrkesutövning (t.ex. läkare, tandläkare, barnmorskor, sjuksköterskor och psykologer samt sådana personers biträden). I vissa avseenden omfattas även personer verksamma inom medieföretag, auktoriserade patentombud och deras biträden samt personer med anknytning till viss statistisk verksamhet.

Vid verkställighet av hemlig dataavläsning kan det komma fram uppgifter som omfattas av avlyssningsförbudet, nämligen kommunikationsavlyssnings- eller rumsavlyssningsuppgifter som avser samtal med t.ex. en advokat, läkare eller psykolog. Uppgifterna bör då omfattas av samma skydd som gäller för de bakomliggande tvångsmedlen. Det bör därför införas en bestämmelse som föreskriver ett sådant förbud.

Om skyddade uppgifter ändå läses av eller tas upp, ska verkställigheten omedelbart avbrytas och upptagningar eller uppteckningar förstöras i de delar de innehåller skyddad information. Liksom förbudet mot att läsa av

eller ta upp uppgifter som omfattas av beslagsförbudet (se föregående avsnitt) bör avläsningsförbudet gälla under pågående verkställighet, vilket innebär att den verkställande myndigheten ska kontrollera att det efterlevs.

Regeringen gör i denna del samma bedömning som tidigare avseende *Civil Rights Defenders* synpunkt om underrättelser till Säkerhets- och integritetsskyddsnämnden (avsnitt 10.3.3).

10.4 Tillträdestillstånd

Regeringens förslag: Vid hemlig dataavläsning ska den verkställande myndigheten, efter särskilt tillstånd, i hemlighet få skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd ska endast få avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller en person som är föremål för hemlig dataavläsning i preventivlags- eller LSU-fallen ska tillstånd få beviljas endast om det finns synnerlig anledning att anta att informationssystemet finns där.

Tillträdestillstånd ska inte få avse en plats som stadigvarande används eller är särskilt avsedd att användas

1. i verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen och 2 kap. 3 § yttrandefrihetsgrundlagen,
2. i verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare, eller
3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, vid bikt eller enskild själavård.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Remissutfallet är blandat. Av de remissinstanser som uttalar sig i frågan tillstyrker en majoritet förslaget. *Åklagarmyndigheten* är positiv till förslaget men anser att ett beslut om hemlig dataavläsning ska innebära ett generellt tillträde till vissa typer av platser som annars skyddas mot intrång, till exempel fordon och allmänna förvaringsutrymmen, men inte sådana platser som lagen föreslår har ett absolut förbud. Alternativt skulle åklagaren kunna besluta om tillträdestillstånd till sådana platser när tillfälle uppkommer. *Polismyndigheten* anser att det bör förtydligas om det behövs ett särskilt tillträdestillstånd för att på elektronisk väg bereda sig tillgång till informationssystemet eller om detta omfattas av grundtillståndet till hemlig dataavläsning. Polismyndigheten anser vidare att det finns en risk att regleringen om hemlig dataavläsning avseende kameraövervakningsuppgifter blir tandlös eftersom det kan vara straffbart att tränga in i någons bostad för att installera en dold övervakningskamera. Slutligen ställer myndigheten frågan om det kan vara straffbart att placera programvara i någons telefon eller dator om denna kommer till användning i någons hem. *Säkerhetspolisen* anför att det är viktigt att tillträdestillståndet inte ges en för snäv tolkning eller begränsad räckvidd. Det kan nämligen i vissa fall vara möjligt att installera ett tekniskt hjälpmedel på distans, till exempel via ett switchskåp i källaren

till ett flerbostadshus för att komma åt trafikflödet till en viss utrustning utan att göra fysiskt intrång i en lägenhet. Detta bör enligt Säkerhetspolisen ses som en mindre ingripande åtgärd än intrång i bostad.

Säkerhets- och integritetsskyddsnämnden avstyrker förslaget. Nämnden anser att förslaget utgör en oacceptabel utvidgning av området för hemlig tvångsmedelsanvändning eftersom liknande tillträdestillstånd endast får beviljas vid hemlig rumsavlyssning och förutsätter misstanke om mycket allvarliga och samhällsfarliga brott. Nämnden anser också att det är oklart hur långt ett tillträdestillstånd kan sträcka sig. Enligt förslaget skulle det exempelvis vara tillåtet att göra intrång på en plats för att rent fysiskt komma åt en dator och göra ingrepp i den. Detta skapar gränsdragningsproblem gentemot reglerna om husrannsakan. Även *Civil Rights Defenders* avstyrker förslaget och anför att det inte är förenligt med Europakonventionen.

Sveriges advokatsamfund anför att den föreslagna bestämmelsen om tillträdestillstånd är mycket integritetskränkande och att kravet på att det finns särskild anledning att anta att ett informationssystem finns på platsen för att sådant tillstånd ska ges är för vagt formulerad. Kravet bör därför skärpas ytterligare.

Skälen för regeringens förslag: Av dagens hemliga tvångsmedel är det endast hemlig rumsavlyssning som kan föranleda intrång i annars skyddade utrymmen för att i hemlighet och efter tillstånd installera tekniska hjälpmedel (27 kap. 25 a § RB). Om en plats blir föremål för både hemlig rumsavlyssning och hemlig kameraövervakning får ett särskilt tillstånd till intrång beviljas även för kameraövervakningen. Ett sådant tillstånd får dock inte avse tillträde för installation av tekniska hjälpmedel i någons stadigvarande bostad med hänsyn till det mycket betydande integritetsintrång det kan innebära med kameraövervakning i bostäder. Det största intrånget har dock ansetts utgöras av själva kameraövervakningen och inte av det fysiska intrånget (prop. 2013/14:237 s. 153–154). Även husrannsakan kan i vissa fall utföras utan att den som åtgärden riktas mot vet om detta. Underrättelse om åtgärden kan då vänta till dess den kan lämnas utan men för utredningen (28 kap. 7 § andra stycket RB).

Vid verkställighet av hemlig dataavläsning kommer det i vissa fall att vara nödvändigt för den som ska verkställa åtgärden att komma närmare informationssystemet eller ha det i sin fysiska besittning, t.ex. då hårdvara ska användas vid verkställighet eller när det inte är möjligt att på distans installera programvara. När det står klart var informationssystemet finns behöver den verkställande myndigheten få tillgång till det. Ett sätt att få tillgång till informationssystemet är att tillåta den brottsbekämpande myndigheten att få tillträde till utrymmen som annars är skyddade mot intrång, t.ex. enligt reglerna i 4 kap. brottsbalken. En möjlighet till tillträdestillstånd för hemlig dataavläsning utgör en utvidgning av möjligheterna till tillträdestillstånd eftersom det i dag endast är tillåtet vid hemlig rumsavlyssning. Åtgärden innebär dock på ett principiellt plan – när det gäller själva det tvångsvisa tillträdet till ett sådant utrymme som skyddas mot intrång – inte något ytterligare intrång än vad som redan är tillåtet vid en husrannsakan, vilken endast kräver anledning att anta att ett brott har begåtts på vilket fängelse kan följa, vilket är ett mycket lägre ställt krav än kravet för hemlig dataavläsning. Ett tillträdestillstånd för hemlig dataavläsning kan emellertid inte i övrigt jämföras med en husrannsakan

eftersom den förra åtgärden görs i hemlighet. Samtidigt är hemlig dataavläsning en metod som fordrar att hårdvara kan installeras. För att tvångsmedlet ska ha önskad effektivitet måste de brottsbekämpande myndigheterna emellanåt kunna få tillträdestillstånd till annars skyddade utrymmen. Regeringen anser därför, till skillnad från *Säkerhets- och integritetsskyddsnämnden, Civil Rights Defenders* och *Sveriges advokatsamfund*, att en möjlighet till tillträdestillstånd bör införas.

För tillstånd till hemlig rumsavlyssning gäller att åtgärden endast får avse en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig (27 kap. 20 e § andra stycket RB). Vid hemlig dataavläsning bör ett liknande uttryckssätt användas men i stället bör det krävas att det finns särskild anledning att anta att informationssystemet ska finnas på den plats som tillträdestillståndet avser. Det betyder att det ska finnas någon faktisk omständighet som med viss styrka talar för att informationssystemet kommer att finnas tillgängligt där i vart fall någon gång under tillståndstiden (jfr prop. 2005/06:178 s. 101). *Åklagarmyndigheten* är i och för sig positiv till bestämmelsen men tillägger att det under verkställighet av hemlig dataavläsning kan uppstå möjlighet till installation på platser som är lämpligare och mindre integritetskänsliga än den misstänktes hem. Dessa tillfällen kan dock vara svåra att förutse vid domstolens tillståndsprövning och ett särskilt tillträdestillstånd för dessa platser, exempelvis ett skåp i ett omklädningsrum, kanske inte hinner inte inhämtas innan tillfället går förlorat. Åklagarmyndigheten anser därför att ett beslut om hemlig dataavläsning bör innebära ett generellt tillstånd till tillträde till vissa typer av platser som annars skyddas mot intrång, till exempel fordon och allmänna förvaringsutrymmen. Den verkställande myndigheten borde därför, enligt Åklagarmyndigheten, ha ett generellt tillstånd att bereda sig tillträde till platser dit allmänheten har tillträde. Alternativt föreslår Åklagarmyndigheten att åklagaren ska kunna besluta om tillträdestillstånd till sådana platser när tillfälle uppkommer.

Kraven för tillträdestillstånd bör med hänsyn till de allvarliga integritetsintrånget vara så högt ställda att det inte bör finnas möjlighet till sådana generella tillstånd som *Åklagarmyndigheten* föreslår. Däremot föreslår regeringen, som framgår i avsnitt 11.1.4, att åklagare ska ha rätt att under vissa förutsättningar fatta intermistiska beslut. Ett sådant beslut ska även kunna avse tillträdestillstånd varför det, om tillfälle till verkställighet plötsligt uppkommer, kommer att finnas möjlighet att snabbt utverka ett interimistiskt tillträdestillstånd.

Hur tillståndet ska se ut och vilka ytor det ska omfatta i det enskilda fallet är en fråga för rätten vid tillståndsprövningen. I vissa fall kan, som *Säkerhetspolisen* anför, tillträde till en viss plats vara mindre integritetskränkande än tillstånd till en annan plats. Det följer då av proportionalitetsprincipen att en sådan plats ska väljas i första hand, vilket alltså gör att det tekniska hjälpmedlet t.ex. kan behöva installeras via ett switchskåp i källaren till ett flerbostadshus i stället för inne i en lägenhet.

Hemlig rumsavlyssning får äga rum i annan stadigvarande bostad än den misstänktes om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där (27 kap. 20 e § andra stycket RB). JO har uttalat att rekvisitet synnerlig anledning att anta, då i fråga om husrannsakan hos tredje man, bör tolkas så att det ska föreligga någon faktisk omständighet som påtagligt visar att man med fog kan förvänta sig något

(se t.ex. JO 1988/89 s. 68). Det bör ställas ytterst höga krav även vid tillträdestillstånd enligt lagen om hemlig dataavläsning när tillståndet ska avse någon annan stadigvarande bostad än en bostad där den misstänkte personen stadigvarande bor. Möjligheten bör dock inte uteslutas. Samma höga krav bör ställas vid hemlig dataavläsning som vid hemlig rumsavlyssning, dvs. det ska finns synnerlig anledning att anta att informationssystemet finns i bostaden.

Vid hemlig dataavläsning i preventivlagsfallen och LSU-fallen finns ingen misstänkt person. Även i dessa fall finns det behov av en möjlighet att läsa av eller ta upp uppgifter från ett informationssystem som finns i en bostad som tillhör någon annan än den som är föremål för åtgärden. I dessa fall bör samma höga krav gälla som nyss nämnts. Om det begärs tillträdestillstånd till en annan stadigvarande bostad än en som tillhör den person som är föremål för hemlig dataavläsning i dessa fall bör det alltså krävas synnerlig anledning att anta att informationssystemet finns i bostaden. För hemlig dataavläsning i inhämtningslagsfallen är det dock inte lämpligt med en reglering som gör skillnad på i vems bostad informationssystemet finns. Skälet till det är att inhämtning enligt inhämtningslagen inte har koppling till en viss person (avsnitt 10.2.7) och att det således är svårt att se hur beviströsklarna skulle kunna differentieras i olika personers bostäder.

Utredningen föreslår att det, på samma sätt som vid hemlig rumsavlyssning, inte bör finnas möjlighet till tillträdestillstånd för hemlig dataavläsning där det bedrivs verksamhet som skyddas av frågeförbudet (36 kap. 5 § andra–sjätte styckena RB). Ingen remissinstans invänder mot förslaget. Regeringen delar utredningens uppfattning.

Vad gäller frågan som *Polismyndigheten* lyfter om huruvida det behövs ett särskilt tillträdestillstånd för att på elektronisk väg göra intrång i ett informationssystem konstaterar regeringen att ett sådant intrång ligger i själva tvångsmedlets natur varför det inte behövs något särskilt tillstånd för åtgärden. Att installera en kamera i någons hem föreslås däremot inte vara tillåtet genom hemlig dataavläsning eftersom regleringen tar sikte på aktivering av en kamerafunktion i t.ex. en dator eller mobiltelefon och inte montering av en fast kamera (avsnitt 10.1.4). Polismyndigheten aktualiserar också frågan om det kan vara straffbart att installera programvara i ett informationssystem om det kommer till användning i någons hem. Regeringen vill här förtydliga att hemlig dataavläsning i någons hem är förbjudet endast såvitt avser avläsning eller upptagning av kameraövervakningsuppgifter. Ett program som läser av eller tar upp andra slags uppgifter omfattas inte av sådant förbud.

Säkerhets- och integritetsskyddsnämnden berör frågan om gränsdragningen mellan tillträdestillstånd och husrannsakan. Även om det är så att själva verkställigheten av både en husrannsakan och ett tillträdestillstånd i vissa fall kommer att gå till på samma sätt (intrång i en viss lokal) kommer ändamålen bakom respektive åtgärd att vara olika. En husrannsakan genomförs huvudsakligen för att eftersöka föremål som kan tas i beslag eller för att utröna omständigheter som kan vara av betydelse för utredningen om ett brott (28 kap. 1 § RB). Ett tillträdestillstånd verkställs för att installera tekniska hjälpmedel. Ett tillträdestillstånd får således inte utnyttjas för att samtidigt genomföra husrannsakan. På motsvarande sätt får de brottsbekämpande myndigheterna inte utnyttja en husrannsakan för

att vidta åtgärder som är hänförliga till hemlig dataavläsning, t.ex. installation av utrustning. Regeringen ser inte någon risk för gränsdragningsproblem.

11 Tillstånd och verkställighet

11.1 Tillståndsprövning

11.1.1 Domstolsprövning

Regeringens förslag: Frågor om hemlig dataavläsning ska prövas av rätten.

Frågor om hemlig dataavläsning under en förundersökning ska prövas av den domstol som pekas ut enligt rättegångsbalkens forumregler. Om förundersökningen avser samhällsfarlig brottslighet får frågan även prövas av Stockholms tingsrätt. Frågor om hemlig dataavläsning i underrättelseverksamhet eller vid särskild utlänningskontroll ska alltid prövas av Stockholms tingsrätt.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: De remissinstanser som yttrar sig i frågan, bl.a. *Justitiekanslern* och *Datainspektionen*, ställer sig positiva till att beslut om hemlig dataavläsning alltid prövas av domstol. *Sveriges advokatsamfund* är av samma uppfattning och anser att rättssäkerheten på så sätt stärks mer än om de verkställande myndigheterna får fatta egna tillståndsbeslut. Vad gäller beslut om hemlig dataavläsning i underrättelseverksamhet anför *Riksdagens ombudsmän (JO*) att en prövning i domstol är en viktig rättssäkerhetsgaranti, särskilt när det gäller ett tvångsmedel av så ingripande slag som hemlig dataavläsning, och att eventuella invändningar av principiellt slag mot den ordningen inte har den tyngden att förslaget i den delen inte bör genomföras.

Skälen för regeringens förslag: Frågor om hemliga tvångsmedel under förundersökning prövas av rätten på ansökan av åklagaren (27 kap. 21 § första stycket RB). Domstolsförfarandet vid hemliga tvångsmedel avseende ansökan, prövning och tillståndsgivning har utvärderats och i allt väsentligt ansetts fungera väl, och dessutom ansetts tillgodose de krav som uppställs enligt både regeringsformen och Europakonventionen (se t.ex. prop. 2013/14:237 s. 117).

Utredningen föreslår att tillstånd till hemlig dataavläsning ska ges av domstol, såväl under en förundersökning som i underrättelseverksamhet, med hänsyn framför allt till åtgärdens ingripande karaktär.

Det finns enligt regeringen ingen anledning att avvika från ordningen med ett krav på föregående domstolsprövning för användning hemliga tvångsmedel i förundersökningsverksamhet. Ett sådant krav bör därför införas.

Utanför en förundersökning är situationen delvis annorlunda. Tillstånd till hemliga tvångsmedel enligt lagen om särskild utlänningskontroll och preventivlagen kräver domstolsprövning. Det ställs dock inte krav på

föregående domstolsprövning vid tvångsmedelsanvändning enligt inhämtningslagen. I stället fattas beslutet av åklagare på ansökan av den brottsbekämpande myndigheten (Polismyndigheten, Säkerhetspolisen eller Tullverket). Som skäl för att åklagare – och inte domstol – ska fatta dessa beslut anfördes i förarbetena bl.a. att det är principiellt tveksamt att de allmänna domstolarna prövar olika åtgärder som vidtas inom ramen för underrättelseverksamhet och att domstolarnas möjlighet att fatta de snabba beslut som kan behövas i underrättelseverksamhet är begränsad med hänsyn till att det saknas tillräcklig jourberedskap, se propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten (prop. 2018/19:86 s. 70–78).

Även i detta sammanhang har regeringen i och för sig samma principiella betänkligheter mot att involvera domstolar i underrättelseverksamhet. De remissinstanser som yttrar sig i frågan, bl.a. *Justitiekanslern* och *Riksdagens ombudsmän (JO*), förordar dock i likhet med utredningen en domstolsprövning. Vid bedömningen av vilken myndighet som bör anförtros beslutsbehörigheten vid hemlig dataavläsning bör vägas in att hemlig dataavläsning skiljer sig från inhämtning enligt inhämtningslagen på så sätt att hemlig dataavläsning, i vart fall vid verkställigheten, är ett mer ingripande tvångsmedel. Även om syftet med tvångsmedlen är detsamma kan hemlig dataavläsning dessutom ge mer exakta uppgifter om lokalisering än uppgifter enligt inhämtningslagen. Detta talar enligt regeringen för att domstolar är mer lämpade att fatta besluten. Dessutom framstår det som olämpligt att ha olika beslutsmyndigheter för ett och samma tvångsmedel. Regeringen instämmer i utredningens förslag i denna del.

När det gäller vilken domstol som ska pröva en ansökan om hemlig dataavläsning finns det en redan etablerad ordning för de nuvarande hemliga tvångsmedlen. Under förundersökning gäller reglerna i rättegångsbalken om laga domstol i brottmål. Som huvudregel är rätten i den ort där brottet begicks behörig. Om det är lämpligt, får prövningen i stället göras där den misstänkte har hemvist eller mera varaktigt uppehåller sig. I vissa brådskande fall får frågor om hemliga tvångsmedel prövas även av domstol på annan ort. Vid sådana samhällsfarliga brott som anges i 27 kap. 2 § andra stycket 2–8 RB får prövningen också göras av Stockholms tingsrätt (27 kap. 34 § RB). Det kan, precis som ordningen redan nu tillåter, finnas särskilda behov av Stockholms tingsrätt som ett alternativt forum. Skälen är främst praktiska och uppstår vid brott som faller inom ramen för Säkerhetspolisens verksamhet. Ingen remissinstans invänder mot förslaget. Regeringen föreslår därför, i likhet med utredningen, att samma forumregler som gäller för befintliga hemliga tvångsmedel bör gälla för hemlig dataavläsning under en förundersökning.

Stockholms tingsrätt är exklusivt forum för hemliga tvångsmedel enligt preventivlagen. Skälen som motiverar detta, att få en sammantagen mer praktisk och rättssäker hantering av ärendena, gör sig gällande även beträffande hemlig dataavläsning (prop. 2013/14:237 s. 162–163). Ingen remissinstans invänder mot förslaget och regeringen föreslår därför, i likhet med utredningen, att Stockholms tingsrätt ska vara exklusivt forum för frågor om hemlig dataavläsning i underrättelseverksamhet.

Stockholms tingsrätt är även exklusivt forum vid handläggning av frågor som rör hemliga tvångsmedel enligt lagen om särskild utlänningskontroll

(14 § andra stycket lagen om särskild utlänningskontroll). Det bör gälla även vid hemlig dataavläsning.

11.1.2 Vem ska ansöka om tillstånd?

Regeringens förslag: Frågor om hemlig dataavläsning ska prövas på ansökan av åklagare. En ansökan om hemlig dataavläsning vid särskild utlänningskontroll ska dock göras av Säkerhetspolisen eller Polismyndigheten.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna yttrar sig inte i denna del. *Polismyndigheten* och *Säkerhetspolisen* anser att det finns skäl att överväga om det är lämpligt att åklagare ska ansöka om tillstånd till hemlig dataavläsning i underrättelseverksamhet eftersom åklagare inte ägnar sig åt sådan verksamhet. Om åklagare ska ansöka i dessa fall anser Polismyndigheten att handläggningen bör skötas av ett begränsat antal särskilt utpekade åklagare som har tillräcklig utbildning och kunskap om underrättelseverksamhet.

Skälen för regeringens förslag: När en förundersökning pågår är det åklagaren som ansöker om tillstånd till hemliga tvångsmedel (27 kap. 21 § RB). Samma sak gäller för hemliga tvångsmedel enligt preventivlagen (6 §). När det däremot är fråga om hemliga tvångsmedel enligt lagen om särskild utlänningskontroll är det i stället Säkerhetspolisen eller Polismyndigheten som ska göra ansökan (21 § andra stycket).

Utredningen föreslår att åklagare ska ansöka om tillstånd till hemlig dataavläsning i förundersökningsverksamhet. Ingen remissinstans invänder mot förslaget. Förslaget stämmer väl överens med regleringen för befintliga tvångsmedel. Regeringen instämmer i utredningens förslag i den delen.

Utredningen föreslår vidare att åklagare ska ansöka om tillstånd till hemlig dataavläsning i underrättelseverksamhet, men inte vid särskild utlänningskontroll då ansökan föreslås göras av Säkerhetspolisen eller Polismyndigheten. Ingen remissinstans invänder mot förslaget att Säkerhetspolisen eller Polismyndigheten ska vara ansökande myndighet vid hemlig dataavläsning i samband med särskild utlänningskontroll. Regeringen instämmer i utredningens förslag. Utredningens förslag om att ansökan om hemlig dataavläsning i underrättelseverksamhet ska göras av åklagare ifrågasätts dock av *Polismyndigheten,* eftersom åklagare normalt sett inte ägnar sig åt underrättelseverksamhet. Det är visserligen så att åklagare typiskt sett inte tar befattning med underrättelseverksamhet. Det kan dock samtidigt konstateras att åklagare redan i dag har vissa uppgifter på underrättelseområdet då de har till uppgift att ansöka om hemliga tvångsmedel enligt preventivlagen och fatta beslut enligt inhämtningslagen. Regeringen gör mot denna bakgrund samma bedömning som utredningen och föreslår att åklagare ska göra ansökan i samtliga fall av hemlig dataavläsning förutom när det görs inom ramen för särskild utlänningskontroll. Det är, som Polismyndigheten påpekar, viktigt att hanteringen sköts av åklagare med tillräcklig kunskap inom ämnet. Som regeringen uttalade vid ändringen av beslutsordningen enligt inhämtningslagen kan

det finnas skäl att inom Åklagarmyndigheten inrätta en särskild organisation där ett begränsat antal åklagare involveras i verksamheten (prop. 2018/19:86 s. 75).

11.1.3 Offentliga ombud, sammanträde och förfarandet

Regeringens förslag: När en ansökan om hemlig dataavläsning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet ska den som gjort ansökan och det offentliga ombudet närvara.

För offentliga ombud i ärenden om hemlig dataavläsning ska samma regler gälla som gäller för offentliga ombud i ärenden om andra hemliga tvångsmedel.

På förfarandet enligt lagen om hemlig dataavläsning i övrigt tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte något annat anges i lagen. Handläggningen ska ske skyndsamt.

Utredningens förslag överensstämmer med regeringen.

Remissinstanserna: Majoriteten av remissinstanserna yttrar sig inte i frågan. *Domarnämnden* har inte någon invändning mot förslaget. *Civil Rights Defenders* anser att det är positivt och bidrar till förenlighet med EU:s rättighetsstadga och Europakonventionen att offentliga ombud utses och att sammanträde hålls.

Skälen för regeringens förslag: Offentliga ombud utses för att bevaka enskildas integritetsintressen i ärenden hos domstol om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning. Det offentliga ombudet ska inte företräda någon särskild misstänkt, eller någon annan särskild person, utan enskildas intressen i allmänhet. Den som agerar som offentligt ombud har rätt att ta del av det som förekommer i ärendet, yttra sig i ärendet och överklaga rättens beslut (27 kap. 26–30 §§ RB). När systemet med offentliga ombud infördes ansåg regeringen att genom det offentliga ombudets funktion kan den enskildes intressen bevakas och ärendet belysas mer allsidigt (prop. 2002/03:74 s. 22–23). Rättegångsbalkens bestämmelser bl.a. om när offentliga ombud ska förordnas gäller genom hänvisningar även för tvångsmedelsanvändningen enligt preventivlagen och lagen om särskild utlänningskontroll.

Det förordnas inte offentliga ombud inför prövning av ansökningar om hemlig övervakning av elektronisk kommunikation. När frågan har utretts har bl.a. nämnts att övervakning av elektronisk kommunikation inte är lika integritetskränkande som hemlig rumsavlyssning, hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning och att det finns ett värde i att ombudens medverkan koncentreras till dessa ärenden, där behovet av ombud är större (se SOU 2012:44 s. 672–674). Det finns inte heller något krav på offentligt ombud vid beslut om inhämtning enligt inhämtningslagen. Likaledes finns inget krav på offentliga ombud när hemlig övervakning av elektronisk kommunikation utförs inom ramen för tillämpning av preventivlagen (prop. 2013/14:237 s. 121–122).

Nuvarande regler om offentliga ombud har utvärderats och ansetts vara ändamålsenliga utifrån de syften som föranlett dem samt uppfylla regeringsformens och Europakonventionens krav på rättssäkerhetsgarantier vid hemliga tvångsmedel (SOU 2012:44 s. 666–677, prop. 2013/14:327 s. 119 och betänkandet Rättssäkerhetsgarantier och hemliga tvångsmedel, SOU 2018:61 s. 153–157).

Vid hemlig dataavläsning kan det potentiellt uppstå komplicerade avvägningar gällande bl.a. integritet och informationssäkerhet, oavsett åtgärd och uppgiftstyp som ska läsas av eller tas upp. Regeringen instämmer därför, i likhet med *Civil Rights Defenders,* i utredningens bedömning att det bör införas bestämmelser om att offentliga ombud ska förordnas i samtliga fall av hemlig dataavläsning, trots att det i vissa fall avviker från vad som gäller för bakomliggande tvångsmedel. De offentliga ombuden bör ha samma roll och regleras på samma sätt som vid övrig tvångsmedelsanvändning.

Eftersom offentliga ombud alltid ska närvara bör rätten hålla sammanträde till vilket aktörerna kallas. Det bör anges i lagen att det offentliga ombudet och den som gjort ansökan ska närvara vid sammanträdet. I övrigt anser regeringen, i likhet med utredningen, att hemlig dataavläsning såvitt avser regleringen av offentliga ombud och sammanträde bör överensstämma med rättegångsbalkens bestämmelser om befintliga hemliga tvångsmedel. I övrigt är det tillräckligt med hänvisningar till rättegångsbalkens regler om offentliga ombud och sammanträde.

Utredningen om regeländringar för vissa hemliga tvångsmedel har i april 2018 lämnat ett förslag om ett förenklat förfarande vid beslut om hemlig avlyssning (SOU 2018:30). Förslaget innebär att om rätten har beviljat tillstånd till hemlig avlyssning av elektronisk kommunikation får en ansökan eller anmälan om ytterligare tillstånd mot samma person och som grundas på samma omständigheter men avser ett annat telefonnummer, en annan adress eller en annan elektronisk kommunikationsutrustning prövas utan sammanträde och utan att offentligt ombud utsetts, om ett sammanträde skulle vara utan betydelse. Ett sådant tillstånd får inte avse annan tid som det tidigare tillståndet och när en sådan fråga har prövats ska rätten skyndsamt utse ett offentligt ombud och underrätta honom eller henne om beslutet. Förslaget bereds i Regeringskansliet.

På samma sätt som har gjorts i preventivlagen är det också tillräckligt att hänvisa till rättegångsbalkens regler om handläggningen vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor. Domstolens beslut om hemlig dataavläsning är, liksom domstolens beslut om befintliga hemliga tvångsmedel, ett slutligt beslut som kan överklagas enligt 49 kap. 3 § RB. Även villkor som inskränker användningen av hemlig dataavläsning bör kunna överklagas. På samma sätt bör det offentliga ombudet kunna överklaga ett tillståndsbeslut på den grunden att det inte är förenat med erforderliga villkor i syfte att förhindra onödigt intrång i enskildas integritet. Av 52 kap. 7 § tredje stycket RB framgår också att hovrätten kan inhibera verkställigheten vid ett överklagande. Det sagda överensstämmer med inte från vad som gäller för övriga hemliga tvångsmedel. Slutligen bör också, vilket även det gäller för övriga hemliga tvångsmedel, införas ett skyndsamhetskrav för handläggningen.

11.1.4 Möjlighet för åklagare att fatta interimistiska beslut

Regeringens förslag: Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens tillstånd i frågor om hemlig dataavläsning, ska tillstånd få ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd ska dock aldrig få avse rumsavlyssningsuppgifter eller fall som avser särskild utlänningskontroll.

Om åklagaren har gett ett interimistiskt tillstånd ska åklagaren utan dröjsmål skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden ska den upphäva beslutet.

Om åklagarens beslut har verkställts innan rätten gjort sin prövning ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, ska de uppgifter som lästs av eller tagits upp inte få användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

Utredningens förslag överensstämmer med regeringens förslag. Utredningen lämnar inte något uttryckligt författningsförslag om att åklagare ska få bevilja interimistiska beslut för att förebygga eller upptäcka brottslig verksamhet.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget särskilt.

Polismyndigheten, som tillstyrker förslaget, anser att åklagares interimistiska beslutsrätt skulle kunna ge hemlig dataavläsning bättre förutsättningar att överhuvudtaget kunna genomföras vid brådskande situationer. Om ett tillträdestillstånd måste inväntas från domstol finns nämligen risk att tillfället går förlorat. Även *Säkerhetspolisen* tillstyrker förslaget och uppfattar bestämmelsen som att tillträdestillståndet utgör en del av beslutet om hemlig dataavläsning och fattas i samband med detta. I vissa fall kan det enligt Säkerhetspolisen behövas tillträdestillstånd till en annan plats än vad som framgår av grundbeslutet, t.ex. om en misstänkt har tagit med sig sin mobiltelefon från hemmet till arbetet och låst in den i ett skåp. För att kunna verkställa beslutet om hemlig dataavläsning krävs i sådana fall ett nytt tillträdestillstånd. Säkerhetspolisen önskar därför att det tydliggörs att tillträdestillstånd kan fattas separat och avskilt från ett beslut om hemlig dataavläsning. Även *Civil Rights Defenders* tillstyrker förslaget men betonar att beslut från åklagare bör ske med försiktighet efter en noga genomgången proportionalitetsbedömning och åtgärderna måste alltid utföras med minsta möjliga integritetsintrång. Detta måste enligt föreningen framgå av bestämmelsen.

Säkerhets- och integritetsskyddsnämnden, Datainspektionen, *Sveriges advokatsamfund, Svenska Journalistförbundet* och *Dataskydd.net* anser att ett beslut om hemlig dataavläsning är så pass ingripande att det alltid bör fattas av domstol. Sveriges advokatsamfund tillägger under alla förhållanden att kravet på att det ska finnas risk för fördröjning av väsentlig betydelse bör skärpas väsentligt. *Uppsala universitet (Juridiska fakulteten)* uttrycker tveksamhet kring behovet av en interimistisk beslutanderätt för

åklagare inom ramen för en försöksperiod och anför att det är angeläget att det är domstol som ger tillstånd till hemlig dataavläsning.

Skälen för regeringens förslag: Domstolsprövningen är en viktig del av det system med rättssäkerhetsgarantier som omgärdar tillämpningen av de hemliga tvångsmedlen. Möjligheten för åklagare att fatta interimistiska beslut om hemliga tvångsmedel bör därför endast förekomma om det kan antas att syftet med regleringen annars inte kan uppnås (prop. 2002/03:74 s. 42–43). Möjligheten finns redan vid hemlig avlyssning och övervakning av elektronisk kommunikation och vid hemlig kameraövervakning, både under en förundersökning och i underrättelseverksamhet (27 kap. 21 a § RB och 6 a § preventivlagen). Det har framför allt motiverats med att avsaknaden av möjlighet till interimistiska beslut medför problem vid minutoperativa åtgärder som t.ex. att polisen med mycket kort varsel får reda på möten mellan kriminella eller byten av sim-kort. I sådana fall motsvarar domstolarnas tillgänglighet inte fullt ut behovet (prop. 2013/14:237 s. 138–139). Hemlig rumsavlyssning omfattas inte av bestämmelserna om interimistiska åklagarbeslut eftersom det är det nuvarande hemliga tvångsmedel som typiskt sett leder till störst intrång i enskildas personliga integritet (samma prop. s. 142).

Ett interimistiskt beslut av åklagare är ett undantag från huvudregeln om domstolsprövning och avsaknaden av kontradiktion innebär en viss försvagning av rättssäkerheten. Därför ska ett interimistiskt beslut enligt nuvarande ordning utan dröjsmål anmälas till rätten, som därefter skyndsamt ska pröva ärendet på samma vis som vid en ordinär ansökan. Om rätten då finner att det inte finns skäl för åtgärden, ska rätten upphäva beslutet. Om åtgärden redan har verkställts när rätten gör sin prövning gäller i stället att rätten ska pröva om det funnits skäl för den och, om rätten finner att sådana skäl saknats, att de inhämtade uppgifterna inte får användas i en brottsutredning till nackdel för den som har omfattats av åtgärden eller någon annan som uppgifterna avser (27 kap. 21 a § andra och tredje styckena RB och 6 a § preventivlagen). Genom dessa åtgärder minimeras de negativa konsekvenserna för enskildas rättssäkerhet (samma prop. s. 141).

Utredningen framhåller att de brottsbekämpande myndigheterna har ett behov av att även i brådskande situationer kunna få tillstånd till hemliga tvångsmedel. Behovet, som ökar i takt med den tekniska utvecklingen, har även tidigare konstaterats inte motsvaras av domstolarnas öppettider (samma prop. s. 138–139) och detsamma gäller enligt utredningen för hemlig dataavläsning. Utredningen föreslår därför att åklagare ska ha rätt att bevilja interimistiska beslut om hemlig dataavläsning utom såvitt gäller tillgång till rumsavlyssningsuppgifter eller i fall som avser särskild utlänningskontroll. Regeringen instämmer i utredningens bedömning att de brottsbekämpande myndigheterna i vissa fall snabbt behöver kunna få tillstånd till hemlig dataavläsning. Vissa remissinstanser bl.a. *Säkerhets- och integritetsskyddsnämnden, Datainspektionen, Sveriges advokatsamfund, Svenska Journalistförbundet* och *Dataskydd.net* invänder mot utredningens förslag att tillåta interimistiska beslut. Emellertid är det så att utan möjlighet till interimistiska beslut riskerar hemlig dataavläsning att bli utan verkan när verkställighetsåtgärder behöver vidtas med mycket kort varsel, något som bekräftas av *Polismyndigheten* och *Säkerhetspolisen*.

För att interimistisk åklagarprövning ska kunna tillåtas är det nödvändigt att beslutet omgärdas av starka rättssäkerhetsgarantier. De rättssäkerhetsgarantier som behandlas i avsnitt 12 och som föreslås gälla för hemlig dataavläsning i allmänhet bör också gälla när åklagare ger interimistiska beslut. Regeringen gör bedömningen att dessa krav är tillräckliga. Det bör därför införas en möjlighet för åklagare att bevilja interimistiska tillstånd till hemlig dataavläsning. Förutsättningarna för interimistisk åklagarprövning bör vara desamma som för befintliga tvångsmedel. Åklagarens prövning bör således vara underkastad samma krav och innehålla samma överväganden avseende proportionalitet och potentiella integritetsintrång som ett domstolsbeslut. Det finns därmed inte skäl att, som *Civil Rights Defenders* föreslår, föreskriva särskilda regler för beslut som ges av åklagare. Regeringen ser inte heller skäl att skärpa kravet för när ett interimistiskt beslut kan aktualiseras, vilket *Sveriges advokatsamfund* föreslår.

Eftersom det inte finns någon rätt för åklagare att ge interimistiska beslut vid hemlig rumsavlyssning bör det inte heller finnas någon sådan möjlighet när hemlig dataavläsning ska avse rumsavlyssningsuppgifter. Möjligheten bör inte heller finnas vid hemlig dataavläsning i LSU-fallen, eftersom åklagaren där inte har någon roll vid handläggningen.

Det finns inte några avgörande skäl mot att åklagaren även i inhämtningslagsfallen ska få ge interimistiska beslut om uppgifterna behövs omgående, t.ex. konkreta uppgifter om en nära förestående terroristattack, åtgärden är proportionerlig och uppgifterna inte går att hämta in på något annat rimligt sätt. Utredningen lämnar dock inte något uttryckligt författningsförslag om att det i dessa fall ska vara möjligt för åklagare att fatta interimistiska beslut om hemlig dataavläsning trots att utredningen lämnar en motivering till varför åklagare bör ha en sådan beslutanderätt. Att utredningens författningsförslag uttryckligen endast inrymmer möjlighet att fatta interimistiska beslut för att förhindra brottslig verksamhet (och inte även för att förebygga och upptäcka brottslig verksamhet) måste därmed närmast vara ett redaktionellt förbiseende. Ingen remissinstans invänder mot utredningens motivering till att interimistisk beslutanderätt bör finnas även i inhämtningslagsfallen. Även regeringen anser att en sådan beslutanderätt bör införas.

Slutligen, vad gäller *Säkerhetspolisens* synpunkt om beslut om tillträdestillstånd, kommer det med regeringens förslag inte att finnas något som hindrar en sökande från att komplettera en ansökan om hemlig dataavläsning i efterhand, till exempel med en ansökan om tillträdestillstånd, och få den prövad av domstol. Kompletterande beslut om tillträdestillstånd bör också kunna ges interimistiskt av åklagare. Även för sådana beslut gäller de rättssäkerhetskrav som uppställs i övrigt.

11.1.5 Vad ska ett beslut om hemlig dataavläsning innehålla?

Regeringens förslag: I ett tillstånd till hemlig dataavläsning ska det anges vilken tid tillståndet avser, vilket avläsningsbart informationssystem tillståndet avser, vilken typ av uppgift som får läsas av eller tas upp, villkor för att tillgodose intresset av att enskildas personliga

integritet inte kränks i onödan och, vid åtgärd som gäller rumsavlyssningsuppgifter, vem som är skäligen misstänkt för brottet.

Om ansökan gäller kameraövervaknings- eller rumsavlyssningsuppgifter ska det även anges vilken plats tillståndet gäller. Om tillståndet är förenat med ett tillträdestillstånd ska det anges i beslutet.

Tiden för tillståndet får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får inte tiden överstiga en månad från dagen för beslutet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget eller lämnar det utan invändning. *Svea hovrätt* ifrågasätter utredningens bedömning att den enskilde domaren är bäst skickad att avgöra på vilket sätt ett tillstånd till hemlig dataavläsning ska begränsas för att värna den enskildes integritet. Det borde tvärtom krävas att åklagaren ska ange eller till och med föreslå vilka villkor tillståndet bör förenas med i det enskilda fallet. *Datainspektionen* instämmer i att ansökan till domstolen, men även domstolens beslut, måste innehålla en redovisning av de tekniska åtgärder som ska vidtas.

Åklagarmyndigheten anser att det finns ett behov av att domstolen kan ge tillstånd om att verkställande myndigheter får installera tekniska hjälpmedel genom att kortvarigt rubba den misstänktes eller annan innehavares besittning till informationssystemet.

Svenska Journalistförbundet anser att ett beslut om hemlig dataavläsning bör innehålla en bedömning av vilka risker ett tillstånd skulle kunna medföra i form av kränkningar av tystnadsplikter. *Dataskydd.net*, med vilka *Civil Rights Defenders* instämmer, anser att det finns stora risker med hemlig dataavläsning och föreslår därför att det redan vid tillståndsprövningen måste finnas en plan för hur skadliga effekter ska minimeras. *Dataskydd.net* föreslår att det redan vid ansökan till domstolen bör finnas ett aktsamhetskrav på de åtgärder som föreslås. Dessutom föreslår föreningen att samtliga planerade åtgärder som utnyttjar sårbarheter i informationssystem bör redovisas för domstolen inför beslutet.

Skälen för regeringens förslag: I beslut om befintliga hemliga tvångsmedel ska det anges vilken tid tillståndet avser. Tiden får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet (27 kap. 21 § andra stycket RB, 7 § preventivlagen och 4 § inhämtningslagen). Motsvarande regler bör, som utredningen föreslår, gälla vid hemlig dataavläsning.

På samma sätt som gäller för tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation bör det, som utredningen föreslår, i beslutet också anges vilket objekt som tillståndet avser, alltså vilket informationssystem som tvångsmedlet ska användas på (jfr 27 kap. 21 § tredje stycket RB, 8 § preventivlagen och 4 § inhämtningslagen).

För att tillgodose skyddet för den enskilde bör det även, som utredningen föreslår, i beslutet anges vilken eller vilka uppgiftstyper som tillståndet avser. I avsnitt 9.3 redogörs för vilka uppgiftstyper ett tillstånd kan avse. Den som ansöker måste alltså för domstolen redogöra för vilken eller vilka uppgiftstyper som den anser behövs och rätten ska i beslutet ange vilken eller vilka uppgiftstyper som tillstånd har beviljats för. Det ska inte vara

möjligt att läsa av andra uppgiftstyper än vad som är tillåtet och de brottsbekämpande myndigheterna kommer att behöva anpassa verkställighetstekniken efter tillståndet (avsnitt 11.2.2).

När det gäller synpunkten från *Dataskydd.net* att åtgärder som utnyttjar sårbarheter i informationssystem bör redovisas för domstolen gör regeringen följande bedömning. Å ena sidan är utnyttjande av sårbarheter mycket känsligt ur ett informationssäkerhetsperspektiv, vilket talar för att sådana bör redovisas för domstolen. Å andra sidan hör en sådan fråga mycket nära ihop med själva verkställigheten samtidigt som det är mycket komplext att tekniskt beskriva en sådan sårbarhet. Det talar mot att Dataskydd.nets förslag. Regeringens uppfattning är sammantaget att det inte bör lagfästas en plikt för sökanden att ange om sårbarheter i informationssystem kommer att utnyttjas vid verkställighet eller att domstolens beslut måste innehålla en sådan förteckning. Inget hindrar dock att sökanden redovisar planerade åtgärder för domstolen eller att domstolen ställer frågor om detta vid sammanträdet, som en av många omständigheter som kan ha betydelse för domstolens proportionalitetsbedömning.

Svenska Journalistförbundet förordar att ett beslut om hemlig dataavläsning ska innehålla en bedömning av vilka risker ett tillstånd skulle kunna medföra i form av kränkningar av tystnadsplikter. Tystnadsplikten i den journalistiska verksamheten är av mycket stor betydelse. Det är därför viktigt att myndigheterna både vid ansökning om, beslut om och verkställighet av hemlig dataavläsning noggrant beaktar risker för att det som tystnadsplikten är avsedd att skydda äventyras. En viktig komponent i detta skydd är förslaget att proportionalitetsprincipen ska lagfästas (avsnitt 9.4). Regeringen anser härigenom att tystnadsplikten är tillräckligt värnad och att det inte, som förbundet förordar, behövs särskilda regler om att det i ett beslut om hemlig dataavläsning ska tas in en bedömning av risken för kränkning av tystnadsplikten. Det kan tilläggas att det inte finns någon sådan särskild reglering för befintliga tvångsmedel.

I ett tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning ska platsen där åtgärderna får vidtas anges (27 kap. 21 § fjärde stycket RB samt 8 § preventivlagen avseende kameraövervakning). När hemlig dataavläsning avser kameraövervaknings- och rumsavlyssningsuppgifter bör motsvarande platskrav gälla som för de bakomliggande tvångsmedlen (avsnitt 10.1.4). Vilken plats som avses bör, i likhet med vad utredningen föreslår, anges i tillståndsbeslutet för hemlig dataavläsning.

Dessutom bör det på samma sätt som i dag krävs vid hemlig rumsavlyssning anges i beslutet vem som är misstänkt, när hemlig dataavläsning avser rumsavlyssningsuppgifter (jfr 27 kap. 21 § femte stycket RB). Vidare bör det också anges i beslutet om ett tillträdestillstånd har beviljats och vilken plats det i så fall avser (jfr 27 kap. 21 § fjärde stycket RB).

Slutligen bör det i beslutet anges de särskilda villkor som domstolen ställt upp för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan (jfr 27 kap. 21 § sjätte stycket RB). Sådana villkor kan ta sikte på i stort sett vilka omständigheter som helst som kan gagna skyddet för den personliga integriteten, t.ex. att användningen av hemlig dataavläsning ska begränsas när avläsningen eller upptagningen avser ett avläsningsbart informationssystem som används av en större krets av personer, t.ex. en dator på ett internetcafé. I sådana fall bör avläsning eller upptagning endast utföras när man vet att den misstänkte använder datorn.

Ett annat exempel är att användningen av hemlig dataavläsning bör begränsas när det finns risk att utomstående, som inte alls har med utredningen att göra, riskerar att figurera i tal eller på film vid aktivering av en mikrofon eller kamera på en mobiltelefon. *Svea hovrätt* förordar att den som ansöker om hemlig dataavläsning ska ange vilka villkor tillståndet bör förenas med för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Något sådant krav finns inte beträffande bakomliggande tvångsmedel och regeringen ser inte behov av att införa ett sådant krav avseende hemlig dataavläsning. Vid sammanträdet kan det dock finnas anledning för den som söker om tillstånd att motivera sin ansökan genom att på ett övergripande plan beskriva hur tvångsmedlet ska verkställas. Vid eventuella oklarheter eller behov av kompletteringar har dessutom domstolen möjlighet att genom frågor skaffa sig ett tillräckligt underlag för att fatta beslut i ärendet, inklusive villkor för att skydda enskildas personliga integritet.

Åklagarmyndigheten förordar att ett beslut om hemlig dataavläsning ska kunna innehålla en befogenhet för den verkställande myndigheten att installera tekniska hjälpmedel genom att kortvarigt rubba den misstänktes eller annan innehavares besittning till informationssystemet. Åklagarmyndigheten ger som exempel på en sådan besittningsrubbning att kortvarigt omhänderta en misstänkts mobiltelefon vid trafikkontroll, vid avlägsnande enligt 13 § polislagen (1984:387) eller vid avvisitering vid en tullkontroll. Även om en sådan ordning skulle ha verkställighetsmässiga fördelar kan konstateras att de möjligheter till besittningsrubbningar som myndigheterna har till sitt förfogande skulle användas utanför sitt tänkta ändamål; något som i sig inger betänkligheter. Dessutom skulle en sådan ordning i princip kräva att myndigheterna skulle ljuga om orsaken till den tillfälliga besittningsrubbningen, vilket inger ännu starkare betänkligheter. Regeringen lämnar därför, i likhet med utredningen, inget sådant förslag.

11.1.6 Omedelbar verkställighet och omedelbart hävande

Regeringens förslag: Beslut i frågor om hemlig dataavläsning ska få verkställas omedelbart.

Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, ska den som ansökt om åtgärden eller rätten omedelbart häva beslutet.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna yttrar sig inte i denna del. *Stockholms tingsrätt* väcker frågan om inte hänvisningen till rättegångsbalkens regler om handläggning vid domstol av frågor om tvångsmedel i brottmål innefattar frågan om att beslut under rättegången beträffande tvångsmedel genast ska gå i verkställighet. Därmed anser tingsrätten att bestämmelsen möjligen är överflödig.

Skälen för regeringens förslag: I både rättegångsbalken och de lagar som reglerar hemlig tvångsmedelsanvändning i underrättelseverksamhet finns bestämmelser om att åklagaren eller rätten omedelbart ska upphäva beslutet om det inte längre finns skäl för åtgärden (se t.ex. 27 kap. 23 § RB). Regeringen delar utredningens bedömning att det finns skäl att införa

en motsvarande bestämmelse för hemlig dataavläsning. Eftersom åklagaren inte har någon roll i LSU-fallen bör den dock formuleras något annorlunda än befintliga bestämmelser.

Häktning och hemliga tvångsmedel som finns i rättegångsbalken får verkställas omedelbart efter beslut (30 kap. 12 § RB). Även hemlig dataavläsning bör kunna verkställas omedelbart. Frågan är, som *Stockholms tingsrätt* lyfter, om hänvisningen till rättegångsbalkens procedurregler medför att det saknas behov av en sådan bestämmelse som utredningen föreslår och som tillåter omedelbar verkställighet. Det kan konstateras att preventivlagen innehåller en bestämmelse om omedelbar verkställighet. Eftersom preventivlagen i nu relevant hänseende är uppbyggd på samma sätt som föreslås för hemlig dataavläsning delar regeringen utredningens bedömning att – inte minst av pedagogiska skäl – en bestämmelse med nu aktuellt innehåll bör införas i lagen.

11.2 Genomförande av hemlig dataavläsning

11.2.1 Verkställighetstekniken

Regeringens förslag: När tillstånd till hemlig dataavläsning har lämnats ska de verkställande myndigheterna få använda de tekniska hjälpmedel som behövs för avläsning och upptagning.

Om det är nödvändigt ska systemskydd få brytas eller kringgås och tekniska sårbarheter utnyttjas.

Regeringens bedömning: Det bör inte införas ett krav för de brottsbekämpande myndigheterna att rapportera säkerhetsrisker och sårbarheter som upptäcks vid verkställighet.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen lämnar inte någon uttrycklig bedömning i frågan om krav att rapportera säkerhetsbrister och sårbarheter.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget.

Säkerhets- och integritetsskyddsnämnden påpekar att de verkställande myndigheterna genom förslaget får stor frihet att avgöra vilka tekniska hjälpmedel som ska användas vid verkställighet av hemlig dataavläsning. I avsaknad av närmare uppgifter om på vilket sätt rättssäkerhetsgarantierna (bl.a. krav på teknikanpassning och aktsamhet) ska verka i praktiken kan inte nämnden tillstyrka förslaget i dessa delar. Nämnden anser att domstolen måste ha en reell möjlighet att kunna ange villkor för att enskildas personliga integritet inte kränks i onödan, varför verkställighetstekniken i så fall borde ingå i domstolsprövningen. *Datainspektionen* delar uppfattningen att domstolen måste få veta vilka tekniska åtgärder som ska genomföras för att kunna göra en fullständig nödvändighets- och proportionalitetsbedömning. Datainspektionen anser att det därför bör ingå i ansökan till domstolen att redogöra för vilka slags åtgärder som ska genomföras. *Svea hovrätt* noterar att utredningen inte föreslår att verkställighetstekniken ska ingå i domstolsprövningen samtidigt som det anges att domstolen ska förhöra sig om hur verkställigheten ska gå till och ge föreskrifter för att säkerställa att tillståndet följs. Hovrätten anser att uttalandena

framstår som motstridiga och att det finns skäl att tydliggöra vad som ingår i prövningen.

Myndigheten för samhällsskydd och beredskap anser att det är olyckligt att den kunskap som byggs upp kring informationssäkerhetsbrister i samband med hemlig dataavläsning inte i något skede och inte på något sätt ska kunna nyttjas för att stärka skyddet för sådana system som samhällsviktig verksamhet är beroende av. Myndigheten anser därför att det finns ett behov av en fördjupad analys som balanserar avvägningen mellan de brottsbekämpande myndigheternas behov och informations- och cybersäkerhet.

Andra remissinstanser, bl.a. *Kungliga tekniska högskolan (KTH), Föreningen för digitala fri- och rättigheter, Stiftelsen för Internetinfrastruktur (Internetstiftelsen)*, *Dataskydd.net, IT&Telekomföretagen* och *HI3G Access AB*, har invändningar och synpunkter på att det inte införs någon rapporteringsskyldighet avseende upptäckta sårbarheter i de informationssystem som kommer att läsas av. Remissinstanserna anser att detta ökar risken för informationssäkerheten och kan i förlängningen drabba allmänheten.

Svenska stadsnätsföreningen och *Sveriges advokatsamfund* anför att det finns risk för s.k. ändamålsglidning, alltså att lagstiftningen i takt med den tekniska utvecklingen får ett vidare tillämpningsområde än vad som var tänkt från början, och att detta bör omhändertas i lagen.

Skälen för regeringens förslag och bedömning

Nuvarande regler om verkställighet av hemliga tvångsmedel

I nuvarande regler om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation framgår att de tekniska hjälpmedel som behövs för åtgärden får användas (27 kap. 25 § RB). Även i preventivlagen används samma uttryckssätt (9 §). Det innebär att myndigheterna kan verkställa åtgärden med den avlyssnings- eller övervakningsutrustning som de anser lämplig. Dessutom har den verkställande myndigheten möjlighet till assistans av de operatörer som bedriver verksamhet enligt lagen om elektronisk kommunikation (27 kap. 25 § andra stycket RB och 6 kap. 19 § lagen om elektronisk kommunikation).

Även bestämmelserna om vilken teknik som får användas vid hemlig kameraövervakning och hemlig rumsavlyssning är öppna och teknikneutrala. För hemlig kameraövervakning gäller således att fjärrstyrda TV-kameror, andra optisk-elektroniska instrument eller därmed jämförbara utrustningar får används för optisk personövervakning (27 kap. 20 a § RB). För hemlig rumsavlyssning gäller att åtgärden får vidtas med hjälp av ett tekniskt hjälpmedel som är avsett att återge ljud (27 kap. 20 d § RB).

Verkställighet av hemlig dataavläsning

För att verkställighet av hemlig dataavläsning inte ska orsaka större integritetsintrång och säkerhetsrisker än vad som är oundgängligen nödvändigt, behövs regler som sätter ramar för verkställigheten.

En regel som beskriver verkställighetsförfarandet bör utformas teknikneutralt, för att stå sig över tid, men samtidigt vara någorlunda specifik

och begränsande. Utredningen föreslår att en sådan regel till sin ordalydelse ska stämma överens med vad som gäller för verkställighet av hemlig avlyssning och övervakning av elektronisk kommunikation. För dessa tvångsmedel gäller att de tekniska hjälpmedel som behövs för åtgärden får användas, sedan tillstånd lämnats (27 kap. 25 § RB). Beskrivningen är neutral och kan ge de brottsbekämpande myndigheterna viss frihet att själva bestämma formerna för verkställighet samtidigt som mer ingripande åtgärder än vad som behövs inte bör få användas. *Svenska stadsnätsföreningen* lyfter en fara med en teknikneutral bestämmelse och anför att det, i takt med den tekniska utvecklingen, kan leda till ändamålsglidning. Även *Sveriges advokatsamfund* ser denna risk. Det kan i detta sammanhang konstateras att ändamålen vid hemlig dataavläsning inte påverkas av vilken teknisk metod som används. Det finns inte heller något i erfarenheterna från befintliga hemliga tvångsmedel som leder till misstankarna att en teknisk utveckling riskerar att medföra en ändamålsglidning. Dessutom föreslår regeringen en bestämmelse som innebär att den teknik som används ska anpassas efter det tillstånd som har beviljats så att några andra uppgifter än de som avses med tillståndet inte ska kunna läsas av eller tas upp (avsnitt 11.2.2). I likhet med utredningen föreslår regeringen därför att en bestämmelse införs med innebörden att när tillstånd till hemlig dataavläsning har lämnats får de tekniska hjälpmedel som behövs för avläsning och upptagning användas.

Med tekniska hjälpmedel avses både hårdvara och programvara. De tekniska hjälpmedlen kan vara fysiskt placerade i informationssystemet eller, när det är fråga om avläsning av uppgifter i informationssystem som t.ex. ett internetbaserat användarkonto, helt enkelt utgöras av datorer hos den brottsbekämpande myndigheten som utför avläsningen efter inloggning på kontot. Det kan också gälla t.ex. programvara eller funktioner som redan finns i informationssystemet, såsom GPS, kamera eller mikrofon för att kunna avläsa eller ta upp plats-, kameraövervaknings- eller rumsavlyssningsuppgifter, eller programvara som den brottsbekämpande myndigheten placerar i systemet för att hemlig dataavläsning ska kunna genomföras.

Vissa åtgärder som kan vidtas av de brottsbekämpande myndigheterna kan inte ses som verkställighet med tekniska hjälpmedel. De åtgärder som myndigheterna får vidta måste dock vara uttryckligt tillåtna i lag för att de som verkställer åtgärden ska undgå ansvar för dataintrång (se avsnitt 9.2). Ett exempel på en sådan åtgärd som utredningen beskriver är att det bör vara möjligt att genom inloggning med den misstänktes inloggningsuppgifter, om de är kända, bereda sig tillgång till ett informationssystem. Ett annat exempel kan vara att myndigheterna helt enkelt gissar sig fram till lösenordet eller tar sig förbi lösenordsskyddet på något annat sätt, t.ex. genom att utnyttja sårbarheter. Ett sammanfattande uttryck för en sådan åtgärd, och andra liknande åtgärder, är att den brottsbekämpande myndigheten får bryta eller kringgå systemskydd om det är nödvändigt för att kunna verkställa ett beslut om hemlig dataavläsning. Som utredningen föreslår bör en bestämmelse som tillåter det föras in i lagen.

Verkställighetstekniken ingår inte i domstolsprövningen

Utredningen föreslår att domstolens prövning vid tillståndsgivningen inte ska omfatta vilken teknik som får användas. *Säkerhets- och integritetsskyddsnämnden, Civil Rights Defenders* och *Datainspektionen* är kritiska till detta och anför att verkställighetstekniken är en nödvändig komponent för att domstolen korrekt ska kunna pröva åtgärden. Som redogörs för ovan är reglerna kring de befintliga hemliga tvångsmedlen utformade på så sätt att domstolen inte särskilt prövar vilka verkställighetsmetoder som ska användas trots att bestämmelserna är teknikneutralt utformade. Domstolen ska däremot pröva om de lagliga förutsättningarna för åtgärderna är uppfyllda och vid verkställighet är de brottsbekämpande myndigheterna skyldiga att iaktta grundläggande principer om ändamål, behov och proportionalitet. Dessutom kommer användningen av hemlig dataavläsning att vara föremål för tillsyn. Regeringen föreslår mot denna bakgrund, i likhet med utredningen, att verkställighetstekniken inte ska ingå i tillståndsprövningen. *Svea hovrätt* tycker att det ter sig motsägelsefullt att utredningen förutsätter att domstolen ska förhöra sig om verkställighet samtidigt som frågor om verkställighetsteknik inte ingår i prövningen. Regeringen noterar härvid att den verkställighet som utredningen föreslår att beslutsfattaren ska orientera sig om rör omständigheter kring säkerställandet av det s.k. platskravet. Det finns inte heller något som hindrar att domstolen ställer frågor om verkställighetsteknik i syfte att kunna utforma eventuella villkor för att tillgodose intresset av att enskildas integritet inte kränks i onödan (se avsnitt 11.1.3).

Det bör inte införas en skyldighet att rapportera sårbarheter och säkerhetsrisker

Utredningen behandlar frågan om huruvida det vid hemlig dataavläsning bör finnas en skyldighet för de brottsbekämpande myndigheterna att rapportera sårbarheter och säkerhetsbrister till tillverkaren av informationssystemet. Utredningen bedömer att det inte finns tillräckligt starka skäl för att införa en skyldighet för de brottsbekämpande myndigheterna att redovisa vilka tekniker de använder eller att rapportera säkerhetsbrister eller sårbarheter i ett informationssystem.

När svagheterna är kända för tillverkaren anser utredningen att den som utvecklar eller producerar informationssystemet redan i dag har möjlighet att åtgärda svagheterna och upplysa användarna om bristen. Utredningen bedömer att brottsbekämpande myndigheters utnyttjande av sådana sårbarheter eller säkerhetsbrister inte kan öka riskerna för att användarna drabbas eller att det på annat sätt upprätthålls nya vägar in i informationssystem. Regeringen instämmer av samma skäl i bedömningen att det för kända säkerhetsbrister inte finns skäl att införa en lagstadgad rapporteringsskyldighet för de brottsbekämpande myndigheterna.

När det gäller utnyttjande av sårbarheter eller säkerhetsbrister som inte är kända av den som utvecklar eller producerar informationssystemet (så kallade dag noll-sårbarheter) ger utredningen en något annan bild. Dessa sårbarheter har ännu inte upptäckts av tillverkaren och om de skulle upptäckas vid verkställighet av hemlig dataavläsning skulle tillverkaren efter information från de brottsbekämpande myndigheterna kunna åtgärda felet. Om inte tillverkaren får reda på att sårbarheterna finns, men myndigheten

känner till det och inte rapporterar dem, kan det finnas risk att t.ex. kriminella personer kan använda samma sårbarhet. Detta skulle, som bl.a. *Dataskydd.net* och *Föreningen för digitala fri- och rättigheter* anför, kunna leda till virusspridning och även i övrigt bristande cybersäkerhet.

Utredningen anser att det finns vissa skäl som talar för att en rapporteringsskyldighet för sårbarheter som inte är kända för tillverkaren bör införas. Trots det föreslås inte något sådant krav. Utredningen konstaterar emellertid att för tillverkaren okända sårbarheter kommer att finnas oavsett om de brottsbekämpande myndigheterna får kännedom om dem eller inte. Därmed kommer sårbarheterna att kunna utnyttjas av den som upptäcker eller får kännedom om dem och har tillräcklig kunskap att utnyttja dem oberoende av de brottsbekämpande myndigheternas arbete. Den enda ökade risken med att använda tidigare okända sårbarheter är om information om dem sprids från de brottsbekämpande myndigheterna. Som regeringen föreslår i avsnitt 12.2.4 kommer kännedomen om sårbarheterna dock att begränsas till vissa noggrant säkerhetskontrollerade personer hos de brottsbekämpande myndigheterna, varför risken för spridning utanför denna krets bedöms vara synnerligen liten (se avsnitt 12.2.4).

Regeringen anser därför, i likhet med utredningen men till skillnad från bl.a. *Internetstiftelsen* och *IT&Telekomföretagen,* att det inte bör införas någon rapporteringsskyldighet avseende tidigare okända sårbarheter. Därmed finns inte heller skäl till sådan dokumentation av sårbarheter som *Myndigheten för samhällsskydd och beredskap* förespråkar. Det bör dock anmärkas att brottsbekämpande myndigheter, i den mån de upptäcker sårbarheter eller säkerhetsbrister som de bedömer kan utgöra stor risk för informationssystem eller den generella informations- eller cybersäkerheten, är oförhindrade att rapportera dessa till tillverkaren även utan lagkrav. Detta kan vara särskilt angeläget om det skulle vara fråga om sårbarheter i samhällsviktig verksamhet.

11.2.2 Anpassning av verkställighetsteknik

Regeringens förslag: Den teknik som används i samband med hemlig dataavläsning ska anpassas efter det tillstånd som beviljats. Tekniken får inte göra det möjligt att läsa av eller ta upp någon annan uppgiftstyp än vad som anges i tillståndet.

Om det kommer fram att någon annan typ av uppgifter än den som tillståndet avser har lästs av eller tagits upp ska upptagningarna och uppteckningarna av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. Uppgifter som kommit fram vid sådan avläsning eller upptagning får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna kommenterar inte förslaget eller lämnar det utan invändning. *Säkerhets- och integritetsskyddsnämnden* ifrågasätter dock behovet av att underrättas efter att otillåten överskottsinformation har förstörts, eftersom det då inte finns något material kvar att granska.

Skälen för regeringens förslag: Den teknik som används i samband med hemlig dataavläsning kan möjliggöra avläsning och upptagning av olika slags uppgifter. Tillståndet till hemlig dataavläsning begränsar vilka uppgiftstyper det kan bli fråga om i det enskilda fallet och det är således endast uppgiftstyper som uttryckligen framgår av tillståndet som får läsas av eller tas upp.

Även om det saknas skäl att tro att de brottsbekämpande myndigheterna inte skulle rätta sig efter ett beviljat tillstånd instämmer regeringen i utredningens förslag att det behövs en bestämmelse om att den teknik som används måste anpassas efter vilka uppgiftstyper som ska läsas av eller tas upp. Det kommer att utgöra en teknisk spärr mot att tillståndet inte överträds. Om myndigheterna vid något enskilt tillfälle inte på ett korrekt sätt har anpassat tekniken och därför av misstag hämtat in uppgifter utanför tillståndets ram bör det som utredningen föreslår finnas ytterligare en rättssäkerhetsgaranti i form av begränsningar för hur den felaktigt inhämtade informationen ska få användas. Med hänsyn till de rådande principerna om fri bevisprövning och fri bevisföring skulle felaktigt inhämtade uppgifter annars kunna användas som bevisning i domstol, se t.ex. propositionen Överskottsinformation vid användning av hemliga tvångsmedel m.m. (prop. 2004/05:143 s. 36). Regeringen instämmer därför i att det behöver regleras vad som ska gälla för otillåten tilläggsinformation. bör Upptagningar av sådana uppgifter bör omedelbart förstöras, i likhet med vad som gäller för uppgifter som omfattas av de s.k. beslagsförbuden och frågeförbuden i rättegångsbalken (27 kap. 2 § och 36 kap. 5 §). Dessutom bör myndigheten underrätta Säkerhets- och integritetsskyddsnämnden om att otillåten tilläggsinformation har lästs av eller tagits upp. En sådan underrättelse tillförsäkrar att nämnden får underlag som kan läggas till grund för att bedöma om ett tillsynsärende bör initieras. Den bedömningen är inte beroende av om tilläggsinformationen finns kvar eller inte. Regeringen gör därmed en annan bedömning än *Säkerhets- och integritetsskyddsnämnden* i detta avseende.

Slutligen bör det föreskrivas att otillåten tilläggsinformation inte ska få användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser. Även om upptagningar och uppteckningar måste förstöras finns det ett behov av en sådan bestämmelse. Förstörandet av upptagningar och uppteckningar betyder nämligen inte alltid att själva uppgiften försvinner. Det kan t.ex. vara så att en polisman redan har tagit del av upptagningen och uppgiften finnas då kvar i polismannens medvetande. Kännedomen om uppgiften bör då inte få utnyttjas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser. En sådan reglering har visserligen inte någon lagfäst motsvarighet i någon annan författning, men med hänsyn till lagens ingripande karaktär är det nödvändigt med tydliga och uttryckliga bestämmelser till skydd för rättssäkerheten.

11.2.3 Aktsamhetskrav och informationssäkerhet i samband med verkställighet

Regeringens förslag: När ett beslut om hemlig dataavläsning verkställs ska inte någon olägenhet eller skada få förorsakas utöver vad som är

absolut nödvändigt. Informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser ska inte få åsidosättas, minskas eller skadas till följd av verkställigheten. När verkställigheten avslutas ska den verkställande myndigheten vidta de åtgärder som behövs för att informationssäkerheten i det avläsningsbara informationssystem som tillståndet avser ska hålla åtminstone samma nivå som vid verkställighetens början.

Ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet gått ut eller tillståndet upphävts.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget. Några remissinstanser, bl.a. *Post- och telestyrelsen* och *Civil Rights Defenders,* tillstyrker att det införs en regel om aktsamhet. *Försvarsmakten* anför att det är angeläget att inte myndighetens egen informationssäkerhet påverkas efter att hemlig dataavläsning genomförts. Därför föreslår Försvarsmakten att samråd ska ske med myndigheten innan dess system blir föremål för åtgärd.

Sveriges advokatsamfund anser att tidskravet för när ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart bör skärpas ytterligare. För att minimera risken för att uppgifter inhämtas efter att ett tillstånd löpt ut eller hävts bör detta ske i direkt anslutning till eller omedelbart efter att så skett.

Myndigheten för samhällsskydd och beredskap anser att ett krav att dokumentera vidtagna åtgärder är en förutsättning för att kunna genomföra en efterkontroll av att informationssäkerheten de facto har återställts till åtminstone samma nivå som vid verkställighetens början. Även om det kan finnas skäl för att inte i detalj specificera i lag vilka åtgärder som ska göras för att återställa informationssäkerheten är det enligt myndighetens mening centralt att införa ett tydligt krav på att arbetet dokumenteras.

Skälen för regeringens förslag

En allmän aktsamhetsregel införs

Även om proportionalitetsprincipen gäller också vid verkställighet finns det för befintliga tvångsmedel särskilda regler som påminner om att olägenhet eller skada inte får förorsakas utöver vad som är absolut nödvändigt vid verkställighet (t.ex. 28 kap. 6 § RB). För att regleringen om hemlig dataavläsning ska korrespondera med regleringen om de bakomliggande tvångsmedlen och med hänsyn till tvångsmedlets ingripande karaktär finns det behov av en liknande bestämmelse i lagen om hemlig dataavläsning. I enlighet med vad utredningen föreslår bör därför en sådan bestämmelse införas.

Informationssäkerhet

Utredningen bedömer att hemlig dataavläsning medför risker för informationssäkerheten, vilka måste balanseras för att det ska vara försvarligt att införa regelverket. De risker som utredningen redovisar är bl.a. risker att information sprids till obehöriga från det informationssystem som åtgärden avser, risker för minskad säkerhet i och utanför systemet och

risker för att sårbarheter blir kända utanför kretsen av personer som ska vara betrodda med informationen. Utredningen föreslår därför att det bör införas en reglering i lagen om att den som ska verkställa hemlig dataavläsning ska vidta nödvändiga åtgärder för att informationssäkerheten utanför det informationssystem som är föremål för hemlig dataavläsning inte åsidosätts, minskas eller skadas till följd av verkställigheten. Det står klart att utredningen härvid åsyftar informationssäkerheten i andra informationssystem än det som tillståndet avser. Även om det får accepteras att det i det informationssystem som är föremål för hemlig dataavläsning uppstår en minskning av informationssäkerheten är det inte avsikten att andra informationssystem som finns i dess närhet, har kontakt med informationssystemet eller inte har något samröre med informationssystemet ska drabbas. Regeringen instämmer i utredningens förslag och bedömning.

Utredningen föreslår också att det införs en allmän aktsamhetsregel som har karaktären av en instruktion för myndigheterna att vidta nödvändiga åtgärder för att undvika en minskad informationssäkerhet. Regeringen delar uppfattningen att regeln bör utformas generellt och teknikneutralt, för att fånga upp de olika typer av risker och situationer som kan uppstå. Genom en generell aktsamhetsregel kan risken för informationssäkerheten samt övriga olägenheter och skador begränsas till vad som är absolut nödvändigt. Lämpligen kan detta uttryckas så att vid verkställigheten ska nödvändiga åtgärder vidtas för att informationssäkerheten i andra informationssystem än det tillståndet avser inte får åsidosättas, minskas eller skadas till följd av verkställigheten. Regeringen återkommer i avsnitt 12.2.4 med förslag om att verkställigheten av hemlig dataavläsning endast ska få utföras av vissa, särskilt kvalificerade personer.

När det gäller förslaget från *Försvarsmakten* om att den verkställande myndigheten ska samråda med Försvarsmakten innan hemlig dataavläsning riktas mot dess system gör regeringen följande bedömning. Vid de få tillfällen där det kan bli aktuellt med hemlig dataavläsning mot avläsningsbara informationssystem hos Försvarsmakten kan det vara fråga om synnerligen allvarliga brott mot rikets säkerhet där den berörda personkretsen inte är fullt klarlagd. I ett sådant fall kan det inte komma på fråga att införa någon samrådsskyldighet. En annan sak är att det inte ter sig främmande att samråd av praktiska skäl måste genomföras med Försvarsmakten för att överhuvudtaget kunna utföra hemlig dataavläsning mot informationssystem som den förfogar över. Sammantaget ser således regeringen inte skäl att införa någon samrådsskyldighet före avläsning av Försvarsmaktens – eller någon annans – informationssystem.

Myndigheten för samhällsskydd och beredskap anser att vidtagna åtgärder bör dokumenteras för att det ska vara möjligt att kontrollera att informationssäkerheten har återställts efter verkställighet. Frågan om dokumentation aktualiseras i betänkandet Rättssäkerhetsgarantier och hemliga tvångsmedel (SOU 2018:61 s. 201 och 218–223). Betänkandet bereds i Regeringskansliet. Det saknas skäl att här föregripa den beredningen.

Åtgärder när verkställighet avslutas

Utredningen bedömer att när hemlig dataavläsning avslutas bör informationssystemet som tillståndet avser inte ha ett sämre skydd för informationssäkerheten än när avläsningen påbörjats. Det bör därför införas regler om att den verkställande myndigheten i samband med att verkställighet avslutas ska vidta de åtgärder som behövs för att informationssäkerheten i det informationssystem som tillståndet avser ska hålla åtminstone samma nivå som vid verkställighetens början. Kravet bör gälla oavsett vilken verkställighetsteknik som har använts.

Det bör också enligt utredningen föreskrivas att ett tekniskt hjälpmedel som har använts i samband med verkställighet ska tas bort eller göras obrukbart när tvångsmedelsanvändningen avslutats. Det betyder att myndigheterna ska ta bort eller avinstallera t.ex. programvaror och hårdvaror som använts så snart det kan göras efter att tiden för tillståndet har gått ut eller tillståndet upphävts. *Sveriges advokatsamfund* förordar att tidskravet ska skärpas. Regeringen noterar dock i detta sammanhang att en motsvarande regel med samma tidskrav som utredningen föreslår finns beträffande hemlig kameraövervakning och hemlig rumsavlyssning (27 kap. 25 a § fjärde stycket RB). Inget har framkommit som ger skäl att ifrågasätta att detta är en väl avvägd frist. Regeringen delar således utredningens bedömning.

12 Rättssäkerhetsgarantier och andra frågor

12.1 Vissa rättssäkerhetsgarantier

12.1.1 Allmänt om rättssäkerhetsgarantier i lagstiftningen om hemliga tvångsmedel

Som redogörs för i avsnitt 4.2 måste staten vid användning av hemliga tvångsmedel respektera vissa grundläggande mänskliga rättigheter. En viktig komponent i detta är att införa ett integritetsstärkande ramverk kring reglerna om hemliga tvångsmedel som reglerar överskottsinformation, granskning, bevarande och förstörande av upptagningar och uppteckningar samt underrättelse till enskild. Härutöver brukar regler om tillsyn införas. Den svenska regleringen av hemliga tvångsmedel – och dess rättssäkerhetsgarantier – utvärderas emellanåt och har generellt sett ansetts leva upp till både regeringsformens och Europakonventionens krav (se SOU 2012:44 och SOU 2018:61).

12.1.2 Överskottsinformation

Regeringens förslag: När hemlig dataavläsning används eller har använts under en förundersökning ska det som gäller för överskottsinformation vid hemlig avlyssning av elektronisk kommunikation tillämpas för åtgärden. Det som gäller hemlig rumsavlyssning ska dock tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

När hemlig dataavläsning används eller har använts i underrättelseverksamhet ska de regler om överskottsinformation som gäller vid förhindrande av vissa särskilt allvarliga brott respektive inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, tillämpas på motsvarande sätt. Detsamma ska gälla vid särskild utlänningskontroll.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget. *Civil Rights Defenders* tillstyrker förslaget och betonar att det måste vara tydligt hur överskottsinformation hanteras med hänsyn till reglerna i Europakonventionen.

Dataskydd.net anser att utredningen inte på ett tillräckligt sätt har beaktat att överskottsinformation ofta kan vara information av mycket privat karaktär. Dataskydd.net anser vidare att det inte finns något visat behov av att få använda överskottsinformation vid hemlig dataavläsning.

Skälen för regeringens förslag

Nuvarande regler om användning av överskottsinformation

När tvångsmedel verkställs kan det komma fram uppgifter som inte har med den brottslighet som legat till grund för tillståndet att göra. Detta benämns överskottsinformation. Överskottsinformation får alltid användas för att förhindra förestående brott (27 kap. 23 a § RB, 12 § preventivlagen, 21 a § LSU samt 6 och 7 §§ inhämtningslagen). En förundersökning eller motsvarande utredning får dock enligt 27 kap 23 a § RB och 21 a § LSU inledas på grund av överskottsinformationen endast om det är föreskrivet fängelse i ett år eller däröver för brottet och det kan antas att brottet inte föranleder endast böter, eller om det finns särskilda skäl. Pågår det redan en förundersökning beträffande det andra brottet, eller inleds en sådan på grund av andra uppgifter än överskottsinformationen, får de senare uppgifterna användas i den undersökningen.

För hemlig rumsavlyssning gäller att överskottsinformation får användas för att utreda brottet endast om det är fråga om ett brott som kan föranleda hemlig rumsavlyssning, eller annat brott, om det är föreskrivet fängelse i tre år eller däröver för brottet.

Enligt preventivlagen får överskottsinformation användas för att utreda ett brott om det är fråga om ett brott som omfattas av den lagen eller om det är ett brott för vilket det är föreskrivet fängelse i tre år eller däröver (12 §).

Enligt inhämtningslagen får uppgifterna användas för att förhindra brott (6 §). Vidare får uppgifter som kommit fram vid inhämtning enligt lagen 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 beslut om att inleda en förundersökning (7 §).

I sammanhanget kan även framhållas att Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel sett över reglerna om överskottsinformation (SOU 2018:61). Betänkandet bereds i Regeringskansliet.

Överskottsinformation vid hemlig dataavläsning

Utredningen föreslår att reglerna om överskottsinformation i den föreslagna lagen ska följa de regler som gäller för överskottsinformation som kommit fram genom användandet av bakomliggande hemliga tvångsmedel. Regeringen instämmer i detta. Överskottsinformation kan nämligen innehålla uppgifter som är viktiga för att utreda allvarlig brottslighet och det är, som *Civil Rights Defenders* poängterar, angeläget att det regleras hur sådan information får användas. Det finns inte skäl eller underlag att i detta lagstiftningsärende göra någon annan bedömning än vad som har gjorts i tidigare lagstiftningsärenden när det gäller frågan om överskottsinformation från hemliga tvångsmedel i övrigt, vilket *Dataskydd.net* efterfrågar.

Som framgår ovan skiljer sig reglerna om överskottsinformation åt beroende på om hemliga tvångsmedel används i förundersöknings-, underrättelseverksamhet eller vid särskild utlänningskontroll och behöver därför regleras på olika sätt, även gällande hemlig dataavläsning.

I förundersökningsverksamhet bör, i enlighet med vad utredningen föreslår, således följande gälla. För överskottsinformation när hemlig dataavläsning använts för att ta upp rumsavlyssningsuppgifter bör motsvarande regler gälla som vid hemlig rumsavlyssning (27 kap. 23 a § RB). För överskottsinformation vid övrig användning av hemlig dataavläsning bör motsvarande regler gälla som för hemlig avlyssning och övervakning av elektronisk kommunikation och hemlig kameraövervakning (27 kap. 23 a § första stycket RB).

När det gäller överskottsinformation i underrättelseverksamhet bör motsvarande regler gälla för hemlig dataavläsning som för dagens underrättelseverksamhet (12 § preventivlagen respektive 6 och 7 §§ inhämtningslagen). Detsamma bör gälla vid särskild utlänningskontroll (21 a § LSU).

Regeringen instämmer med utredningen att det är lämpligt att de regler som nu redovisats görs tillämpliga genom hänvisningar i den nu föreslagna lagen.

12.1.3 Granskning, bevarande och förstörande av upptagningar och uppteckningar vid hemlig dataavläsning

Regeringens förslag: När hemlig dataavläsning används eller har använts under en förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation avseende granskning, bevarande och förstörande av upptagningar och uppteckningar även tillämpas vid hemlig dataavläsning. Det som gäller om hemlig rumsavlyssning ska dock tillämpas när hemlig dataavläsning används eller har använts för att läsa av eller ta upp rumsavlyssningsuppgifter.

När hemlig dataavläsning används eller har använts i underrättelseverksamhet ska de regler om granskning, bevarande och förstörande av upptagning och uppteckningar tillämpas som gäller vid förhindrande av vissa särskilt allvarliga brott respektive inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas

underrättelseverksamhet. Detsamma ska gälla vid särskild utlänningskontroll.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker förslaget eller kommenterar det inte närmare. *Säkerhets- och integritetsskyddsnämnden* anser att den nuvarande regleringen av i vilken utsträckning material från hemliga tvångsmedel får användas är otydlig. Det väcker frågan om den nuvarande regleringen är ändamålsenlig för hemlig dataavläsning.

Datainspektionen anser att det finns risk att bestämmelserna om förstörande av handlingar efter granskning kan leda till att en stor mängd uppgifter rutinmässigt bevaras under en längre tid. Därför anser Datainspektionen att det bör införas uttryckliga regler som anger att uppgifter som inte är relevanta för att utreda brott ska förstöras omedelbart efter att de har granskats.

Skälen för regeringens förslag

Nuvarande regler om granskning, bevarande och förstörande av upptagningar och uppteckningar

Det finns regler om granskning, bevarande och förstörande av upptagningar och uppteckningar vid användning av hemliga tvångsmedel (27 kap. 24 § RB, 13 § preventivlagen, 22 § LSU och 8 § inhämtningslagen). Dessa regler anger att upptagningar eller uppteckningar som har gjorts vid hemlig tvångsmedelsanvändning ska granskas snarast möjligt. De delar som är av betydelse från brottsutredningssynpunkt ska som huvudregel bevaras så länge de behövs för det ändamål för vilket de har samlats in, t.ex. för att förhindra brott.

Brottsbekämpande myndigheter får också behandla uppgifter från upptagningar och uppteckningar i enlighet med vad som är särskilt föreskrivet i lag. Det kan vara fallet om det har kommit fram uppgifter som, trots att de annars skulle ha förstörts, får behandlas i register eller på annat sätt enligt de förutsättningar som ställs upp i exempelvis lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område. Uppgifter från hemlig rumsavlyssning får dock behandlas endast om de rör förestående brott eller brott som kan föranleda beslut om hemlig rumsavlyssning eller annat brott, om det är föreskrivet fängelse i tre år eller mer för brottet (27 kap. 24 § tredje stycket RB, 13 § tredje stycket preventivlagen, 22 § andra stycket LSU, 8 § tredje stycket inhämtningslagen och prop. 2013/14:237 s. 129–130).

Granskning, bevarande och förstörande av upptagningar och uppteckningar vid hemlig dataavläsning

Enligt utredningen bör som utgångspunkt reglerna om granskning, bevarande och förstörande av upptagningar och uppteckningar vid hemlig dataavläsning följa de regler som gäller för sådan information för bakomliggande hemliga tvångsmedel. Regeringen delar, till skillnad från *Datainspektionen,* denna uppfattning. Eftersom reglerna skiljer sig åt beroende på om hemliga tvångsmedel används i förundersökningsverksamhet, underrättelseverksamhet eller vid särskild utlänningskontroll är det också

i detta sammanhang lämpligt att låta bestämmelser om granskning, bevarande och förstörande av upptagningar och uppteckningar utformas olika beroende på ändamålet med åtgärden. Regleringen avseende lagrade uppgifter och uppgifter som visar hur ett informationssystem används bör, som tidigare nämnts, motsvara vad som enligt rättegångsbalken gäller för hemlig avlyssning av elektronisk kommunikation.

När hemlig dataavläsning används under en förundersökning bör reglerna om granskning, bevarande och förstörande följa vad som gäller för hemlig avlyssning av elektronisk kommunikation (27 kap. 24 § RB).

Reglerna om granskning, bevarande och förstörande av upptagningar och uppteckningar för hemlig dataavläsning i underrättelseverksamhet bör motsvara vad som i dag gäller i underrättelseverksamhet och vid särskild utlänningskontroll (13 § preventivlagen, 22 § LSU och 8 § inhämtningslagen).

Säkerhets- och integritetsskyddsnämnden anser att den nuvarande regleringen är otydlig och att det därför kan ifrågasättas om den är lämplig att tillämpa även för hemlig dataavläsning. Nämnden pekar på att 27 kap. 24 § tredje stycket RB föreskriver att brottsutredande myndigheter – trots det som sägs i paragrafen om förstöring av material – får behandla uppgifter från upptagningar och uppteckningar i enlighet med vad som är särskilt föreskrivet i lag. Nämnden anser att det ger intryck av att uppgifter från material generellt får bevaras så snart uppgifterna får behandlas enligt registerlagstiftningen, t.ex. i underrättelseverksamhet, och att detta knappast kan ha varit lagstiftarens avsikt. Frågan om överskottsinformation har utretts av Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel (SOU 2018:61 s. 167–200). Betänkandet bereds i Regeringskansliet. Det finns inte skäl att här föregripa beredningen av det betänkandet. Trots den invändning som *Säkerhets- och integritetsskyddsnämnden* framför anser regeringen alltså att det finns skäl att införa motsvarande reglering för hemlig dataavläsning som för befintliga hemliga tvångsmedel.

12.1.4 Underrättelse till enskilda om hemlig dataavläsning

Regeringens förslag: Motsvarande regler som gäller för underrättelse till enskilda vid hemlig avlyssning av elektronisk kommunikation enligt rättegångsbalken och preventivlagen ska gälla vid hemlig dataavläsning när tvångsmedlet har använts i en förundersökning och i fall som avses i preventivlagen. Det som anges i de bestämmelserna om telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska i sådana fall avse avläsningsbart informationssystem. De särskilda regler om underrättelse till enskilda som gäller för hemlig kameraövervakning och hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller kameraövervaknings- och rumsavlyssningsuppgifter.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser yttrar sig inte över förslaget. Några, bl.a. *Åklagarmyndigheten* och *Civil Rights Defenders,* tillstyrker det.

Svenska Journalistförbundet anser att det borde finnas en obligatorisk skyldighet att informera personer som lyder under tystnadsplikt att de varit föremål för ett hemligt tvångsmedel.

Skälen för regeringens förslag: Som framgår av avsnitt 4.4.7 är huvudregeln att den som är eller har varit misstänkt för ett brott i efterhand ska underrättas om eventuell användning av hemliga tvångsmedel även om det finns undantag från denna underrättelseskyldighet. Tillsammans med andra rättssäkerhetsgarantier bidrar underrättelseskyldigheten till att uppfylla de krav som ställs i artikel 13 i Europakonventionen om rätten till effektiva rättsmedel.

De regler som gäller för underrättelse till enskilda är väl avvägda och har bl.a. i betänkandet Rättssäkerhetsgarantier och hemliga tvångsmedel ansetts förenliga med regeringsformen och Europakonventionen (SOU 2018:61 s. 223–229). Samma bedömning har gjorts i förhållande till EU-rätten när det gäller hemlig övervakning av elektronisk kommunikation vid förundersökning och vid tillämpning av preventiva tvångsmedel. Även avsaknaden av underrättelseskyldighet vid särskild utlänningskontroll och vid inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet har ansetts förenlig med EU-rätten (prop. 2018/19:86 s. 78–83 och bet. 2018/19:JuU27).

Underrättelseskyldighet bör, som utredningen föreslår, gälla för hemlig dataavläsning på samma sätt som för befintliga hemliga tvångsmedel. Det finns inte skäl att, som *Svenska Journalistförbundet* föreslår, införa en längre gående underrättelseskyldighet än vad som gäller för befintliga tvångsmedel. Det bör alltså vid hemlig dataavläsning under förundersökning och i preventivlagsfallen finnas samma underrättelseskyldighet som vid hemlig avlyssning av elektronisk kommunikation enligt rättegångsbalken respektive preventivlagen. När hemlig dataavläsning används för att hämta in kameraövervaknings- eller rumsavlyssningsuppgifter bör det gälla motsvarande skyldigheter som i dag gäller för hemlig kameraövervakning respektive hemlig rumsavlyssning. I bakomliggande tvångsmedel, både i rättegångsbalken och preventivlagen, föreskrivs en skyldighet att underrätta innehavaren till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning som en åtgärd vidtagits i, även om den personen inte är misstänkt. Samma skyldighet bör gälla vid hemlig dataavläsning. Verkställighet av hemlig dataavläsning avser emellertid inte ett telefonnummer, en annan adress eller en viss elektronisk kommunikationsutrustning utan i stället ett avläsningsbart informationssystem. Det bör därför, när det hänvisas till bestämmelser i rättegångsbalken om underrättelse till enskild, tydliggöras att det i sådana fall är avgörande vem som innehar det avläsningsbara informationssystemet och att det är den personen som ska underrättas. När begreppen telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning används avses därför begreppet avläsningsbart informationssystem. Det bör anges i den föreslagna lagen.

12.1.5 Parlamentarisk kontroll

Regeringens bedömning: Regeringen bör till riksdagen redovisa de brottsbekämpande myndigheternas användning av hemlig dataavläsning.

Utredningen lämnar inte någon uttrycklig bedömning i frågan.

Remissinstanserna: *Justitiekanslern* betonar att det är viktigt att planera för utvärderingen och säkra kontinuerlig tillgång till nödvändiga data redan när lagen träder i kraft. *Stiftelsen för internetinfrastruktur (Internetstiftelsen)* uppmanar regeringen att lägga till information om både hemlig dataavläsning och andra införda tvångsåtgärder i den årliga redovisningen till riksdagen om användningen av hemliga tvångsmedel för att erbjuda en möjlighet att i efterhand analysera nyttoeffekter.

Skälen för regeringens bedömning: Regeringen lämnar årligen en skrivelse om användningen av hemliga tvångsmedel till riksdagen (se avsnitt 4.7). Redovisningen innefattar tillämpningen av reglerna om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning vid förundersökning i brottmål samt tillämpningen av reglerna i preventivlagen och inhämtningslagen. Vid sidan av andra rättssäkerhetsgarantier, t.ex. domstolsprövning, fyller denna parlamentariska kontroll en viktig funktion och bidrar till allmänhetens insyn i myndigheternas tvångsmedelsanvändning.

Hemlig dataavläsning innebär ett allvarligt integritetsintrång för den som utsätts för åtgärden. Det finns därför som *Internetstiftelsen* påtalar skäl att låta den parlamentariska granskningen omfatta även hemlig dataavläsning. En sådan granskning bidrar även till att det finns tillgång till nödvändiga data för utvärderingen av lagen inför ställningstagande om den ska permanentas, vilket *Justitiekanslern* lyfter som angeläget. Regeringen har därför för avsikt att inkludera uppgifter om myndigheternas användning av hemlig dataavläsning i den årliga skrivelsen med redovisning av användningen av hemliga tvångsmedel.

12.2 Frågor om tillsyn, medverkan, sekretess och andra särskilda bestämmelser

12.2.1 Tillsyn över hemlig dataavläsning

Regeringens förslag: När rätten har beslutat i frågor om hemlig dataavläsning ska den underrätta Säkerhets- och integritetsskyddsnämnden om beslutet.

Regeringens bedömning: Det som redan gäller för Säkerhets- och integritetsskyddsnämndens tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel bör gälla även användning av hemlig dataavläsning enligt den föreslagna lagen. Det krävs inte några kompletterande bestämmelser för att nämnden ska kunna utöva sin tillsyn.

Utredningens förslag och bedömning överensstämmer delvis med regeringens. Utredningen föreslår att Säkerhets- och integritetsskyddsnämnden ska underrättas endast när tillstånd till hemlig dataavläsning har beviljats.

Remissinstanserna: Majoriteten av remissinstanserna tillstyrker förslaget och bedömningen eller kommenterar det inte särskilt. *Justitiekanslern* anser att den externa tillsynen är en av flera ändamålsenliga kontrollfunktioner för att så långt som möjligt värna om den personliga integriteten. *Säkerhets- och integritetsskyddsnämnden* tillstyrker att nämnden ska utöva tillsyn över användningen av hemlig dataavläsning. Nämnden anser dock att underrättelseskyldigheten till nämnden bör omfatta beslut om såväl avslag som tillstånd. Nämnden anför vidare att utredningen förutsätter en mer aktiv tillsyn än vad som är fallet med övriga tvångsmedel, där granskningen är av rättslig art och görs i efterhand genom uttalanden. Nämnden anför också att det vore önskvärt med en dokumentationsskyldighet av material som förstörts efter verkställighet eftersom nämndens granskning redan i dagsläget försvåras av att vidtagna åtgärder och överväganden inte har dokumenterats. *Civil Rights Defenders* tillstyrker förslaget men anser att Säkerhets- och integritetsskyddsnämnden borde få utöva tillsyn redan under pågående verkställighet för att kunna få en uppfattning om de brottsbekämpande myndigheterna följer lagens regler om vad som får göras under genomförandefasen.

Myndigheten för samhällsskydd och beredskap anför att det saknas förslag om hur vidtagna åtgärder ska dokumenteras. En väl utförd dokumentation är nödvändig för att inte bara möjliggöra effektiv tillsyn över hemliga dataavläsning utan även tillvarata erfarenheter och utveckla arbetssätt.

Skälen för regeringens förslag och bedömning: Säkerhets- och integritetsskyddsnämnden har till uppgift att inom sitt tillsynsområde bidra till att värna rättssäkerheten och skyddet för den personliga integriteten i förhållande till den brottsbekämpande verksamheten.

Nämnden har enligt 1 och 2 §§ lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (tillsynslagen) till uppgift att genom inspektioner och andra undersökningar utöva tillsyn över de brottsbekämpande myndigheternas användning av bl.a. hemliga tvångsmedel och vissa brottsbekämpande myndigheters personuppgiftsbehandling. Tillsynen ska särskilt syfta till att säkerställa att de brottsbekämpande myndigheternas verksamhet bedrivs i enlighet med lag och andra författningar.

Nämnden är enligt 3 § tillsynslagen skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel och om användningen av tvångsmedel och därmed sammanhängande verksamhet har skett i enlighet med lag eller annan författning. Om nämnden finner att någon tvångsmedelsanvändning inte har förekommit eller att sådan användning visserligen förekommit men att den är författningsenlig, får den enskilde besked av nämnden att kontrollen har utförts. Om nämnden vid kontroll upptäcker att hemliga tvångsmedel har använts i strid med gällande författningar ska den person som har begärt kontrollen underrättas även om detta. Nämnden är då också skyldig att efter omständigheterna anmäla det till Justitiekanslern, Åklagarmyndigheten, Datainspektionen eller någon annan behörig myndighet för åtgärd. Nämnden får göra sådan anmälan till Justitiekanslern även om kontroll inte begärts av den enskilde (20 §

förordningen [2007:1141] med instruktion för Säkerhets- och integritetsskyddsnämnden). Nämndens verksamhet har utvärderats och har ansetts utgöra en väl fungerande kontrollmekanism. Tillsynen har ansetts leda till efterlevnad hos de brottsbekämpande myndigheterna (se t.ex. Riksrevisionen rapport En granskning av Säkerhets- och integritetsskyddsnämnden, RiR 2016:2 s. 8 och 10–11 och SOU 2012:44 s. 667).

Åtgärderna som får vidtas inom ramen för hemlig dataavläsning kan i stor utsträckning ses som en förlängning av nuvarande hemliga tvångsmedel. De nya delarna av hemlig dataavläsning (avläsning eller upptagning av lagrade uppgifter eller uppgifter som visar hur ett informationssystem används) är inte väsensskilda från existerande tvångsmedel och tillsynen över sådan användning bör också kunna hanteras av nämnden. Det är därför rimligt att Säkerhets- och integritetsskyddsnämnden, som också tillstyrker förslaget i denna del, bör utses att vara tillsynsmyndighet över användningen av hemlig dataavläsning. Det behövs inte några författningsändringar för att nämnden ska ha befogenhet att utöva tillsyn eftersom det redan anges i tillsynslagen att nämnden ska utöva tillsyn över hemlig tvångsmedelsanvändning, vilket begrepp kommer att omfatta hemlig dataavläsning.

Nästa fråga är på vilket sätt tillsynen ska bedrivas och vilka uppgifter Säkerhets- och integritetsskyddsnämnden bör få del av. Regeringen konstaterar att nämndens frihet att själv välja hur och när den ska genomföra tillsyn av hemliga tvångsmedel bör gälla även för tillsynen av hemlig dataavläsning. Utredningen bedömer att det kan behövas en mer aktiv tillsyn vid hemlig dataavläsning än vad som är fallet vid tillsynen avseende övriga hemliga tvångsmedel och att tillsynen kan påbörjas redan under pågående verkställighet. Bedömningen grundar sig framför allt på de risker för informationssäkerheten som kan uppstå om de brottsbekämpande myndigheterna inte följer lagen. Bl.a. därför föreslår regeringen att det ska införas en bestämmelse om att Säkerhets- och integritetsskyddsnämnden ska underrättas om s.k. otillåten tilläggsinformation har tagits upp eller lästs av (avsnitt 11.2.2).

Utredningen föreslår att rätten ska underrätta Säkerhets- och integritetsskyddsnämnden om beviljade tillstånd till hemlig dataavläsning. *Säkerhets- och integritetsskyddsnämnden* anser dock att den har ett behov av att få del av även beslut om avslag på en ansökan om hemlig dataavläsning. Med hänsyn till att lagstiftningen är begränsad i tiden är det angeläget att för den kommande utvärderingen få en överblick över beslutsprocessen och hur de brottsbekämpande myndigheterna har följt lagen. Dessutom ger en mer omfattande underrättelseskyldighet ett bättre underlag för en effektiv tillsyn, varför regeringen instämmer i nämndens synpunkt. Det bör därför införas en bestämmelse som ålägger den domstol som har beslutat i frågor om hemlig dataavläsning att underrätta nämnden om beslutet, såväl bifall som avslag. Denna underrättelseskyldighet bör gälla samtliga beslut som rätten fattar om hemlig dataavläsning och således även t.ex. tilläggsbeslut om tillträdestillstånd. Det står nämnden fritt att själv bedöma vilka åtgärder, om några, den ska vidta med anledning av mottagna underrättelser. Genom införandet av bestämmelsen finns det förutsättningar för tillsyn även under pågående verkställighet, något som *Civil Rights Defenders* lyfter fram som önskvärt.

Myndigheten för samhällsskydd och beredskap och *Säkerhets- och integritetsskyddsnämnden* lyfter frågan om dokumentationsskyldighet vid myndigheternas beslut och åtgärder vid hemlig dataavläsning. Frågan om dokumentation avseende befintliga tvångsmedel övervägs i betänkandet Rättssäkerhetsgarantier och hemliga tvångsmedel (SOU 2018:61 s. 201 och 218–223). Betänkandet bereds i Regeringskansliet. Beredningen av det bör inte föregripas.

12.2.2 Medverkan vid verkställighet

Regeringens förslag: Den som bedriver anmälningspliktig verksamhet enligt lagen om elektronisk kommunikation ska vara skyldig att på begäran av den verkställande myndigheten medverka i samband med verkställigheten av hemlig dataavläsning.

Den operatör som medverkar har rätt till ersättning för de kostnader som uppstår. Kostnaderna ska betalas av den verkställande myndigheten.

Utredningens förslag överensstämmer inte med regeringens. Utredningen föreslår att den som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation får bistå den verkställande myndigheten i samband med verkställighet av hemlig dataavläsning.

Remissinstanserna: Många remissinstanser, bl.a. *Svea hovrätt, Göteborgs tingsrätt, Åklagarmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Skatteverket, Säkerhets- och integritetsskyddsnämnden* och *Myndigheten för samhällsskydd och beredskap*, motsätter sig att det endast införs en möjlighet för operatörerna att medverka vid verkställighet och anser att det finns en risk att operatörerna inte kommer att medverka om det är frivilligt. Därför föreslår de att det införs en skyldighet för operatörerna att bistå de brottsbekämpande myndigheterna. *Svea hovrätt* anser dessutom att det bör vara möjligt att förena medverkansskyldigheten med vitesföreläggande. *Säkerhets- och integritetsskyddsnämnden* tillägger att operatörerna enligt lagen om elektronisk kommunikation redan i dagsläget är skyldiga att bedriva verksamheten så att beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs. Nämnden anser därför att utredningens förslag skapar en omotiverad skillnad mellan regleringen om hemlig dataavläsning och redan gällande reglering.

Enligt *Åklagarmyndigheten* bör medverkansskyldigheten framgå av domstolens tillståndsbeslut och operatörerna bör ges en kopia av beslutet när verkställande myndigheterna begär deras medverkan. Sådan insyn i processen skulle öka förståelsen och motivera operatörerna att genomföra de åtgärder som domstolen har beslutat. *Polismyndigheten* och *Säkerhetspolisen* tillägger att regleringen om ersättning för samtliga tvångsmedel bör ses över. Säkerhetspolisen anser dessutom att en utebliven medverkansskyldighet kommer att innebära ökade kostnader för verkställande myndigheter, eftersom de kommer att behöva utveckla egen teknik för att ersätta operatörernas medverkan.

Lunds universitet (Juridiska fakulteten) anser att det inte finns tillräckliga skäl att avstå från att införa en skyldighet för operatörer att medverka vid verkställighet. Om inte en uttrycklig medverkansskyldighet införs bör det regleras på annat sätt hur de brottsbekämpande myndigheterna ska samverka med operatörer för att underlätta verkställighet.

Justitiekanslern, Malmö tingsrätt, Datainspektionen, Sveriges advokatsamfund, Civil Rights Defenders, Post- och telestyrelsen, Uppsala universitet (Juridiska fakulteten) och *Kungliga tekniska högskolan* är kritiska till att utredningen väljer en lagstiftningsteknik som ger operatörer möjlighet att medverka men anger i motiven att operatörerna måste medverka för att åtgärden ska kunna bli effektiv. Dessa remissinstanser anser att förslaget måste göras tydligare, oavsett vilken riktning det tar. *Uppsala universitet (Juridiska fakulteten)* tillägger att det kan framgå av utvärderingen av den tidsbegränsade lagstiftningen om det finns behov av specifika sanktioner för de operatörer som vägrar bistå vid verkställighet av hemlig dataavläsning.

Post- och telestyrelsen anför att det bör framgå av lagen hur operatörerna får behandla och lämna ut uppgifter som de har tillgång till och vad som gäller om tredje man drabbas av skada av de åtgärder som myndigheterna genomför. Det måste vidare stå klart vilka förväntningar som ställs på operatörerna och vad som händer om operatörerna inte uppfyller de krav som ställs vid verkställighet av hemlig dataavläsning. Styrelsen ser även behov av en tillsynsmyndighet som kan övervaka att operatörerna inte överskrider vad som är proportionerlig medverkan i det enskilda fallet. Det krävs dessutom en översyn av regelverket rörande integritetsskydd, lagring respektive inhämtning av uppgifter om elektronisk kommunikation för brottsbekämpande ändamål som föreslår en sammanhållen reglering av tillsyn och kontroll av regelverkets tillämpning. Även *Stiftelsen för internetinfrastruktur (Internetstiftelsen)* anser att de tekniska konsekvenserna för en operatör som medverkar vid verkställighet måste utredas närmare.

IT&Telekomföretagen, Com Hem AB och *HI3G Access AB* anser att det finns stora risker med förslaget och att det kan ifrågasättas om operatörer aktivt vill medverka till att släppa in okända virus och spionprogram i deras nät och utrustning. Om svenska operatörer ska medverka aktivt krävs att de ges tillräcklig insyn i den teknik som används så att de självständigt kan bedöma vilka risker det innebär. Dessutom bör relevanta myndigheter kopplas in för att avgöra om riskerna är godtagbara.

Slutligen anser *Telia Company AB* och *Internetstiftelsen* att förslaget är problematiskt eftersom det innebär att det överlämnas åt operatören att besluta om domstolens beslut ska verkställas eller inte, vilket inte bör vara en uppgiftför privata aktörer.

Skälen för regeringens förslag

Behovet av en aktiv medverkan vid verkställighet av hemlig dataavläsning

Utredningen redogör för att hemlig dataavläsning i vissa fall förutsätter en aktiv medverkan från teleoperatörer för att kunna genomföras. Med begreppet operatörer avses de som tillhandahåller allmänt tillgängliga elektroniska kommunikationsnät och kommunikationstjänster (2 kap. 1 § lagen om elektronisk kommunikation). Medverkan vid verkställighet kan t.ex.

handla om att operatörerna bistår de brottsbekämpande myndigheterna med att identifiera vilka tjänster en specifik användare har och vilka förbindelser som används och ger råd om vilka tekniska hjälpmedel som kan användas. Dessutom kan operatörerna ge möjlighet att installera brottsbekämpande myndigheters tekniska hjälpmedel och ansluta dem till operatörernas nät. En aktiv medverkan kan också bestå i att ge den verkställande myndigheten möjlighet att t.ex. installera utrustning som aktivt påverkar och förändrar trafikflödet mellan den som ska vara föremål för hemlig dataavläsning och annan utrustning som denne kommunicerar med.

De brottsbekämpande myndigheterna har ett behov av operatörens medverkan för att kunna installera de tekniska hjälpmedel som ska användas vid hemlig dataavläsning på ett så effektivt, snabbt och säkert sätt som möjligt. Om en operatör inte medverkar när det behövs kommer verkställigheten av hemlig dataavläsning i vissa fall inte att kunna genomföras eller kräva tillstånd under betydligt längre tid. Det kan också leda till att mer komplicerade metoder behöver användas, vilket kan innebära att de tekniska hjälpmedel som föranleder minst risker i verkställighetsfasen inte kan användas. Det kan i förlängningen ge upphov till större risker för informationssäkerhet och den personliga integriteten än vad som annars hade uppstått.

De brottsbekämpande myndigheterna, bl.a. *Polismyndigheten, Säkerhetspolisen* och *Tullverket,* har genom särskilt yttrande i utredningen och i sina remissvar anfört att det är absolut nödvändigt med en lagstadgad skyldighet för operatörerna att medverka vid verkställighet av hemlig dataavläsning. Mot bakgrund av det fåtal fall av hemlig dataavläsning som kan förväntas har de dock bedömt att det inte är nödvändigt med en anpassningsskyldighet för operatörerna, liknande den som finns i lagen om elektronisk kommunikation (6 kap. 19 §). Med anpassningsskyldighet avses att innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand.

Utredningen redogör för att hemlig dataavläsning i många fall borde kunna verkställas utan medverkan från operatörerna. Det finns dock enligt regeringen goda skäl att tro att verkställigheten i enskilda fall kommer att kräva en aktiv medverkan och att resultatet annars skulle försämras betänkligt. Det är därför nödvändigt att ta ställning till om det bör införas en skyldighet till medverkan eller bara en möjlighet till detta.

En regel om medverkansskyldighet införs

Utredningen föreslår att det ska införas en möjlighet för teleoperatörer att medverka vid verkställighet. Ställningstagandet bygger bl.a. på att operatörerna har ett samhällsansvar att bistå de brottsbekämpande myndigheterna och att det med de regler om personlig integritet och informationssäkerhet som föreslås saknas skäl för operatörerna att avstå från att medverka. Utredningen anser att en skyldighet att medverka skulle utgöra ett alltför stort intrång i operatörernas verksamhet. Många remissinstanser, bl.a. *Polismyndigheten*, *Säkerhetspolisen* och *Åklagarmyndigheten*, ifrågasätter utredningens resonemang i den delen. Som *Säkerhets- och integritetsskyddsnämnden* framhåller skulle en ordning som bygger på frivillighet inte stämma överens med regelverket för de bakomliggande tvångsmedlen, där operatörerna är skyldiga att bedriva sin verksamhet så

att verkställighet av hemlig avlyssning och övervakning av elektronisk kommunikation ska kunna verkställas. Som framförs av bl.a. *Justitiekanslern, Malmö tingsrätt* och *Datainspektionen* framstår det också som inkonsekvent att införa en möjlighet för operatörerna att medverka men indirekt kräva deras medverkan för att verkställigheten ska lyckas. *Telia Company AB* och *Internetstiftelsen* invänder mot att den föreslagna lösningen innebär att det överlämnas åt operatören att besluta om domstolens beslut ska verkställas eller inte, vilket inte bör vara en uppgift för privata aktörer. Som framgår av remisskritiken finns det både principiella och praktiska invändningar mot utredningens förslag. Regeringen delar de tveksamheter som många remissinstanser ger uttryck för inför en frivillig medverkan. Att införa en medverkansskyldighet är dessutom väl förenligt med det samhällsansvar som följer med den bedrivna verksamheten, se propositionerna Teleoperatörernas skyldigheter vid hemlig teleavlyssning och hemlig teleövervakning (prop. 1995/96:180 s. 29–30) och Lagring av trafikuppgifter för brottsbekämpande ändamål (prop. 2010/11:46 s. 66–68).

Mot denna bakgrund gör regeringen en annan bedömning än utredningen och föreslår en skyldighet för operatörer att medverka vid verkställighet. De ingrepp som de brottsbekämpande myndigheterna vidtar hos den enskilde operatören ska dock, precis som övriga åtgärder, vara proportionerliga och tekniken ska vara anpassad efter vilka slags uppgifter som ska läsas av eller tas upp. Det är också en förutsättning att informationssäkerheten utanför de informationssystem som blir föremål för hemlig dataavläsning inte åsidosätts, minskas eller skadas till följd av verkställigheten (se avsnitt 11.2.1 – 11.2.3). Regeringen delar därmed inte *IT&Telekomföretagen* och *Com Hem AB:s* uppfattning att förslaget om medverkansskyldighet innebär sådana risker att det inte bör genomföras.

Regeringen anser, liksom utredningen, att det med hänsyn till det begränsade antal fall av hemlig dataavläsning det förväntas bli fråga om inte finns skäl att i nuläget införa en anpassningsskyldighet för operatörerna i likhet med den som finns i 6 kap. 19 § lagen om elektronisk kommunikation.

Frågan om medverkan väcks, precis som redan är fallet vid annan tvångsmedelsanvändning, lämpligen av den verkställande myndigheten när den konstaterat att operatörens medverkan i något avseende behövs för att kunna verkställa åtgärden. *Post- och telestyrelsens* synpunkt att det bör regleras hur operatörerna behandlar informationen som kommit fram vid hemlig dataavläsning och att det bör finnas en tillsynsmyndighet som övervakar proportionaliteten av åtgärderna återkommer regeringen till i avsnitten om tillsyn, sekretess och tystnadsplikt (se avsnitt 12.2.1 och 12.2.3). Det föreslås också bestämmelser om aktsamhetskrav (se avsnitt 11.2.3) som säkerställer att olägenhet eller skada inte får förorsakas utöver vad som är absolut nödvändigt. Detta gäller även i förhållande till operatörer som medverkar vid verkställighet. Regeringen ser således inte något behov av att införa bestämmelser om vad som ska gälla om tredje man drabbas av skada, som Post- och telestyrelsen föreslår. Det kan här noteras att det i 3 kap. skadeståndslagen (1972:207) finns bestämmelser om statens skadeståndsskyldighet vid fel eller försummelse vid myndighetsutövning. Inte heller finns det anledning att särskilt reglera att operatörer ska hållas ansvarsfria, vilket också Post- och telestyrelsen föreslår.

Regeringen ser i nuläget inte behov av att införa en bestämmelse om vite eller andra sanktioner om medverkansskyldigheten inte följs, som bl.a. *Svea hovrätt* föreslår. Inte heller finns det skäl att införa bestämmelser om att operatören ska få del av beslutet, som *Åklagarmyndigheten* föreslår. Sådana frågeställningar kan det dock finnas anledning att återkomma till vid en kommande utvärdering av den tillfälliga lagstiftningen.

När det gäller frågan om ersättning för medverkan bör, som i befintliga tvångsmedel, den verkställande myndigheten betala ersättning till operatören för de faktiska kostnader som uppstår vid medverkan. En bestämmelse om det bör därför införas i lagen. *Polismyndigheten*, *Säkerhetspolisen* och till viss del *Post- och telestyrelsen* påpekar att en översyn behövs av den ersättning som utbetalas av brottsbekämpande myndigheter. Det är dock en fråga som det inte finns underlag för att behandla i detta lagstiftningsarbete.

12.2.3 Sekretess, tystnadsplikt och partsinsyn

Regeringens förslag: Vid hemlig dataavläsning ska tystnadsplikten ha företräde framför rätten att meddela och offentliggöra uppgifter när det gäller intresset av att förebygga eller beivra brott.

Vid internationellt rättsligt samarbete i fråga om hemlig rumsavlyssning och hemlig dataavläsning ska tystnadsplikten ha företräde framför rätten att meddela och offentliggöra uppgifter.

Den som i samband med verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen om elektronisk kommunikation har fått del av eller tillgång till en uppgift som hänför sig till användning av hemlig dataavläsning, får inte obehörigen föra vidare eller utnyttja det han eller hon fått del av eller tillgång till. Sådan tystnadsplikt ska ha företräde framför rätten att meddela och offentliggöra uppgifter.

Regeringens bedömning: Nuvarande sekretessregler till skydd för både intresset av att förebygga eller beivra brott och intresset av enskildas personliga och ekonomiska förhållanden ger adekvat skydd för de uppgifter om hemlig dataavläsning som kan behöva hemlighållas. Någon ändring av dessa bör därför inte göras. Inte heller bör det göras någon ändring av reglerna om kollision mellan rätten till partsinsyn och sekretessbestämmelserna.

Utredningens förslag och bedömning överensstämmer med regeringens.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget i denna del. *Säkerhets- och integritetsskyddsnämnden* motsätter sig inte att det införs en bestämmelse om tystnadsplikt för de operatörer som medverkar vid verkställighet men anser att bestämmelsen borde placeras i lagen om elektronisk kommunikation i stället. Nämnden anser också att som en konsekvens av att lagen om hemlig dataavläsning tidsbegränsas så bör även ändringarna i offentlighets- och sekretesslagen tidsbegränsas på motsvarande sätt. Det finns annars risk för att det kommer att finnas bestämmelser om hemlig dataavläsning som kommer att gälla oavsett om den tidsbegränsade lagen upphör att gälla. Även *Uppsala*

universitet (Juridiska fakulteten) anser att ändringarna i de övriga föreslagna lagarna bör tidsbegränsas.

Skälen för regeringens förslag och bedömning

Sekretess och rätten att meddela och offentliggöra uppgifter

Det finns ett antal sekretessregler i offentlighets- och sekretesslagen till skydd för intresset av att förebygga och beivra brott. Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott, om det kan antas att syftet med åtgärderna motverkas eller den framtida verksamheten skadas om uppgiften röjs. Sekretess gäller också för uppgifter i annan verksamhet, som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen (18 kap. 1 § OSL). Sekretess gäller vidare för uppgift som hänför sig till underrättelseverksamhet, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas (18 kap. 2 § OSL). Även hos myndigheter som biträder en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott gäller sekretess för dessa uppgifter (18 kap. 3 § OSL). Vidare finns bestämmelser om när sekretess ska gälla för uppgifter i verksamhet som avser rättsligt samarbete rörande förundersökning i brottmål eller tvångsmedel. Sekretess ska gälla i dessa fall om det kan antas att det varit en förutsättning för den andra statens eller den mellanfolkliga domstolens begäran att uppgiften inte skulle röjas (18 kap. 17 § OSL). Tystnadsplikten avseende användningen av hemliga tvångsmedel har, förutom när det gäller hemlig rumsavlyssning i internationella förhållanden, företräde framför rätten att meddela och offentliggöra uppgifter (18 kap. 19 § OSL samt 21 kap. 5 § och 21 kap. 8 § OSL för LSU-fallen).

Gällande reglering innebär alltså en tystnadsplikt som inskränker rätten att meddela och offentliggöra uppgifter, bl.a. när det är fråga om uppgifter som gäller användning av hemliga tvångsmedel. Att tystnadsplikt har företräde i dessa fall har motiverats bl.a. med att syftet med åtgärderna skulle kunna omintetgöras om uppgifterna kommer ut (se t.ex. prop. 2005/06:178 s. 81).

Det finns också sekretessregler till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott. Sekretess gäller bl.a. för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott eller annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen (35 kap. 1 § OSL). För dessa uppgifter har dock rätten att meddela och offentliggöra uppgifter företräde framför tystnadsplikten.

Partsinsyn

Den som är misstänkt för brott har som huvudregel rätt till insyn i och således rätt att få del av det som förekommit vid förundersökningen. Rätten till sådan insyn är central för den enskildes rättssäkerhet och möjligheter att på ett adekvat sätt försvara sig mot misstankar eller anklagelser. Att den som är misstänkt för brott snarast möjligt och fortlöpande får kännedom om resultaten av olika utredningsåtgärder är av stor betydelse för hans eller hennes möjligheter att på ett adekvat sätt försvara sig mot misstankarna. Han eller hon får också möjlighet att påkalla utredningsåtgärder, se t.ex. propositionen Misstänktas rätt till insyn i förundersökningar (prop. 2016/17:68 s. 32).

Den misstänktes insynsrätt inträder när han eller hon i samband med förhör underrättas om skälig misstanke om ett visst brott (23 kap. 18 § första stycket RB). Det finns vissa begränsningar i insynsrätten som innebär att uppgifter inte får lämnas ut till parten i den utsträckning det av hänsyn till allmänt eller enskilt intresse är av synnerlig vikt att sekretessbelagd uppgift i materialet inte röjs (10 kap. 3 § OSL). I sådana fall ska myndigheten på något annat sätt lämna parten upplysning om vad materialet innehåller i den utsträckning det behövs för att parten ska kunna ta till vara sin rätt och det kan ske utan allvarlig skada för det intresse som sekretessen ska skydda.

Sedan slutdelgivning gjorts har den misstänkte och försvararen rätt att ta del av det som har förekommit vid förundersökningen (23 kap. 18 a § RB). Det gäller även efter det att åtal har väckts och fram till dess att det slutligt har prövats eller saken annars slutligt har avgjorts. Även här finns dock begränsningar i partsinsynen enligt samma bestämmelser i offentlighets- och sekretesslagen (10 kap. 3 och 3 a §§OSL).

I ärenden om särskild utlänningskontroll gäller inte vad som sagts ovan. Rätten till insyn regleras i 14 § fjärde stycket LSU.

Det finns sekretessbestämmelser som redan omfattar hemlig dataavläsning

Utredningen bedömer att befintliga sekretessbestämmelser redan omfattar hemlig dataavläsning. Regeringen instämmer i den bedömningen. I offentlighets- och sekretesslagen finns nämligen, som redogörs för i det föregående, bestämmelser som reglerar sekretess under förundersökning och i underrättelseverksamhet samt regler om partsinsyn och förbehåll (18 kap. 1–3 och 17 §§, 10 kap. 3 och 3 a §§ och 35 kap. 1 § OSL). Dessa bestämmelser är generella och bedöms komma att gälla även för hemlig dataavläsning. På motsvarande sätt finns redan en särskild reglering avseende mål om särskild utlänningskontroll. Sekretesskyddet för hemlig dataavläsning bedöms därför vara fullgott.

Ändringar behövs när det gäller tystnadsplikten och rätten att meddela och offentliggöra uppgifter

Att tystnadsplikten har företräde framför rätten att meddela och offentliggöra uppgifter gäller för befintliga hemliga tvångsmedel (18 kap. 19 § OSL). Om det inte fanns en tystnadsplikt för dessa uppgifter skulle uppgifterna kunna få spridning och syftet med hemliga tvångsmedel kunna omintetgöras. Uppgifterna som kan inhämtas med hemlig dataavläsning

har samma sekretessbehov som befintliga tvångsmedel. Utredningen föreslår därför att hemlig dataavläsning ska omfattas av samma regler. Regeringen delar denna uppfattning. Hemlig dataavläsning bör därför läggas till i uppräkningen av övriga hemliga tvångsmedel i 18 kap. 19 § andra stycket OSL.

Hemlig dataavläsning bör dessutom tas upp i katalogen av tvångsmedel som kan användas enligt lagen om internationell rättslig hjälp i brottmål och i lagen om en europeisk utredningsorder (se avsnitt 13.1). Även i dessa fall finns en reglering i offentlighets- och sekretesslagen med innebörd att rätten att meddela och offentliggöra uppgifter får ge vika för tystnadsplikten när det gäller uppgifter hänförliga till det internationella rättsliga samarbetet (18 kap. 19 § tredje stycket). Hemlig dataavläsning bör behandlas på samma sätt som övriga hemliga tvångsmedel. Det finns därmed skäl att införa hemlig dataavläsning i regleringen, för att åtgärden ska kunna hemlighållas även när den användas i det internationella rättsliga samarbetet.

Utredningen noterar att hemlig rumsavlyssning inte omfattas av den nämnda bestämmelsen och att det framstår som svårförklarligt. Skillnaden har inte motiverats i förarbetena till hemlig rumsavlyssning eller till offentlighets- och sekretesslagen (prop. 2005/06:178 och prop. 2008/09:150). Utredningen bedömer därför att hemlig rumsavlyssning av förbiseende inte nämnts i 18 kap. 19 § tredje stycket OSL och föreslår att tystnadsplikten bör få företräde framför rätten att meddela och offentliggöra uppgifter även när det är fråga om hemlig rumsavlyssning vid internationella förhållanden. Det finns ett tydligt behov av en stark tystnadsplikt för uppgifter om användningen av hemliga tvångsmedel även när de används i det internationella rättsliga samarbetet. Det är inte tillfredsställande att uppgifter som rör hemlig rumsavlyssning inte täcks av det skydd som uppgifter om övriga hemliga tvångsmedel åtnjuter. Regeringen instämmer således i utredningens förslag.

En särskild regel om operatörernas tystnadsplikt införs

De operatörer som ska medverka vid verkställighet av hemlig dataavläsning omfattas inte av regleringen om tystnadsplikt i offentlighets- och sekretesslagen (18 kap. 1–3 och 17 §§). För hemlig avlyssning och övervakning av elektronisk kommunikation finns i stället särskilda bestämmelser i lagen om elektronisk kommunikation som ålägger operatörer tystnadsplikt (6 kap. 21 §). Regeringen föreslår nu en skyldighet för operatörer att medverka vid hemlig dataavläsning (se avsnitt 12.2.2). Om inte en liknande bestämmelse om tystnadsplikt införs avseende hemlig dataavläsning skulle det inte finnas något rättsligt hinder mot att operatörer offentliggör uppgifter om tvångsmedlet till obehöriga. Det skulle medföra stora risker för brottsbekämpningen och kunna omintetgöra syftet med tvångsmedlet om det blev känt t.ex. vem som är föremål för pågående hemlig dataavläsning eller vilka detaljerade åtgärder som vidtas. Behovet av att hålla vissa uppgifter hemliga är i många fall lika stort även efter det att åtgärden avslutats. Det finns sammantaget behov av en bestämmelse om tystnadsplikt. Bestämmelsen bör ta sikte på alla situationer då personer verksamma vid de företag som medverkar i samband med verkställighet

av hemlig dataavläsning får kännedom om uppgifter som hänför sig till åtgärden.

Bestämmelsen bör lämpligen utformas med 6 kap. 21 § lagen om elektronisk kommunikation som förebild. Regeringen föreslår därför att en bestämmelse om tystnadsplikt införs i lagen om hemlig dataavläsning som omfattar den som i samband med verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen om elektronisk kommunikation har fått del av eller tillgång till uppgift som hänför sig till angelägenhet som avser användning av hemlig dataavläsning och att den som tystnadsplikten gäller inte obehörigen får föra vidare eller utnyttja det han fått del av eller tillgång till. Bestämmelsen motsvarar därmed den sekretess som gäller enligt 18 kap. 1–3 och 17 §§ OSL och 6 kap. 21 § lagen om elektronisk kommunikation.

Säkerhets- och integritetsskyddsnämnden föreslår att bestämmelsen om tystnadsplikt vid hemlig dataavläsning ska placeras i lagen om elektronisk kommunikation. Eftersom det föreslås att medverkansbestämmelsen vid hemlig dataavläsning införs i den nu föreslagna lagen och inte i lagen om elektronisk kommunikation och det är just operatörernas medverkan vid hemlig dataavläsning som huvudsakligen medför att de får tillgång till information som bör skyddas av tystnadsplikt anser regeringen, i likhet med utredningen, att bestämmelsen om tystnadsplikt lämpligen bör införas i lagen om hemlig dataavläsning.

Inskränkningar i rätten att meddela och offentliggöra uppgifter

Utredningen föreslår att det i offentlighets- och sekretesslagen införs en bestämmelse som inskränker rätten att meddela och offentliggöra uppgifter som omfattas av den föreslagna bestämmelsen om tystnadsplikt för operatörer för uppgifter som hänför sig till hemlig dataavläsning. Utan en sådan sekretessregel skulle information om hemlig dataavläsning, som i många fall kan vara av mycket känslig natur, kunna spridas till obehöriga.

I 44 kap. offentlighets- och sekretesslagen finns bestämmelser som reglerar situationer där tystnadsplikt som följer av andra författningar än offentlighets- och sekretesslagen har företräde framför rätten att meddela och offentliggöra uppgifter, bl.a. 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 inhämtningslagen (4 § 3). Eftersom den bestämmelsen tar sikte på lagen om elektronisk kommunikation anser utredningen att en bestämmelse med inskränkningar i meddelarfriheten för uppgifter som hänför sig till hemlig dataavläsning inte bör införas där, utan i 44 kap. 5 § offentlighets- och sekretesslagen, som reglerar annan lagstiftning. Regeringen delar den uppfattningen.

Ändringarna i offentlighets- och sekretesslagen bör inte tidsbegränsas

Regeringen bedömer, till skillnad från *Säkerhets- och integritetsskyddsnämnden* och *Uppsala universitet (Juridiska fakulteten)*, att reglerna om hemlig dataavläsning i offentlighets- och sekretesslagen inte bör vara tidsbegränsade. Däremot, som anges i avsnitt 9.1, bör lagen om hemlig dataavläsning tidsbegränsas för att sedan utvärderas. En motsvarande lösning användes när hemlig kameraövervakning och hemlig rumsavlyssning

infördes (prop. 1995/96:85 och 2005/06:178). Skälen för en sådan lösning är huvudsakligen lagtekniska.

12.2.4 Kvalifikationskrav på den som ansvarar för verkställighet

Regeringens förslag: Den verkställande myndigheten ska utse en eller flera personer som får verkställa hemlig dataavläsning. Sådana personer ska vara särskilt lämpade för uppdraget och ha särskilda kunskaper om informationssäkerhet samt den särskilda kompetens, utbildning och erfarenhet som i övrigt är nödvändig.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna kommenterar inte förslaget. *Föreningen för digitala fri- och rättigheter* anser att utredningen visar en betydande okunnighet om verkligheten när den gör bedömningen att risken för spridning utanför den skara personer som känner till sårbarheterna på myndigheterna skulle vara synnerligen liten. Föreningen anser att risken för spridning är uppenbar.

Skälen för regeringens förslag: Eftersom hemlig dataavläsning är mer tekniskt komplicerat än många andra tvångsmedel och kan innebära särskilda risker för den personliga integriteten behöver det utses en eller flera personer som får verkställa av hemlig dataavläsning.

Det finns alltid en risk, så som *Föreningen för digitala fri- och rättigheter* påtalar, att den teknik som används för att verkställa hemlig dataavläsning sprids och utnyttjas av kriminella. Det är därför av yttersta vikt att sådana risker minimeras, inte minst eftersom verkställighetstekniken ofta kommer att handla om att utnyttja sårbarheter i informationssystem. I likhet med utredningen menar regeringen att ett sätt att minska risken för spridning är att endast en mycket begränsad mängd personer med rätt kompetens har kännedom om de tekniker som används vid hemlig dataavläsning. Förutom att en sådan lösning kommer att minska risken för spridning av de tekniker som används kommer den också att minska risken för spridning av information om eventuella sårbarheter i informationssäkerheten (se avsnitt 11.2.1 och 11.2.3). Det bör vara myndighetschefen som ansvarar för beslutanderätten om vilka som ska utses till detta uppdrag. Denna beslutanderätt bör kunna delegeras. Dem som utses behöver den kompetens, utbildning och erfarenhet som är nödvändig samt särskild kunskap om informationssäkerhet. Den utvalda personkretsen torde även behöva genomgå noggranna säkerhetskontroller. Till skillnad från Föreningen för digitala fri- och rättigheter anser regeringen härigenom att risken för spridning utanför den skara personer som känner till sårbarheterna är synnerligen liten.

En bestämmelse som reglerar utseende av, och kompetenskrav för, de personer som ska verkställa hemlig dataavläsning bör, som utredningen föreslår, införas i lagen.

12.2.5 Särskilda bestämmelser vid krig eller krigsfara

Regeringens förslag: Om riket är i krig eller krigsfara eller om det råder sådana utomordentliga förhållanden som beror på krig eller krigsfara och regeringen förordnar det ska tillstånd till hemlig dataavläsning av rumsavlyssningsuppgifter få ges av åklagaren i avvaktan på rättens beslut, om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna kommenterar inte förslaget. *Säkerhets- och integritetsskyddsnämnden* och *Uppsala universitet (Juridiska fakulteten)* anser dock att som en konsekvens av att lagen om hemlig dataavläsning tidsbegränsas så bör även ändringarna i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. tidsbegränsas på motsvarande sätt.

Skälen för regeringens förslag: Det finns särskilda bestämmelser som reglerar vad som ska gälla om Sverige är i krig, eller om det råder krigsfara eller utomordentliga förhållanden föranledda av krig eller av krigsfara som Sverige har befunnit sig i och regeringen så förordnar (2 § lagen [1988:97] om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.; lagen föreslås få ändrat namn, prop. 2018/19:262). Om förhållandena i landet är sådana att lagen är tillämplig och det i en situation då hemlig rumsavlyssning behövs kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till åtgärden, får tillstånd ges av åklagaren i avvaktan på rättens beslut (28 §). Möjligheten till interimistiska åklagarbeslut för övriga hemliga tvångsmedel regleras i rättegångsbalken och omfattas därför inte av den aktuella lagen (prop. 2013/14:237 s. 146 och 191–192).

Åklagare har inte en generell möjlighet att ge intermistiska beslut om hemlig rumsavlyssning. Under extraordinära omständigheter när riket är i krig eller krigsfara anses det dock finnas skäl att avvika från den huvudregeln. I likhet med vad utredningen föreslår anser regeringen att detta bör gälla även för hemlig dataavläsning avseende rumsavlyssningsuppgifter. En möjlighet till sådana interimistiska beslut bör därför införas i lagen. I likhet med vad som anges i avsnitt 12.2.3 beträffande ändringarna i offentlighets- och sekretesslagen bedömer regeringen, till skillnad från *Säkerhets- och integritetsskyddsnämnden* och *Uppsala universitet (Juridiska fakulteten),* att reglerna om hemlig dataavläsning i lagen inte bör vara tidsbegränsade (se avsnitt 12.2.3).

12.2.6 Rätt att meddela föreskrifter

Regeringens förslag: Det ska upplysas att regeringen eller den myndighet regeringen bestämmer kan meddela närmare föreskrifter om medverkan och ersättning vid verkställighet och om underrättelser som i vissa fall ska skickas till Säkerhets- och integritetsskyddsnämnden.

Utredningen lämnar inget förslag på upplysningsbestämmelse.

Remissinstanserna: *Polismyndigheten* och *Säkerhetspolisen* framför att det finns skäl att i föreskrifter reglera nivåerna för ersättning till den operatör som ska medverka vid verkställigheten. Övriga remissinstanser yttrar sig inte i frågan.

Skälen för regeringens förslag: Det föreslås att operatörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation ska vara skyldiga att medverka vid verkställighet och att de ska ha rätt till ersättning för kostnader som uppstår vid sådan medverkan (se avsnitt 12.2.2). Det kan uppstå behov av att meddela verkställighetsföreskrifter som preciserar medverkan och ersättningsskyldigheten. Det är härvid framför allt den närmare formen för operatörernas medverkan som kan behöva preciseras ytterligare samt de närmare nivåerna på ersättning som operatörerna kan ha rätt till vid sådan medverkan.

Regeringen föreslår också att Säkerhets- och integritetsskyddsnämnden ska underrättas om otillåten tilläggsinformation har tagits upp (se avsnitt 11.2.2). Den mer detaljerade utformningen av de underrättelser som ska lämnas till nämnden kan behöva regleras i form av verkställighetsföreskrifter.

13 Hemlig dataavläsning och internationella förhållanden

13.1 Det behövs regler om hemlig dataavläsning i det internationella straffrättsliga samarbetet

Regeringens bedömning: Det bör införas regler om hemlig dataavläsning både i lagen om internationell rättslig hjälp i brottmål och i lagen om en europeisk utredningsorder.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Ingen remissinstans har några invändningar mot utredningens bedömning. *Säkerhets- och integritetsnämnden* och *Uppsala universitet (Juridiska fakulteten)* anser att som en konsekvens av att lagen om hemlig dataavläsning tidsbegränsas så bör även ändringarna i bl.a. lagen om internationell rättslig hjälp tidsbegränsas på motsvarande sätt.

Skälen för regeringens bedömning: Den brottslighet som regeringen föreslår ska omfattas av reglerna om hemlig dataavläsning är inte sällan av gränsöverskridande natur. Vissa brottsutredningar förutsätter mer eller mindre rättsligt samarbete med andra stater, t.ex. vid grov narkotikabrottslighet, människohandel och terroristbrottslighet. Även i utredningar av mer nationell brottslighet kan det många gånger behövas bistånd utomlands, t.ex. om bevisningen finns i en annan stat. I detta samarbete används hemliga tvångsmedel vid allvarlig brottslighet. En given utgångspunkt är att all brottslighet – såväl nationell som internationell – ska bekämpas. De utredningsåtgärder som är möjliga att vidta i Sverige vid allvarlig brottslighet ska svenska åklagare kunna begära att de vidtas i en annan stat. På samma sätt ska utländska åklagare kunna begära att en motsvarande åtgärd

vidtas i Sverige. Detta talar för att det finns ett behov av särskilda regler beträffande hemlig dataavläsning i de lagar som reglerar det internationella rättsliga samarbetet.

Sedan den 1 december 2017 gäller lagen (2017:1000) om en europeisk utredningsorder i Sverige. Lagen genomför Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området. Lagen gäller gentemot alla medlemsstater i EU utom Danmark och Irland. Med en europeisk utredningsorder avses ett beslut i Sverige – eller i en annan medlemsstat – som innebär att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning i den andra medlemsstaten respektive Sverige. Åtgärden ska ha meddelats av – i huvudsak – en åklagare eller domstol under en utredning eller rättegång i brottmål. De utredningsåtgärder som är möjliga att vidta enligt lagen är bl.a. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning (1 kap. 4 §). Direktivets tillämpningsområde sätter inga gränser för vilka utredningsåtgärder som kan ingå i lagstiftningen, så länge det rör sig om en åtgärd som innebär bevisinhämtning. Tvärtom förutsätter direktivet att medlemsstaterna när det kommer en utredningsorder från ett annat land, kan tillhandahålla samtliga åtgärder som de nationella myndigheterna kan använda sig av. Även detta talar för att hemlig dataavläsning bör omfattas av de åtgärder som lagen avser.

I förhållande till övriga stater tillämpas lagen (2005:562) om internationell rättslig hjälp i brottmål (LIRB). Även om det inte föreligger en internationell förpliktelse att införa regler om hemlig dataavläsning är en uttalad målsättning med lagen att svenska åklagare och domstolar ska kunna lämna rättslig hjälp till utländska myndigheter med alla de åtgärder som kan vidtas vid en svensk förundersökning eller rättegång (prop. 1999/2000:61 s. 79–80). Av det skälet bör det införas regler om hemlig dataavläsning i lagen om internationell rättslig hjälp i brottmål.

Regeringens sammantagna bedömning är således, i likhet med utredningen, att det bör införas regler om hemlig dataavläsning i både lagen om internationell rättslig hjälp i brottmål och i lagen om en europeisk utredningsorder. Det bör dock noteras att vissa av de åtgärder som enligt svensk rätt kommer att utgöra hemlig dataavläsning i andra länder anses vara en metod för att verkställa ett hemligt tvångsmedel, t.ex. hemlig avlyssning av elektronisk kommunikation. Det kan medföra att den åtgärd som anges i en ansökan eller i en utredningsorder inte rubriceras på samma sätt i Sverige eller i andra länder. Det innebär att den åklagare som vill att en åtgärd ska vidtas i en annan stat måste ta hänsyn till detta när en ansökan eller utfärdad utredningsorder sänds över. På motsvarande sätt kan den åklagare som handlägger ett ärende om att en åtgärd ska vidtas i Sverige behöva göra en bedömning av om ansökan om rättslig hjälp eller en utredningsorder rör hemlig dataavläsning eller något annat hemligt tvångsmedel.

Regeringen bedömer till skillnad från *Säkerhets- och integritetsskyddsnämnden* och *Uppsala universitet (Juridiska fakulteten)* att reglerna om hemlig dataavläsning i de båda lagarna inte bör vara tidsbegränsade. Skälen till det är desamma som redovisas i avsnitt 12.2.3 om offentlighets- och sekretesslagen.

13.2 Hemlig dataavläsning enligt lagen om internationell rättslig hjälp i brottmål

13.2.1 Hemlig dataavläsning ska omfattas av lagen om internationell rättslig hjälp i brottmål

Regeringens förslag: I lagen om internationell rättslig hjälp i brottmål ska det införas bestämmelser om hemlig dataavläsning. Rättslig hjälp med hemlig dataavläsning ska lämnas under de förutsättningar som gäller för motsvarande åtgärd under en svensk förundersökning. Ett krav på dubbel straffbarhet ska ställas upp.

Tekniskt bistånd med och tillstånd till gränsöverskridande hemlig dataavläsning ska lämnas under de förutsättningar som följer av de särskilda bestämmelserna i lagen om internationell rättslig hjälp i brottmål. För tillstånd till gränsöverskridande hemlig dataavläsning ska ett krav på dubbel straffbarhet ställas upp.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: Hemlig dataavläsning finns inte med i förteckningen avseende vilka åtgärder som rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål (LIRB) omfattar. Hemlig dataavläsning bör mot bakgrund av vad som anges i föregående avsnitt anges som en åtgärd som omfattas av lagen genom ett tillägg.

På samma sätt som för övriga tvångsmedel bör rättslig hjälp med hemlig dataavläsning i Sverige lämnas under de förutsättningar som gäller för åtgärden i en svensk förundersökning. (2 kap. 1 § första stycket). Vidare bör det ställas upp ett krav på dubbel straffbarhet, dvs. den gärning som avses i den utländska brottsutredningen ska vara straffbar i Sverige (2 kap. 2 §).

I lagen finns även regler om tekniskt bistånd med och tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation som specifikt avser det internationella samarbetet (1 kap. 2 § första stycket 7 och 8). Bestämmelserna avser en ansökan om sådant bistånd och tillstånd såväl i Sverige som i utlandet.

Tekniskt bistånd innebär att meddelanden överförs omedelbart till den ansökande staten samt att dessa meddelanden avlyssnas och tas upp där och inte i den anmodade staten, som endast bistår i vissa tekniska avseenden. Biståndet går ut på att möjliggöra verkställighet av ett svenskt eller utländskt beslut om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. Tillstånd till gränsöverskridande hemlig avlyssning och hemlig övervakning av elektronisk kommunikation innebär att en stat medger att en annan stats myndigheter avlyssnar eller övervakar t.ex. en teleadress som finns på den förstnämnda statens territorium utan att något bistånd behövs från den staten. Tillståndet gör det möjligt för den avlyssnande staten att vidta eller fortsätta med åtgärden.

Motsvarande möjlighet bör även finnas för hemlig dataavläsning beträffande kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter (se avsnitt 13.2.2 och 13.2.3). Åtgärderna behöver därför föras

in i förteckningen i 1 kap. 2 § första stycket. På samma sätt som för tekniskt bistånd med och tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation ska hemlig dataavläsning beträffande dessa åtgärder lämnas under de förutsättningar som följer av de särskilda bestämmelser som finns i lagen om internationell rättslig hjälp i brottmål (2 kap. 1 § andra stycket). Detta mot bakgrund av att några motsvarande åtgärder inte finns för svensk förundersökning. När det gäller kravet på dubbel straffbarhet, dvs. att den gärning som ansökan avser ska motsvara ett brott enligt svensk lag (2 kap. 2 §) bör regleringen motsvara den som gäller i dag för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation. För tekniskt bistånd med hemlig dataavläsning bör inte något sådant krav ställas upp, men däremot för tillstånd till gränsöverskridande hemlig dataavläsning.

13.2.2 Hemlig dataavläsning i Sverige

Regeringens förslag: En ansökan om hemlig dataavläsning i Sverige ska handläggas 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 i motsvarande nationellt fall, själv besluta om åtgärden.

Upptagningar och uppteckningar som avser hemlig dataavläsning behöver inte granskas.

Om åklagaren har fattat beslut om hemlig dataavläsning ska återredovisning ske först sedan rätten fattat beslut om hemlig dataavläsning. Upptagningar och uppteckningar får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning skett endast om det är tillåtet i motsvarande nationellt fall.

I fråga om underrättelse till en enskild ska det som gäller vid rättslig hjälp med hemlig avlyssning och hemlig övervakning av elektronisk kommunikation tillämpas på motsvarande sätt vid hemlig dataavläsning.

Verkställighet av ett beslut om hemlig dataavläsning genom omedelbar överföring av meddelanden eller uppgifter om meddelanden samt tekniskt bistånd och tillstånd till gränsöverskridande hemlig dataavläsning ska endast få avse kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter. Vidare ska de regler som gäller för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation i motsvarande situation tillämpas vid hemlig dataavläsning. I stället för hänvisningar till vissa bestämmelser i rättegångsbalken, ska hänvisningar göras till lagen om hemlig dataavläsning.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att verkställighet av ett beslut om hemlig dataavläsning genom omedelbar överföring av uppgifter samt tekniskt bistånd med och tillstånd till gränsöverskridande hemlig dataavläsning även ska omfatta platsuppgifter.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 2 kap. LIRB finns – utöver de allmänna förutsättningarna för att lämna rättslig hjälp (se föregående avsnitt) – bestämmelser om rättslig hjälp i Sverige, t.ex. om förfarandet och när en ansökan ska avslås. Dessa regler kommer att bli tillämpliga även vid hemlig dataavläsning och något behov av ändringar finns inte (se dock nedan om tillägg till 2 kap 4 § om ansökans innehåll.)

I lagens fjärde kapitel finns särskilda bestämmelser om olika former av rättslig hjälp. De hemliga tvångsmedlen behandlas i 25–28 b §§. Det framstår som naturligt att införa nya bestämmelser om hemlig dataavläsning i direkt anslutning till dessa regler.

Det finns skäl att i så stor utsträckning som möjligt låta de gällande bestämmelserna om rättslig hjälp i Sverige med hemliga tvångsmedel bilda utgångspunkt vid utformningen av reglerna om rättslig hjälp med hemlig dataavläsning. Enligt samtliga dessa gäller att ansökan om rättslig hjälp avseende någon som befinner sig i Sverige handläggs av åklagare. Bestämmelserna anger även vilka uppgifter som ska framgå av ansökan. Det finns ingen anledning att avvika från detta vid hemlig dataavläsning. Samma skyndsamhetskrav som finns beträffande åklagarens prövning, vad en ansökan bör innehålla och överlämnande till rätten som gäller för de övriga tvångsmedlen bör gälla vid hemlig dataavläsning. Det bör därför föreskrivas att åklagaren genast ska pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd. När det gäller åklagarens möjlighet att besluta om åtgärden interimistiskt, vilken alltså finns för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning under de förutsättningar som gäller enligt rättegångsbalken, bör en hänvisning göras till bestämmelsen om sådant beslut i lagen om hemlig dataavläsning. Av en sådan hänvisning klargörs bl.a. att interimistiska beslut inte får avse hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter. Förslagen medför behov av en komplettering i 2 kap. 4 §.

För samtliga hemliga tvångsmedel enligt lagen om internationell rättslig hjälp gäller vidare att upptagningar eller uppteckningar inte behöver granskas i Sverige. Det ligger nämligen i sakens natur att svenska myndigheter, som på begäran av en annan stat genomför åtgärderna, inte vid en granskning av materialet kan bedöma vad som är av intresse för den andra statens brottsutredning, se propositionen Internationell rättslig hjälp i brottmål (prop. 2004/05:144 s. 170). Samma bör gälla vid rättslig hjälp med hemlig dataavläsning.

Det bör vidare, liksom enligt 4 kap. 25 och 27 §§, framgå att om åklagaren har fattat beslut om hemlig dataavläsning får återredovisning till det ansökande landet inte ske förrän domstol fattat beslut att tillåta åtgärden. Dessutom bör det av bestämmelsen framgå att upptagningar och uppteckningar endast får bevaras när ärendet avslutats och återredovisning skett om det är tillåtet i motsvarande inhemska förfarande.

När det gäller underrättelse till enskilda bör samma sak gälla vid rättslig hjälp med hemlig dataavläsning som gäller vid rättslig hjälp med övriga hemliga tvångsmedel enligt lagen. Det kan enklast åstadkommas genom en direkt hänvisning till vad som gäller för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 § tredje stycket.

För hemlig avlyssning och hemlig övervakning av elektronisk kommunikation finns vissa särskilda åtgärder som är specifika för det internationella samarbetet. De åtgärder som avses är verkställighet av ett beslut om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation genom omedelbar överföring av meddelanden eller uppgifter om meddelanden samt tekniskt bistånd med och tillstånd till gränsöverskridande hemlig avlyssning och övervakning av elektronisk kommunikation. Reglerna grundar sig ursprungligen på 2000 års konvention om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater. Konventionen genomfördes genom propositionen Internationell rättslig hjälp i brottmål: Tillträde till 2000 års EU-konvention m.m. (prop. 2004/05:144).

Verkställighet genom omedelbar överföring av meddelanden eller uppgifter om meddelanden innebär att meddelandena eller uppgifterna om meddelandena överförs direkt till den ansökande staten (4 kap. 25 a § LIRB). Någon upptagning eller uppteckning görs inte i Sverige. En förutsättning är att en överföring kan göras under betryggande former. Genom tekniskt bistånd överförs meddelanden eller uppgifter om meddelanden omedelbart som ovan men skillnaden gentemot omedelbar överföring enligt 4 kap. 25 a § är att den avlyssnade telefonen finns i den ansökande staten eller en tredje stat (4 kap. 25 b §). Det är alltså inte fråga om någon avlyssning av en utrustning i Sverige. Tillstånd till gränsöverskridande hemlig avlyssning eller övervakning av elektronisk kommunikation innebär att Sverige tillåter en annan stat – som har kapaciteten – att avlyssna eller övervaka en kommunikationsutrustning som finns i Sverige (4 kap. 26 a och 26 b §§).

EU-konventionen tar visserligen sikte på avlyssning av telemeddelanden men avsikten är att begreppet ska tolkas brett och utifrån hur kommunikationstekniken utvecklas (prop. 2004/05:144 s. 93). Eftersom hemlig dataavläsning i praktiken kommer att vara ett nytt sätt att verkställa hemlig avlyssning och hemlig övervakning av elektronisk kommunikation bör motsvarande gälla för hemlig dataavläsning beträffande verkställighet av ett beslut om hemlig dataavläsning genom omedelbar överföring av uppgifter om meddelanden samt tekniskt bistånd med och tillstånd till gränsöverskridande hemlig dataavläsning.

När det sedan gäller tillämpningsområdet för bestämmelserna om verkställighet genom omedelbar överföring av meddelanden eller uppgifter om meddelanden samt tekniskt bistånd med och tillstånd till gränsöverskridande hemlig avlyssning och övervakning av elektronisk kommunikation omfattade hemlig övervakning av elektronisk kommunikation, vid tidpunkten för genomförandet, endast uppgifter motsvarande platsuppgifter (lokaliseringsuppgifter) i samband med kommunikation. Möjligheten till hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § första stycket 2 och 3 rättegångsbalken för att hämta in uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits existerade inte då. Genom propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation (prop. 2011/12:55) infördes möjligheten att inhämta dessa specifika uppgiftstyper genom hemlig övervakning av elektronisk kommunikation. I det internationella regelverket fick detta dock endast genomslag i huvudregeln i 4 kap. 25 § LIRB, som

reglerar att rättslig hjälp kan ges med hemlig avlyssning och hemlig övervakning av elektronisk kommunikation av någon som befinner sig i Sverige. Uppgifterna kan då hämtas in på sedvanligt sätt och lämnas över till den ansökande staten. Några ändringar gjordes emellertid inte i 4 kap. 25 a och 25 b §§ om verkställighet genom omedelbar överföring av meddelanden och uppgifter om meddelanden respektive tekniskt bistånd med hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. Dessa bestämmelser omfattar, vad avser hemlig övervakning av elektronisk kommunikation endast uppgifter enligt 27 kap. 19 § första stycket 1 rättegångsbalken

Inte heller bestämmelserna om tillstånd till gränsöverskridande hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation ändrades i samband med att hemlig övervakning av elektronisk kommunikation utvidgades till att omfatta nya typer av platsuppgifter. Visserligen preciseras inte i 4 kap. 26 a § LIRB att tillstånd till gränsöverskridande hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation endast kan avse meddelanden eller uppgifter om meddelanden, vilket däremot gjordes i den omvända situationen, dvs. när svenska åklagare i en annan stat begär tillstånd till gränsöverskridande hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation (se 4 kap. 26 c §). Anledningen till detta var att i förhållande till en annan stats regler om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation ha en mer teknikneutral reglering. Dessutom kan påpekas att dessa bestämmelser baserar sig på en och samma artikel i EU-konventionen (artikel 20) och ska hanteras reciprokt, dvs. svenska åklagare ska inte ha färre möjligheter till gränsöverskridande åtgärder i nu aktuellt avseende än myndigheter i andra stater. Tillämpningsområdet för 4 kap. 26 a § får därför endast anses omfatta, vad gäller hemlig övervakning av elektronisk kommunikation, uppgifter om meddelanden enligt 27 kap. 19 § första stycket 1 rättegångsbalken. Eftersom platsuppgifter enligt 27 kap. 19 § första stycket 2 och 3 rättegångsbalken inte omfattas av gällande bestämmelser om verkställighet genom omedelbar överföring av uppgifter om meddelanden eller tekniskt bistånd med eller tillstånd till gränsöverskridande hemlig övervakning av elektronisk kommunikation, bör dessa uppgifter inte omfattas när motsvarande åtgärder blir aktuella vid hemlig dataavläsning.

Regeringen anser därför till skillnad från utredningen att verkställighet av ett beslut om hemlig dataavläsning genom omedelbar överföring av uppgifter eller tekniskt bistånd med eller tillstånd till gränsöverskridande hemlig dataavläsning, endast bör få avse kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter. I stället för hänvisningar till rättegångsbalken bör hänvisningar göras till motsvarande bestämmelser i lagen om hemlig dataavläsning. Det ska dock påpekas att de uppgifter som nu är aktuella, dvs. hemlig dataavläsning som gäller platsuppgifter, kan den andra staten få tillgång till genom att uppgifterna tas upp i Sverige för att sedan överlämnas till den andra staten.

13.2.3 Hemlig dataavläsning som gäller någon i utlandet

Regeringens förslag: Vid rättslig hjälp och tekniskt bistånd med hemlig dataavläsning i en annan stat ska motsvarande bestämmelser som

gäller vid rättslig hjälp och tekniskt bistånd med hemlig avlyssning och hemlig övervakning av elektronisk kommunikation tillämpas. Detsamma gäller vid tillstånd till gränsöverskridande hemlig dataavläsning i utlandet. Tekniskt bistånd med och tillstånd till gränsöverskridande hemlig dataavläsning ska endast få avse kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter.

Om en underrättelse till en enskild ska lämnas, ska motsvarande bestämmelser i den föreslagna lagen om hemlig dataavläsning tillämpas.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att tekniskt bistånd med och tillstånd till gränsöverskridande hemlig dataavläsning, även ska omfatta platsuppgifter.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 4 kap. 26 § LIRB finns bestämmelser om att åklagare kan ansöka om rättslig hjälp och tekniskt bistånd med hemlig avlyssning och hemlig övervakning av elektronisk kommunikation av någon som befinner sig i en annan stat eller i Sverige. Vidare anges det i bestämmelsen att om den anmodade staten kräver att åklagarens ansökan först ska prövas av domstol i Sverige får en svensk domstol, på åklagarens begäran, pröva frågan om att tillåta hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. Därutöver finns uttryckliga bestämmelser om vad en ansökan ska innehålla. Motsvarande bestämmelser bör gälla för rättslig hjälp och tekniskt bistånd med hemlig dataavläsning utomlands. Några skäl för en avvikande reglering finns inte. Däremot bör tekniskt bistånd med hemlig dataavläsning endast kunna avse kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter, med hänsyn till att nuvarande bestämmelser om tekniskt bistånd vid hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation, vilka baserar sig på EU-konventionen, inte omfattar fler uppgifter än dessa (se resonemanget i avsnitt 13.2.2).

I 4 kap. 26 § fjärde stycket finns bestämmelser om underrättelse till enskilda. En sådan underrättelse ska endast lämnas i de fall rätten lämnat tillstånd till ansökan om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation och när upptagningen eller uppteckningen av avlyssningen eller övervakningen görs i Sverige. Motsvarande bör gälla för hemlig dataavläsning. Det innebär att någon underrättelse aldrig blir aktuell när upptagningen eller uppteckningen görs i den andra staten, t.ex. vid hemlig dataavläsning av kameraövervaknings- eller rumsavlyssningsuppgifter (jfr 4 kap. 28 § andra stycket LIRB). När underrättelse väl ska lämnas bör, i stället för rättegångsbalkens bestämmelser om underrättelse, motsvarande bestämmelser i den föreslagna lagen om hemlig dataavläsning tillämpas.

På samma sätt som för rättslig hjälp och tekniskt bistånd med hemlig dataavläsning utomlands bör en åklagare kunna ansöka om tillstånd till gränsöverskridande hemlig dataavläsning. En sådan ansökan bör dock endast kunna avse kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter. Nuvarande bestämmelse i 4 kap. 26 c § om tillstånd från en annan stat till hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation omfattar nämligen inte platsuppgifter enligt 27 kap. 19 § första stycket 2 och 3 rättegångsbalken (jfr resonemanget i avsnitt 13.2.2). Motsvarande bör gälla för hemlig dataavläsning.

13.3 Hemlig dataavläsning enligt lagen om en europeisk utredningsorder

13.3.1 Hemlig dataavläsning ska omfattas av lagen om en europeisk utredningsorder

Regeringens förslag: En europeisk utredningsorder ska kunna avse hemlig dataavläsning.

Innan en åklagare utfärdar en utredningsorder om hemlig dataavläsning ska åklagaren ansöka om domstolens tillstånd att utfärda utredningsordern.

I avvaktan på domstolens beslut får åklagaren enligt de förutsättningar som gäller för ett nationellt beslut om hemlig dataavläsning, utfärda en utredningsorder om hemlig dataavläsning. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

Om en utredningsorder om hemlig dataavläsning ska erkännas och verkställas i Sverige får åklagaren i avvaktan på domstolens beslut och under de förutsättningar som gäller för ett nationellt beslut om hemlig dataavläsning, besluta att erkänna och verkställa utredningsordern.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: För att omfattas av lagen om en europeisk utredningsorder bör, som utredningen föreslår, hemlig dataavläsning tas in i förteckningen i 1 kap. 4 § lagen om en europeisk utredningsorder, vilken definierar vilka utredningsåtgärder som en europeisk utredningsorder ska avse eller motsvara. Som en följd av att hemlig dataavläsning tas in som en utredningsåtgärd i lagen om en europeisk utredningsorder behövs vissa följdändringar.

För övriga hemliga tvångsmedel enligt lagen krävs det domstolsprövning innan en utredningsorder kan utfärdas (2 kap. 5 § första stycket 2). En sådan ordning bör, som utredningen föreslår, även gälla för hemliga dataavläsning.

För övriga hemliga tvångsmedel finns det en möjlighet för åklagaren att i avvaktan på domstolens beslut, under de förutsättningar som anges i rättegångsbalken, fatta ett interimistiskt beslut om en utredningsorder (2 kap. 5 § andra stycket). En sådan möjlighet bör finnas även avseende hemlig dataavläsning. För att åklagaren ska ha en möjlighet att fatta interimistiska beslut även avseende hemlig dataavläsning bör det, som utredningen föreslår, införas en hänvisning till hemlig dataavläsning så att även sådana beslut får fattas i avvaktan på domstolens beslut under de förutsättningar som gäller för ett nationellt beslut om hemlig dataavläsning. På samma sätt som för övriga hemliga tvångsmedel bör gälla att åklagaren utan dröjsmål ska anmäla till domstolen att en utredningsorder har utfärdats.

Även när det gäller erkännande och verkställande i Sverige av en europeisk utredningsorder från en annan medlemsstat ska domstolsprövning föregå utredningsordern om det hade varit ett krav i motsvarande situation i Sverige (3 kap. 9 §). Åklagaren får dock i avvaktan på domstolens beslut, under de förutsättningar som gäller enligt rättegångsbalken, besluta att

erkänna och verkställa en utredningsorder avseende hemliga tvångsmedel (3 kap. 10 §). Hemlig dataavläsning bör behandlas på samma sätt och åklagaren bör därför, som utredningen föreslår, ges möjlighet att interimistiskt fatta beslut om att erkänna eller verkställa en utredningsorder avseende hemlig dataavläsning. För att det ska vara möjligt behöver det föras in en hänvisning till den föreslagna lagen om hemlig dataavläsning i 3 kap. 10 § lagen om en europeisk utredningsorder.

13.3.2 Utfärdande av en europeisk utredningsorder i Sverige om hemlig dataavläsning

Regeringens förslag: En utredningsorder ska få utfärdas för hemlig dataavläsning i Sverige eller i en annan medlemsstat. En utredningsorder för hemlig dataavläsning i Sverige eller i en annan medlemsstat än den stat dit utredningsordern sänds ska endast få avse kommunikationsavlyssnings-, kommunikationsövervaknings- och platsuppgifter.

När hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter ska göras i en annan medlemsstat än den stat dit utredningsordern översänds ska de regler som gäller i motsvarande fall vid hemlig avlyssning och hemlig övervakning av elektronisk kommunikation om utredningsorder tillämpas.

När en utredningsorder för hemlig dataavläsning har utfärdats ska reglerna som gäller för hemlig dataavläsning om omedelbart hävande av beslut, om avlyssningsförbud, om överskottsinformation, om granskning och bevarande och om fortsatt behandling av uppgifter tillämpas. I de fall där upptagningen eller upptecknigen görs i Sverige ska reglerna som gäller för underrättelse till en enskild vid hemlig dataavläsning tillämpas.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna uttalar sig inte särskilt i denna del.

Skälen för regeringens förslag: För samtliga hemliga tvångsmedel finns särskilda bestämmelser i lagen om en europeisk utredningsorder beträffande vad som gäller när en sådan har utfärdats i Sverige (2 kap. 17–19 §§). När upptagningar och upptecknigar görs i utlandet ska reglerna i 27 kap. 22–24 §§ RB tillämpas. De innehåller bestämmelser om att rätten eller åklagaren omedelbart ska häva ett beslut om det inte finns skäl för det, om avlyssningsförbud, om överskottsinformation samt om granskning och bevarande av upptagning eller upptecknig.

För hemlig avlyssning och hemlig övervakning av elektronisk kommunikation gäller ytterligare bestämmelser, vilket hänger samman med att det vid hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation är möjligt dels att utfärda en utredningsorder för avlyssning eller övervakning i en annan medlemsstat än den stat dit ordern översänds, inklusive den stat som utfärdat ordern, dels med omedelbar överföring av meddelanden eller uppgifter om meddelanden till det land som utfärdat utredningsordern.

I avsnitt 13.3.1 föreslås att hemlig dataavläsning ska omfattas av lagen om en europeisk utredningsorder. Eftersom hemlig dataavläsning kommer att kunna användas för att läsa av eller ta upp uppgifter som i dag får

hämtas in med stöd av hemlig avlyssning och hemlig övervakning av elektronisk kommunikation och mot bakgrund av vad som anförs ovan om dessa tvångsmedel bör det i lagen införas en uttrycklig bestämmelse om att en utredningsorder får utfärdas för hemlig dataavläsning i Sverige eller i en annan medlemsstat på motsvarande sätt som föreskrivs 2 kap. 17 §. Huvudfallet är att den hemliga dataavläsningen görs i den stat som tar emot ordern och kan då avse samtliga uppgifter som föreslås kunna hämtas in med hemlig dataavläsning. I de fall utredningsordern avser dataavläsning i Sverige eller i en annan medlemsstat än den stat dit utredningsordern översänds, bör, med hänsyn till att bestämmelserna i direktivet om en europeisk utredningsorder enbart avser åtgärder som i dag motsvaras av hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation, hemlig dataavläsning i dessa fall endast få avse kommunikationsavlyssnings-, kommunikationsövervaknings- och platsuppgifter, eftersom det europeiska samarbetet inte omfattar fler uppgifter än dessa. Om dataavläsningen ska göras i en annan medlemsstat än dit utredningsordern översänds bör – på samma sätt som gäller vid hemlig avlyssning och hemlig övervakning av elektronisk kommunikation om att det av utredningsordern ska framgå att en underrättelse enligt 4 kap. 12 § lagen om en europeisk utredningsorder har lämnats – utredningsordern om hemlig dataavläsning innehålla motsvarande uppgifter. I de fall upptagningen, med tillämpning av ovan föreslagna bestämmelser, görs i Sverige, bör de bestämmelser om underrättelse till enskild som föreslås i lagen om hemlig dataavläsning tillämpas.

De bestämmelser som i dag ska tillämpas vid utfärdande av en utredningsorder för hemliga tvångsmedel om att rätten eller åklagaren omedelbart ska häva ett beslut om det inte finns skäl för det, om avlyssningsförbud, om överskottsinformation samt om granskning och bevarande av upptagning eller uppteckning bör tillämpas även vid hemlig dataavläsning. Förutom det avlyssningsförbud som föreslås vid hemlig dataavläsning bör även det föreslagna förbudet som avser uppgifter som skyddas av beslagsförbudet gälla i dessa fall. Om det vid genomförande av hemlig dataavläsning som avser uppgifter som finns lagrade i ett avläsningsbart informationssystem eller uppgifter om hur ett avläsningsbart informationssystem används kommer fram en uppgift som hindrar beslag ska avläsningen omedelbart avbrytas och upptagningarna och uppteckningarna omedelbart förstöras i de delar som omfattas av skyddet.

13.3.3 Verkställighet i Sverige av en europeisk utredningsorder om hemlig dataavläsning

Regeringens förslag: Vid verkställighet av en utredningsorder för hemlig dataavläsning som gäller kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter, ska åklagaren i samråd med behörig myndighet i den andra medlemsstaten besluta om huruvida utredningsorderna ska verkställas genom

- omedelbar överföring av meddelanden eller uppgifter om meddelanden, eller
- upptagning eller uppteckning av meddelanden eller uppgifter om meddelanden i Sverige.

Vid verkställighet genom omedelbar överföring får upptagning eller uppteckning inte göras i Sverige och underrättelse till en enskild ska inte göras. Om åklagaren har meddelat en interimistisk verkställbarhetsförklaring som avser hemlig dataavläsning får verkställighet genom omedelbart överförande av meddelanden och uppgifter till den andra medlemsstaten ske först efter det att domstolen har fastställt förklaringen.

Vid verkställighet av en utredningsorder för hemlig dataavläsning som gäller kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter genom upptagning eller uppteckning av meddelanden i Sverige ska dessa upptagningar eller uppteckningar inte granskas. Detsamma gäller vid verkställighet av en utredningsorder för hemlig dataavläsning som gäller platsuppgifter, kameraövervakningsuppgifter, rumsavlyssningsuppgifter, elektroniskt lagrade uppgifter och uppgifter som visar hur ett avläsningsbart informationssystem används.

Upptagningar och uppteckningar som finns kvar i Sverige efter det att ärendet har avslutats hos åklagaren och bevismaterialet har överlämnats får bevaras om det hade varit tillåtet vid hemlig dataavläsning i en svensk förundersökning.

I fråga om underrättelse till en enskild ska de bestämmelser som gäller när en underrättelse lämnas till en enskild i samband med verkställighet av en utredningsorder för hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation tillämpas på motsvarande sätt vid hemlig dataavläsning.

Utredningens förslag överensstämmer i huvudsak med regeringens. Utredningen föreslår att verkställighet i Sverige av en europeisk utredningsorder även ska kunna omfatta platsuppgifter (av utredningen benämnt lokaliseringsuppgifter).

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 3 kap. lagen om en europeisk utredningsorder finns bestämmelser om erkännande och verkställighet i Sverige av en europeisk utredningsorder. De grundläggande reglerna i kapitlet som behandlar vad som ska gälla för erkännande av en utredningsorder för hemliga tvångsmedel är generellt utformade och behöver inte ändras för att hemlig dataavläsning ska omfattas av dem. Samma sak gäller för reglerna om handläggning av frågor om erkännande och verkställighet med undantag för interimistiska beslut enligt 10 § där en justering är nödvändig (se avsnitt 13.3.1).

När det däremot gäller de regler som särskilt behandlar frågan om verkställighet av olika typer av utredningsåtgärder finns det behov av kompletterande bestämmelser i lagen om en europeisk utredningsorder. De regler som finns i dag är nämligen inte tillämpliga för hemlig dataavläsning.

I 3 kap. 34–36 §§ regleras vad som ska gälla vid verkställighet av en utredningsorder om hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation.

Regeringen delar utredningens bedömning att verkställighet av en utredningsorder för hemlig dataavläsning som utgångspunkt bör regleras på motsvarande sätt som gäller för övriga hemliga tvångsmedel.

Enligt 3 kap. 34 § kan hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation verkställas antingen genom omedelbar överföring av meddelanden eller uppgifter om meddelanden till den andra medlemsstaten eller genom upptagning eller uppteckning i Sverige av meddelanden eller uppgifter om meddelanden för senare befordran till den andra medlemsstaten. Beträffande hemlig övervakning av elektronisk kommunikation gäller bestämmelsen endast uppgifter om meddelanden enligt 27 kap. 19 § första stycket 1 rättegångsbalken, men däremot inte beträffande uppgifter om lokalisering enligt 27 kap. 19 § första stycket 2 och 3. Motsvarande regler för verkställighet genom omedelbar överföring bör införas vid verkställighet av en utredningsorder för hemlig dataavläsning avseende kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter. Regeringen föreslår således, till skillnad från utredningen, att verkställighet av en europeisk utredningsorder inte ska kunna göras för platsuppgifter.

Om verkställighet sker genom omedelbar överföring anges i 3 kap. 35 § lagen om en europeisk utredningsorder att upptagning eller uppteckning inte får göras i Sverige och att reglerna om underrättelse till enskild inte ska tillämpas. Dessutom framgår av den bestämmelsen att om åklagaren har meddelat en interimistisk verkställbarhetsförklaring får verkställighet genom omedelbar överföring inte ske förrän domstolen har fastställt förklaringen. Vid verkställighet av en utredningsorder för hemlig dataavläsning genom omedelbar överföring av kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter bör motsvarande bestämmelser införas. I övriga fall, dvs. när verkställighet av hemlig avlyssning och hemlig övervakning av elektronisk kommunikation inte sker genom omedelbar överföring av meddelanden och uppgifter om meddelanden och i andra fall av verkställighet av en utredningsorder för hemlig övervakning av elektronisk kommunikation tillämpas 3 kap. 36 §. Den bestämmelsen tillämpas också för verkställighet av hemlig kameraövervakning och hemlig rumsavlyssning. När det gäller andra fall av hemlig övervakning av elektronisk kommunikation avser det således uppgifter enligt 27 kap. 19 § första stycket 2 och 3 rättegångsbalken. I 3 kap. 36 § anges att upptagningar och uppteckningar inte behöver granskas enligt 27 kap. 24 § RB och att upptagningar som finns kvar i Sverige när ärendet avslutats får bevaras endast om det är tillåtet enligt 27 kap. 24 § RB.

Dessutom gäller enligt 3 kap. 36 § särskilda regler beträffande underrättelse till enskild som inte helt överensstämmer med rättegångsbalkens reglering. Detta för att anpassa regleringen till att det i dessa fall inte är en svensk förundersökning som pågår, bl.a. tidpunkten för underrättelse och att ytterligare sekretessbestämmelser ska beaktas. För en närmare redogörelse hänvisas till propositionen Nya regler om bevisinhämtning inom EU (prop. 2016/17:218 s. 287).

Vid verkställighet av en utredningsorder för hemlig dataavläsning genom upptagning eller uppteckning bör motsvarande bestämmelser införas. Vad som omfattas är kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter som inte verkställs genom omedelbar överföring av meddelanden eller uppgifter om meddelanden, plats-, kameraövervaknings- och, rumsavlyssningsuppgifter samt uppgifter som finns lagrade i ett avläsningsbart informationssystem eller som visar hur ett

avläsningsbart informationssystem används. En granskning av upptagningen eller upptecknigen bör således inte behöva göras och upptagningar och upptecknigar som finns kvar i Sverige efter det att ärendet har avslutats hos åklagaren och bevismaterialet har överlämnats till den andra staten bör endast få bevaras om det är tillåtet enligt motsvarande regler om hemlig dataavläsning i ett inhemskt förfarande. De regler som gäller underrättelse till enskild i 3 kap. 36 § bör gälla vid hemlig dataavläsning på motsvarande sätt.

13.3.4 Underrättelse om hemlig dataavläsning

Regeringens förslag: Det som gäller för hemlig avlyssning och övervakning av elektronisk kommunikation i fråga om underrättelse från Sverige till en annan stat och från en annan stat till Sverige när det inte behövs något bistånd för att genomföra åtgärden ska gälla även för hemlig dataavläsning vid avläsning av kommunikationsavlyssnings-, kommunikationsövervaknings- och platsuppgifter.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna yttrar sig inte särskilt i denna del.

Skälen för regeringens förslag: I 4 kap. 12 § lagen om en europeisk utredningsorder finns bestämmelser om underrättelse till en annan medlemsstat beträffande hemlig avlyssning eller övervakning av elektronisk kommunikation som avses att genomföras av ett telefonnummer, en annan adress eller elektronisk kommunikationsutrustning som används på den andra statens territorium. I 4 kap. 13–15 §§ samma lag finns motsvarande bestämmelser om förfarandet när en annan medlemsstat underrättar Sverige om hemlig avlyssning och övervakning av elektronisk kommunikation i Sverige utan bistånd av en svensk myndighet. Eftersom hemlig dataavläsning vid avläsning av kommunikationsavlyssnings-, kommunikationsövervaknings- och platsuppgifter i praktiken kommer att vara ett sätt att komma åt samma uppgiftstyper som får hämtas in genom hemlig avlyssning eller övervakning av elektronisk kommunikation bör motsvarande regler gälla beträffande underrättelse och prövning av annan stats underrättelse som gäller för dessa tvångsmedel. Det bör därför, i enlighet med vad utredningen föreslår, införas en bestämmelse i lagen om en europeisk utredningsorder som, när hemlig dataavläsning används i dessa fall, hänvisar till reglerna om hemlig avlyssning och övervakning av elektronisk kommunikation.

13.4 Territorialitetsprincipen vid exekutiv jurisdiktion

Regeringens bedömning: Frågan om en nyansering av den svenska hållningen när det gäller vad territorialitetsprincipen vid exekutiv jurisdiktion innebär för elektroniskt lagrade uppgifter bör inte tas om hand inom ramen för detta lagstiftningsprojekt.

Utredningens bedömning överensstämmer delvis med regeringens. Utredningen bedömer att det finns starka skäl att nyansera den svenska hållningen avseende vad territorialitetsprincipen vid exekutiv jurisdiktion innebär för elektroniskt lagrade uppgifter. Frågan bör enligt utredningen inte bli föremål för nationell lagstiftning utan prövas i rättstillämpningen.

Remissinstanserna: Flera remissinstanser delar utredningens bedömning att den svenska hållningen bör ändras men ifrågasätter utredningens bedömning, enligt vilken frågan överlämnas till rättstillämpningen. *Svea hovrätt*, *Göteborgs tingsrätt, Åklagarmyndigheten, Ekobrottsmyndigheten, Skatteverket* och *Uppsala universitet (Juridiska fakulteten)* anser att lagstiftning i frågan bör övervägas i stället för att överlämna frågan åt rättstillämpningen. Åklagarmyndigheten och *Malmö tingsrätt* är skeptiska till att domstolarna ska kunna utarbeta praxis på området, bl.a. eftersom hemliga tvångsmedel ytterst sällan är föremål för överklagande och beslutsfattandet ska ske skyndsamt. *Lunds universitet (Juridiska fakulteten)* anser att uttalanden om att det finns ett problem men inte någon föreslagen lösning kan skapa osäkerhet om gällande rätt. *Civil Rights Defenders* understryker att när en myndighet utför hemlig dataavläsning måste den uppfylla kraven i internationella rättsliga åtaganden. Hemlig dataavläsning får inte användas för att kringgå internationella överenskommelser och regleringar för att erhålla uppgifter som ligger utanför statens egna territorium.

Tullverket delar utredningens bedömning att det finns skäl att nyansera den svenska hållningen för att hemlig dataavläsning ska kunna bli effektivt.

Polismyndigheten förespråkar en lagstiftning som ger brottsbekämpande myndigheter tillgång till elektroniskt lagrade uppgifter med utgångspunkt där uppgifterna finns tillgängliga för den misstänkte eller där den misstänkte haft en accesspunkt.

Datainspektionen anför att stora mängder information som används i flera kommunikationstjänster som inte har sin bas i Sverige inte kommer att bli tillgänglig genom den föreslagna lagen. Datainspektionen, i likhet med Tullverket och Polismyndigheten, anser därför att lagen inte kommer att bli effektiv.

Skälen för regeringens bedömning: Med exekutiv jurisdiktion avses rätten att verkställa åtgärder och förverkliga beslut som fattats inom ramen för lagstiftning och rättsskipning. När det gäller exekutiv jurisdiktion är utgångspunkten i folkrätten att det råder ett förbud för stater att vidta verkställighetsåtgärder på andra staters territorier, t.ex. att använda hemliga tvångsmedel där. Detta är ett utflöde av den s.k. territorialitetsprincipen.

Elektroniska uppgifter kan finnas lagrade i flera stater samtidigt eller ständigt vara på väg mellan stater. I många fall är det inte ens för den som tillhandahåller en internettjänst möjligt att klargöra var uppgifterna finns i varje givet ögonblick. När detta trots allt är möjligt kan förhållandena ändras på bråkdelen av en sekund. Den svenska hållningen har hittills varit att om uppgifter lagras elektroniskt på annan plats än i Sverige eller om det är okänt var uppgifterna lagras så saknar svenska brottsbekämpande myndigheter jurisdiktion.

Utredningen bedömer att det finns skäl att ändra den svenska hållningen, en slutsats som stöds av bl.a. *Tullverket* och *Skatteverket*. Utredningen

lämnar dock inte något lagförslag utan bedömer att frågan i stället bör lösas i rättspraxis. *Malmö tingsrätt, Åklagarmyndigheten* och *Lunds universitet (Juridiska fakulteten)* anser att ett sådant förhållningssätt skapar osäkerhet om gällande rätt och att möjligheten att utarbeta praxis på området är liten eftersom hemliga tvångsmedel ytterst sällan är föremål för överklagande och beslutsfattandet ska ske skyndsamt. Liknande synpunkter framförs av *Svea hovrätt, Göteborgs tingsrätt, Ekobrottsmyndigheten, Skatteverket* och *Uppsala universitet (Juridiska fakulteten).*

Frågan hur man ska hantera åtkomst av uppgifter som lagras utanför den egna jurisdiktionen eller när det inte är känt var uppgifterna lagras har diskuterats inom EU. Anledningen till att frågan diskuteras internationellt är den ökade globaliseringen och att frågan inte anses kunna lösas av enskilda stater var för sig. Regeringen bedömer att frågan om hur territorialitetsprincipen vid exekutiv jurisdiktion bör tolkas bäst tas om hand inom ramen för det internationella samarbetet eller på annat lämpligt sätt.

Regeringen gör sammanfattningsvis bedömningen att frågan om den svenska tolkningen av territorialitetsprincipen vid exekutiv jurisdiktion i förhållande till elektroniskt lagrade uppgifter bör ändras inte kan tas om hand inom ramen för detta lagstiftningsprojekt.

14 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Lagen om hemlig dataavläsning ska träda i kraft den 1 mars 2020 och tidsbegränsas att gälla till och med den 28 februari 2025. Övriga lagändringar ska träda i kraft den 1 mars 2020.

Regeringens bedömning: Det finns inte behov av några särskilda övergångsbestämmelser.

Utredningens förslag och bedömning överensstämmer i huvudsak med regeringens. Utredningen föreslår att den nya lagen ska träda i kraft den 1 januari 2019.

Remissinstanserna yttrar sig inte särskilt i denna fråga.

Skälen för regeringens förslag och bedömning: De brottsbekämpande myndigheterna kommer att behöva viss tid att förbereda sig för tillämpningen av hemlig dataavläsning. Det är dock angeläget att reglerna träder i kraft så snart som möjligt. Regeringen föreslår därför att lagen om hemlig dataavläsning och övriga lagändringar ska träda i kraft den 1 mars 2020. Då det är fråga om en tillfällig lagstiftning bör dess giltighet tidsbegränsas och enligt vad som anförs i avsnitt 9.1 bör giltighetstiden bestämmas till fem år.

Ny processrättslig lagstiftning ska som utgångspunkt tillämpas genast efter ikraftträdandet. Nya regler ska alltså tillämpas på varje processuell företeelse som inträffar efter det att regleringen har trätt i kraft. De brottsbekämpande myndigheterna och domstolarna ska således tillämpa de nya bestämmelserna även i förundersökningar och tvångsmedelsärenden som

har inletts innan de föreslagna bestämmelserna träder i kraft. Regeringen delar därmed utredningens bedömning att det inte finns behov av några övergångsbestämmelser.

15 Konsekvenser

15.1 Ekonomiska konsekvenser

Regeringens bedömning: Hemlig dataavläsning leder till ökade kostnader för Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket, som ska verkställa tvångsmedlet. Regeringen har i budgetpropositionen för 2020 föreslagit att anslaget för dessa myndigheter höjs för att bl.a. finansiera dessa kostnader. Anskaffning av teknisk utrustning som utgör anläggningstillgångar bör finansieras genom ianspråktagande av låneramar.

De eventuella kostnadsökningar som kan förväntas för andra myndigheter inom rättsväsendet och för offentliga ombud bedöms rymmas inom befintliga anslag.

Utredningens bedömning överensstämmer inte med regeringens. Utredningen bedömer att kostnadsökningarna huvudsakligen bör rymmas inom befintliga anslag eller i vart fall genom omfördelning av befintliga anslag. För Säkerhets- och integritetsskyddsnämnden föreslår utredningen att anslaget bör höjas vilket kan åstadkommas genom omfördelning av befintliga anslag för andra myndigheter.

Remissinstanserna: Majoriteten av remissinstanserna kommenterar inte förslaget. *Domstolsverket* ifrågasätter utredningens bedömning att det endast kommer att bli fråga om ett begränsat antal verkställighetstillfällen av hemlig dataavläsning per år och att dessa kommer att ersätta ansökningar om andra hemliga tvångsmedel. *Ekobrottsmyndigheten* anför att hemlig dataavläsning kommer att ställa krav på mycket goda datatekniska kunskaper hos de myndigheter som verkställer åtgärderna och det kommer också att medföra kostnader för adekvat utrustning. Det kommer att krävas att särskilda insatser genomförs för att utbilda och rekrytera specialister på området och att rutiner tas fram. *Polismyndigheten* och *Säkerhetspolisen* anför att hemlig dataavläsning kommer att medföra ökade kostnader för de brottsbekämpande myndigheterna och att det inte är möjligt att finansiera förslaget inom befintlig anslagsram utan att göra avkall på annan verksamhet. *Säkerhets- och integritetsskyddsnämnden* bedömer att nämnden behöver mer resurser för den nya arbetsuppgiften men kan inte ange någon exakt kostnad förrän det står klart hur lagstiftningen närmare utformas.

Skälen för regeringens bedömning

Hemlig dataavläsning innebär ökade kostnader

För att kunna genomföra hemlig dataavläsning behöver de brottsbekämpande myndigheterna tillgång till ny teknik. Den teknik som används i

samband med verkställighet av åtgärden kan vara kostsam. Med detta menas både tekniska metoder för att bereda sig tillträde till avläsningsbara informationssystem och programvara som kan placeras i avläsningsbara informationssystem för att möjliggöra och genomföra verkställigheten. För sådan verkställighet som består av t.ex. inloggning i en misstänkts konto till en kommunikationstjänst uppstår inte några kostnader utöver ren personalkostnad. Inte heller förväntas det uppstå andra kostnader för att läsa av information sedan en programvara är installerad i t.ex. en misstänkts dator.

Den teknik som behövs för verkställighet av hemlig dataavläsning kan antingen köpas från privata leverantörer eller utvecklas av de brottsbekämpande myndigheterna själva. Som utredningen redogör för finns det både fördelar och nackdelar med respektive lösning. Regeringens uppfattning, liksom utredningens, är att det inte finns skäl att reglera hur myndigheterna väljer att gå tillväga i det avseendet. Det synes dock som att det enda praktiska alternativet är att köpa den tekniska lösning som behövs för hemlig dataavläsning. Den investering som i sådant fall kommer att behöva göras är av sådan natur att den bör finansieras genom ianspråktagande av låneramen för den myndighet som gör inköpet. Det enda rimliga alternativet är att den största myndigheten, dvs. Polismyndigheten, gör inköpet av systemet. Kostnaden för detta inköp kommer härigenom att belasta myndighetens resultat genom årliga avskrivningar. De övriga verkställande myndigheterna kommer i sådant fall att bidra till finansieringen genom licensavgifter eller liknande till Polismyndigheten. Förutom denna kostnad kommer det att uppstå kostnader för nyrekrytering, utbildning, kompetensutveckling, anskaffning av teknisk utrustning, drift och underhåll samt kostnader för medverkande operatörer. Utredningen beräknar den ökade kostnaden för de brottsbekämpande myndigheterna som ska verkställa hemlig dataavläsning till drygt 100 miljoner kronor årligen. Härutöver kommer det dessutom att uppstå kostnader för de resurser som krävs för kartläggning (t.ex. fysisk spaning) av den person som hemlig dataavläsning ska användas mot eller de resurser (t.ex. utredare, underrättelsehandläggare och tolkar) som krävs för bearbetning av det inhämtade materialet. Utredningen gör bedömningen att kostnaderna för resurser bör rymmas inom befintliga anslag efter omdispositioner. Utredningen baserar sin kostnadsberäkning på en uppskattad kapacitet på cirka 20–30 samtidiga installationer årligen. I den bedömningen ska det beaktas att vissa installationer kan genomföras med relativt kort förberedelse och relativt enkelt medan andra är mer komplexa och kräver en mer omfattande kartläggning av både den person och det informationssystem som tillståndet avser. Med ledning av de uppgifter utredningen redovisar bedömer regeringen att myndigheternas kostnader uppgår till 65 miljoner kronor för Polismyndigheten, 35 miljoner kronor för Säkerhetspolisen och 12,5 miljoner kronor för Tullverket. Dessa belopp har regeringen föreslagit att myndigheterna ska tillskjutas i ökade anslag, prop. 2019/20:1 utg.omr. 3 och utg.omr. 4. För Ekobrottsmyndigheten har regeringen, i budgetpropositionen för 2020, föreslagit ett tillskott om 19 miljoner kronor att användas bl.a. för att stärka kapaciteten att säkerställa utredning och lagföring i resurskrävande ärenden. Ärenden där hemliga dataavläsning aktu-

aliseras hör typiskt sett till kategorin resurskrävande ärenden. Ekobrottsmyndighetens förmåga att hantera hemlig dataavläsning inom befintliga ramar – efter de tillskott som föreslås – bedöms därför som goda.

Inga ökade kostnader för Säkerhets- och integritetsskyddsnämnden

Säkerhets- och integritetsskyddsnämnden ska enligt förslaget underrättas om domstolens beslut i frågor om hemlig dataavläsning samt i de fall otillåten tilläggsinformation har tagits upp eller lästs av (20 § och 23 § första stycket). Den åtgärden kommer inte i sig inte att innebära några beaktansvärda ekonomiska konsekvenser för nämnden. Däremot får det i och för sig antas att tillsynen över hemlig dataavläsning kommer att kräva en ökad teknisk, eller annan, kompetens. Tillsynen kan också behöva bedrivas på ett annorlunda sätt än i dag. Sammantaget gör dock regeringen bedömningen att nämnden bör kunna utföra de nya uppgifterna inom tilldelade ramar.

Ökade kostnader för Sveriges domstolar, Åklagarmyndigheten och offentliga ombud

Varje ärende om hemlig dataavläsning ska enligt förslaget prövas av domstol med offentligt ombud närvarande och som huvudregel efter ansökan av åklagare. Utredningen bedömer att det kommer att bli fråga om ett begränsat antal verkställighetstillfällen per år som i flertalet fall kommer att ersätta ansökningar om andra hemliga tvångsmedel. Därför bedömer utredningen att kostnaderna för Sveriges domstolar, offentliga ombud, Åklagarmyndigheten och Ekobrottsmyndighetens åklagarverksamhet inte bör öka i sådan utsträckning att de inte ryms inom befintliga anslag. Regeringen instämmer i den bedömningen och ser inte, som *Domstolsverket*, risk att ärendemängden blir så stor att den kommer att inkräkta på övrig verksamhet mer än vad som är fallet med nuvarande hemliga tvångsmedel. *Ekobrottsmyndigheten* framför att myndighetens kostnader kan komma att öka eftersom den nya tvångsmedelsanvändningen ställer krav på utbildning. Regeringen instämmer i att det behövs utbildning av den operativa personalen. Kostnaderna för sådan utbildning kommer att täckas av den föreslagna ökningen av anslaget.

Det uppstår inga ökade kostnader för företag som medverkar vid verkställighet

Enligt förslaget införs en skyldighet för aktörer som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § lagen om elektronisk kommunikation, dvs. i praktiken företag som tillhandahåller allmänna kommunikationsnät mot ersättning och eller allmänt tillgängliga elektroniska kommunikationstjänster, att medverka vid hemlig dataavläsning. Aktörerna är företag som tillhandahåller elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationsnät mot ersättning. Aktörerna ska enligt förslaget ha rätt till ersättning av den verkställande myndigheten för kostnader som uppstår till följd av medverkan. Förslaget är således avsett att vara kostnadsneutralt för företagen och regeringen instämmer i utredningens bedömning att några kostnadsökningar därför inte bedöms uppstå

för aktörerna. Däremot uppstår kostnader för den brottsbekämpande myndighet som ska betala operatören. Dessa kostnader ingår i den bedömning som nämns ovan beträffande de brottsbekämpande myndigheterna.

Förslaget medför inga ytterligare konsekvenser

Regeringen instämmer i utredningens bedömning att det inte kan förväntas uppstå några ekonomiska konsekvenser för kommuner eller landsting till följd av förslagen. Inte heller har förslagen betydelse för miljön, den kommunala självstyrelsen, sysselsättning och offentlig service i olika delar av landet, små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

15.2 Konsekvenser för den personliga integriteten och för det brottsbekämpande arbetet

Regeringens bedömning: Hemlig dataavläsning innebär ett ökat intrång i den personliga integriteten för de personer som blir föremål för åtgärden men bidrar samtidigt till en stärkt brottsutredande verksamhet, en stärkt underrättelseverksamhet och en bättre utlänningskontroll.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna kommenterar inte bedömningen särskilt, utöver vad som anges i avsnitt 8.4 och 8.5.

Skälen för regeringens bedömning: Som redogörs för i avsnitt 8.5 kommer ett införande av hemlig dataavläsning att innebära att riskerna för enskildas personliga integritet ökar i det enskilda fallet när tvångsmedlet används. Samtidigt kommer hemlig dataavläsning vara ett effektivt verktyg för de brottsbekämpande myndigheterna (se avsnitt 8.5). Det kommer att innebära ökade möjligheterna att utreda och förebygga brott och ökade möjligheter till en effektiv utlänningskontroll.

I stor utsträckning avser hemlig dataavläsning att kompensera för det bortfall i effektivitet som de befintliga tvångsmedlen haft på senare tid. Det är därför rimligt att tro att hemlig dataavläsning främst kommer att användas för samma brottstyper som befintliga hemliga tvångsmedel. Av regeringens redovisning av användningen av hemliga tvångsmedel under 2017 (skr. 2018/19:19) framgår att den användning av hemliga tvångsmedel som där redovisas företrädelsevis har avsett narkotika- och våldsbrottslighet. Det förekommer emellertid många andra brottsrubriceringar vid användning av hemliga tvångsmedel som t.ex. sexualbrott, grovt rån, människohandel och grov mordbrand. Det är alltså rimligt att anta att det är för dessa brottstyper som hemlig dataavläsning främst kommer att användas. Därmed är det troligen också främst för dessa brottstyper som brottsbekämpningen kommer att effektiviseras. Samtidigt ska noteras att narkotikahandel är en motor för mycket annan kriminalitet, varför ett bekämpande av narkotikabrottslighet är positivt även ur den aspekten.

16 Författningskommentar

16.1 Förslaget till lag om hemlig dataavläsning

Ord och uttryck i lagen

1 § Hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem.

I lagen avses med

avläsningsbart informationssystem: en elektronisk kommunikationsutrustning eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst,

kommunikationsavlyssningsuppgifter: uppgifter om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress,

kommunikationsövervakningsuppgifter: uppgifter om annat än innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress,

platsuppgifter: uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits,

kameraövervakningsuppgifter: uppgifter som framkommer genom optisk personövervakning,

rumsavlyssningsuppgifter: uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till.

Paragrafen innehåller en definition av hemlig dataavläsning och definitioner av andra begrepp i lagen. Övervägandena finns i avsnitt 9.2 och 9.3.

I *första stycket* definieras hemlig dataavläsning. Där framgår det att hemlig dataavläsning innebär att uppgifter, som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem.

Definitionen knyter an till bestämmelsen om dataintrång genom att de uppgifter som får läsas av eller tas upp är uppgifter avsedda för automatiserad behandling (jfr 4 kap. 9 c § brottsbalken). Begreppet uppgifter avsedda för automatiserad behandling ska tolkas på samma sätt som enligt bestämmelsen i brottsbalken. Alla sorters uppgifter som uttrycks i en för en dator anpassad och läsbar form kan således omfattas av bestämmelsen (se vidare prop. 2006/07:66 s. 49). Uttrycket avsedda för automatisk behandling syftar på att uppgifterna ska vara anpassade för en teknisk process genom vilken uppgifterna behandlas av ett avläsningsbart informationssystem. Tal mellan två personer (rumsavlyssningsuppgifter) är således avsett för automatisk behandling först när det tas upp av det avläsningsbara informationssystem som åtgärden avser, t.ex. vid inspelning efter att en mikrofon i en mobiltelefon aktiverats.

Avläsningen ska avse uppgifter (avsedda för automatiserad behandling) i ett avläsningsbart informationssystem. Det betyder att uppgifterna ska kunna härledas till det avläsningsbara informationssystem som tillståndet till hemlig dataavläsning avser. Avläsningsbart informationssystem defi-

nieras i andra stycket. Avläsningen får göras genom direkt tillgång till informationssystemet. Avläsningen får också göras i ett angränsande informationssystem, t.ex. via en dator som ger tillgång till uppgifter i en annan dator. I sådana fall kan dock aktsamhetskraven i 25 § andra stycket omöjliggöra avläsningen. Eftersom åtgärden avser en riktad insats mot ett visst informationssystem kommer åtgärden dock endast att kunna omfatta uppgifter som finns i just det informationssystemet.

Att uppgifter ska vara avsedda för automatiserad behandling i ett avläsningsbart informationssystem innebär inte att uppgifterna måste finnas i informationssystemet vid tidpunkten för tillståndsprövningen. Inhämtning av kommunikationsavlyssningsuppgifter kan även avse framtida samtal som först senare blir avsedda för automatiserad behandling, t.ex. när ett telefonsamtal genomförs. Det kan också vara så att uppgifterna blir avsedda för automatiserad behandling först genom att den verkställande myndigheten, efter beviljat tillstånd till hemlig dataavläsning, aktiverar t.ex. en mobiltelefons inspelningsfunktion (se kommentaren till 22 §).

Att uppgifter läses av kan ta sikte både på en helt teknisk process som utförs av en dator eller annat tekniskt hjälpmedel, för att exempelvis göra viss information läsbar, och på den process som äger rum när en person som ansvarar för hemlig dataavläsning tar del av innehållet i informationen. Att uppgifter tas upp innebär att de kan sparas för att granskas i efterhand.

Att åtgärden genomförs i hemlighet innebär att den som blir föremål för åtgärden inte ska känna till den. Därtill kommer att åtgärden ska genomföras med ett tekniskt hjälpmedel. Med tekniskt hjälpmedel avses såväl hårdvara som programvara (se prop. 1994/95:227 s. 29). Hemlig dataavläsning kan således utföras t.ex. sedan hårdvara som kan detektera lösenord fästs på informationssystemet eller efter att programvara som kan fånga upp meddelanden installerats i informationssystemet. Att det ska vara fråga om ett tekniskt hjälpmedel innebär dock inte att det måste utföras en fysisk installation av någonting i eller aptering av någonting på en viss utrustning. Begreppet avläsningsbart informationssystem omfattar nämligen också virtuella tjänster (se kommentaren till andra stycket) varför hemlig dataavläsning även kan genomföras genom att den som verkställer åtgärden använder ett tekniskt hjälpmedel, t.ex. en dator, för att logga in på en misstänkts användarkonto till en internetbaserad kommunikationstjänst. Det tekniska hjälpmedel som används ska kontrolleras och användas av den brottsbekämpande myndighet som verkställer åtgärden. Det är därmed inte fråga om hemlig dataavläsning om de brottsbekämpande myndigheterna vidtar åtgärder utan att använda ett tekniskt hjälpmedel, t.ex. när en polisman vid spaning mot en person ser ett meddelande som personen läser av på sin mobiltelefon eller hör ett samtal mellan två personer. Dessutom ska avläsningen eller upptagningen göras i informationssystemet. Det innebär att det inte är fråga om hemlig dataavläsning om polisen använder en t.ex. bildförstärkare för att bättre kunna uppfatta t.ex. texten på en misstänkts mobiltelefon eftersom avläsningen eller upptagningen då inte görs i informationssystemet.

I *andra stycket* definieras vissa andra centrala begrepp i lagen. Inledningsvis definieras avläsningsbart informationssystem. Det slås för det första fast att en elektronisk kommunikationsutrustning är ett avläsningsbart informationssystem i lagens mening. Begreppet har samma innebörd

som i annan tvångsmedelsreglering (t.ex. i 23 kap. 9 a § och 27 kap. 19 § RB och 1 § inhämtningslagen). Elektronisk kommunikationsutrustning inkluderar således både befintlig och framtida teknisk utrustning som kan användas för elektronisk kommunikation. Begreppet innefattar all slags utrustning som kan användas för att kommunicera elektroniskt, t.ex. datorer, mobiltelefoner, läsplattor, interaktiva högtalare, servrar, smarta klockor och annan liknande utrustning. Utrustning som är sammankopplad – fysiskt eller på annat sätt, t.ex. genom blåtandsteknik – med elektronisk kommunikationsutrustning, t.ex. sladdar, högtalare, tangentbord, USB-minnen, datormus och andra elektroniska tillbehör omfattas också av begreppet. Begreppet ska däremot inte tolkas så att ett helt nätverk som en dator är kopplad till genom en sladd och all utrustning som är ansluten till nätverket, oavsett dess storlek, ingår i det informationssystem som får läsas av. Avgränsningen av vilken utrustning som ska omfattas av tillståndet ska göras utifrån vad som framstår som rimligt med hänsyn till det informationssystem som anges i tillståndet.

Enligt definitionen kan ett avläsningsbart informationssystem också vara ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst. Gemensamt för tjänsterna är att det är möjligt att få åtkomst till uppgifter i dem från olika elektroniska kommunikationsutrustningar efter angivande av t.ex. inloggningsuppgifter, oberoende av var uppgifterna är lagrade. Begreppet omfattar t.ex. internetbaserade meddelande- och telefonitjänster. Med lagringstjänst avses sådana tjänster där enskilda kan lagra uppgifter elektroniskt på annat utrymme än i den egna fysiska utrustningen, s.k. molntjänster. Dessa lagras på en annan geografisk plats än i den egna fysiska utrustningen. Med begreppet liknande tjänster avses exempelvis tjänster vars primära syfte inte är kommunikation eller lagring men som innefattar möjlighet till endera av dessa. Så kan exempelvis vara fallet med internetbaserade innehållstjänster som speltjänster, bokningstjänster eller andra liknande applikationer eller program.

Avläsningen eller upptagningen får inte avse hela tjänsten utan endast ett användarkonto till, eller en på motsvarande sätt avgränsad del av, tjänsten. I avläsningsbara informationssystem som t.ex. sociala medier och internetforum kan det finnas en mycket stor mängd data och avgränsade plattformar för varje enskild användare. Avläsningen eller upptagningen inom ramen för hemlig dataavläsning får endast göras i den del av tjänsten som avser en enskild persons egna utrymme och virtuellt begränsade yta i tjänsten. Detta kan t.ex. vara en personlig sida på ett socialt medium eller ett användarkonto på ett internetforum. Exempel på en på motsvarande sätt avgränsad del av tjänsten är när den enskilde inte har ett användarkonto men en egen personlig yta. Så kan vara fallet när han eller hon använder en tjänst med inloggningsuppgifter som flera har tillgång till, utan ett bestämt användarkonto (t.ex. inloggning till tjänster som företag erbjuder sina anställda eller som högskolor erbjuder sina studerande).

I paragrafen definieras vidare vissa typer av uppgifter som hemlig dataavläsning kan användas för att läsa av eller ta upp. Det bör noteras att definitionerna endast anger vilka uppgiftstyper som får läsas av eller tas upp och även om det nedan görs en jämförelse med uppgifter som kan hämtas in med befintliga hemliga tvångsmedel är inte hemlig dataavläsning inskränkt till att gälla exakt samma uppgifter som kan erhållas genom

dessa tvångsmedel. Skillnaden är framför allt tydlig när det gäller uppgiftstypen platsuppgifter. Genom inhämtningslagen kan nämligen t.ex. Polismyndigheten få del av uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits genom att ta reda på mot vilken basstation som den elektroniska kommunikationsutrustningen har kopplats upp (1 § inhämtningslagen). Vid tillämpning av hemlig dataavläsning kan i stället platsuppgifter erhållas genom t.ex. en uppgift från den elektroniska kommunikationsutrustningens GPS-funktion.

Med kommunikationsavlyssningsuppgifter avses uppgifter i meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress. Med elektroniskt kommunikationsnät avses detsamma som i 1 kap. 7 § lagen om elektronisk kommunikation, nämligen ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och 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. Kommunikationsavlyssningsuppgifter motsvarar de som får hämtas in genom hemlig avlyssning av elektronisk kommunikation (27 kap. 18 § RB).

Kommunikationsövervakningsuppgifter är uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress. Uppgifterna motsvarar de som får hämtas in genom antingen hemlig övervakning av elektronisk kommunikation (27 kap. 19 § första stycket 1 RB) eller inhämtning enligt inhämtningslagen (enligt 1 § 1 den lagen). och omfattar därmed inte uppgifter om vad ett meddelande innehåller. Vidare omfattas inte uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område (27 kap. 19 § första stycket 2). Inte heller omfattar uppgiftstypen uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits (27 kap. 19 § första stycket 3). I de fall som motsvaras av inhämtningslagen får avläsningen eller upptagningen endast avse historiska uppgifter (se vidare i kommentaren till 10 § tredje stycket).

Platsuppgifter avser uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Uppgifterna är till sin typ sådana som får hämtas in genom hemlig övervakning av elektronisk kommunikation (27 kap. 19 § första stycket 3 RB) och vid inhämtning enligt inhämtningslagen (se 1 § 3 den lagen).

Kameraövervakningsuppgifter avser uppgifter som framkommer genom optisk personövervakning. Det motsvarar sådana uppgifter som får hämtas in genom hemlig kameraövervakning utförd med optisk-elektroniska instrument eller annan jämförbar utrustning (27 kap. 20 a § RB).

Slutligen avses med rumsavlyssningsuppgifter uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till. Uppgifterna motsvarar de som får hämtas in genom hemlig rumsavlyssning (se 27 kap. 20 d § RB).

Typer av uppgifter som får läsas av eller tas upp

2 § Tillstånd till hemlig dataavläsning får beviljas för att läsa av eller ta upp

1. kommunikationsavlyssningsuppgifter,
2. kommunikationsövervakningsuppgifter,
3. platsuppgifter,
4. kameraövervakningsuppgifter,
5. rumsavlyssningsuppgifter,
6. uppgifter som finns lagrade i ett avläsningsbart informationssystem men som inte avses i 1–5, eller
7. uppgifter som visar hur ett avläsningsbart informationssystem används men som inte avses i 1–6.

Vid hemlig dataavläsning som gäller kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät även hindras från att nå fram.

Paragrafen anger vilka typer av uppgifter som får läsas av eller tas upp med hemlig dataavläsning och att meddelanden i vissa fall får hindras från att nå fram. Övervägandena finns i avsnitt 9.3.

I *första stycket* finns en punktlista som uttömmande anger vilka olika uppgiftstyper som får läsas av eller tas upp genom hemlig dataavläsning. Uppgifterna ska vara avsedda för automatiserad behandling (se kommentaren till 1 §). Vilka uppgifter som i det enskilda fallet får läsas av eller tas upp bestäms utifrån ändamålet med åtgärden. Som ett exempel kan nämnas att rumsavlyssningsuppgifter (punkt 5) endast får läsas av i brottsutredande verksamhet och aktualiseras således aldrig i underrättelseverksamhet eller vid särskild utlänningskontroll.

Ett tillstånd till hemlig dataavläsning innebär inte att samtliga uppgiftstyper får läsas av eller tas upp. Det krävs tvärtom uttryckligt tillstånd för var och en av uppgiftstyperna (18 § första stycket 3).

Punkt 1–5 omfattar kommunikationsavlyssnings-, kommunikationsövervaknings-, plats-, kameraövervaknings- och rumsavlyssningsuppgifter. Det är uppgiftstyper som får hämtas in genom andra hemliga tvångsmedel. När respektive punkt aktualiseras i ett tillstånd kan hemlig dataavläsning alltså avse avläsning eller upptagning av sådana uppgiftstyper som respektive bakomliggande tvångsmedel kan ge tillgång till. Uppgifterna definieras i 1 § andra stycket.

Punkt 6 avser uppgifter som finns lagrade i ett informationssystem, men som inte avses i punkt 1–5. Det saknar betydelse hur uppgifterna lagrats, dvs. om de lagrats genom en medveten handling av en person eller till följd av en inställning i informationssystemet som användaren inte känt till. Det saknar också betydelse om uppgifterna är varaktigt eller temporärt lagrade eller i vilket format de lagrats. Uppgifterna ska dock finnas lagrade i informationssystemet när avläsningen eller upptagningen genomförs. Lagrade uppgifter kan t.ex. vara datafiler, såsom text-, bild- och ljudfiler, men också program- eller systemfiler. Vidare kan en lagrad uppgift vara ett meddelande som sparats som utkast i ett program för meddelanden eller e-post. Eftersom begreppet avläsningsbart informationssystem innefattar utrustning som anslutits till ett sådant system kan även uppgifter som finns lagrade på ett externt lagringsmedium som kopplats in i en dator läsas av eller tas upp. När det är fråga om uppgifter som är lagrade i ett avläsningsbart informationssystem t.ex. på ett användarkonto för en internetbaserad

lagringstjänst anses uppgifterna lagrade i informationssystemet om de kan tillgängliggöras med det.

Det är vidare ett krav enligt punkten att de uppgifter som läses av eller tas upp inte är sådana som avses i punkterna 1–5. Exempel på uppgifter som kan finnas lagrade men som kan läsas av eller tas upp enligt de andra punkterna är s.k. metadata som kan hämtas in enligt punkt 2 och innehåll i meddelanden som kan hämtas in enligt punkt 1. Det medför att verkställighetstekniken för att ta upp uppgifterna ska anpassas på det sätt som lagen föreskriver (24 §). Om de uppgifter som ska läsas av eller tas upp finns lagrade i informationssystemet men kan samlas in genom användning av hemlig dataavläsning enligt någon av de tidigare punkterna, får tillståndet alltså inte avse punkt 6 utan någon annan punkt som uppgifterna hänför sig till. Ansökan om tillstånd ska därför avgränsas efter vilka slags uppgifter det finns behov av och på vilket sätt de kan läsas av eller tas upp.

Enligt *punkt 7* får avläsning eller upptagning avse uppgifter som visar hur ett informationssystem används men inte avses i punkterna 1–6. Med detta avses uppgifter om vad en användare av ett informationssystem använder det till. Det kan exempelvis handla om användning som inte leder till att information lagras, t.ex. vilka program eller appar som körs, anteckningar som görs och utkast till meddelanden som inte sparas.

Enligt *andra stycket* får meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät hindras från att nå fram, om ett tillstånd till hemlig dataavläsning avser kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter. Motsvarande möjlighet finns vid hemlig övervakning av elektronisk kommunikation (27 kap. 19 § andra stycket RB). Bestämmelsen kan, liksom vid hemlig övervakning av elektronisk kommunikation, t.ex. användas i kritiska lägen för att förhindra att en misstänkt sätter sig i förbindelse med medbrottslingar eller nås av varnande samtal. Något särskilt tillstånd för att hindra meddelanden från att nå fram krävs inte.

Grundläggande förutsättning för hemlig dataavläsning

3 § Ett tillstånd till hemlig dataavläsning får beviljas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

I bestämmelsen lagfästs proportionalitetsprincipen. Övervägandena finns i avsnitt 9.4.

Bestämmelsen tydliggör att proportionalitetsprincipen ska beaktas vid prövningen av om tillstånd ska ges till hemlig dataavläsning. Principen innebär att hemlig dataavläsning i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden (Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas?, 4 uppl. 2018 s. 20–28). Det finns alltså en skyldighet för rätten, och i förekommande fall åklagaren när denne fattar interimistiska beslut, att alltid beakta proportionalitetsprincipen vid prövningen av om hemlig dataavläsning ska tillåtas. Principen får också betydelse för hur ett tillstånd ska utformas och vilka villkor som ska förenas med det (se kommentaren till 18 §).

För att hemlig dataavläsning ska vara en proportionerlig åtgärd måste den som ansöker om hemlig dataavläsning först utreda eller tömma ut möjligheterna till andra åtgärder innan en ansökan om hemlig dataavläsning görs. Det är dock inte något krav att övriga tvångsmedel har använts och misslyckats för att tillstånd till hemlig dataavläsning ska ges. En utgångspunkt är emellertid att hemlig dataavläsning är en proportionerlig åtgärd endast om andra åtgärder för att komma åt uppgifterna i fråga inte är tillräckliga, skulle vara väsentligt svårare att genomföra eller kan förväntas leda till större integritetsintrång än hemlig dataavläsning.

Proportionalitetsprincipen får särskilt stor betydelse när ansökan om hemlig dataavläsning avser fler än en typ av uppgift eftersom intrånget i den personliga integriteten typiskt sett blir större ju mer omfattande åtgärden tillåts vara och ju mer information den ger tillgång till. Vid proportionalitetsprövningen ingår också att beakta vilka eventuella risker åtgärden medför för informationssäkerhet och företagshemligheter eller annan känslig information. Vid bedömningen bör t.ex. vägas eventuella risker för att den brottsbekämpande myndigheten kan få del av uppgifter som helt saknar betydelse för det ärende åtgärden gäller eller uppgifter från personer som inte omfattas av ärendet. Dessutom bör det beaktas om uppgifterna förväntas vara av särskilt känslig karaktär. I så fall kan tillståndet begränsas till att avse endast vissa uppgifter (18 § första stycket 4).

Proportionalitetsprincipen gäller under hela verkställigheten och ska alltså, även sedan tillstånd getts, beaktas självmant och löpande av de brottsbekämpande myndigheterna (se SOU 1995:47 s. 324 och prop. 2005/06:178 s. 101). I situationer där integritetsintrånget under verkställigheten blir oproportionerligt stort måste avläsningen eller upptagningen avbrytas, trots att åtgärden fortfarande har betydelse för utredningen. Så kan t.ex. vara fallet om nyttan av den information som läses av eller tas upp inte står i proportion till den grad av integritetskränkning som åtgärden medför. Det kan bero på att antingen nyttan är låg eller integritetsintrånget särskilt högt eller en kombination av båda.

Hemlig dataavläsning under en förundersökning

4 § Ett tillstånd till hemlig dataavläsning får, om åtgärden är av synnerlig vikt för utredningen och inte annat anges i 6 § första stycket, beviljas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,
2. brott som avses i 27 kap. 2 § andra stycket 2–7 rättegångsbalken,
3. försök, förberedelse eller stämpling till brott som avses i 1 eller 2, om en sådan gärning är belagd med straff, eller
4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Om inte annat anges i 5 § får hemlig dataavläsning under en förundersökning endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för brottet. Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Hemlig dataavläsning som gäller kameraövervakningsuppgifter får användas endast på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Paragrafen reglerar under vilka förutsättningar tillstånd till hemlig dataavläsning får beviljas under en förundersökning. Övervägandena finns i avsnitt 10.1.2–10.1.5.

Av *första stycket* framgår vid vilka slags förundersökningar tillstånd till hemlig dataavläsning får beviljas. Inledningsvis ställer bestämmelsen som krav att åtgärden ska vara av synnerlig vikt för utredningen. Innebörden av kravet är detsamma som gäller för övriga hemliga tvångsmedel. Begreppet inrymmer ett kvalitetskrav avseende vilka upplysningar som åtgärden kan ge. Det ska finnas skäl att räkna med att avläsningen eller upptagningen – ensam eller i förening med andra åtgärder – verkligen kan få effekt. Kravet på synnerlig vikt betyder också att utredningsläget ska vara sådant att hemlig dataavläsning är nödvändig. Åtgärden får inte tillåtas om det som kan vinnas är åtkomligt med andra, mindre ingripande metoder. Synnerlig vikt kan anses föreligga om andra åtgärder inte är tillräckliga, väsentligt svårare att genomföra än hemlig dataavläsning eller förväntas leda till ett större integritetsintrång. Den som ansöker om hemlig dataavläsning måste därmed utreda eller tömma ut möjligheterna till andra åtgärder innan ansökan görs. Det är dock inte något krav att övriga tvångsmedel har prövats och misslyckats för att tillstånd till hemlig dataavläsning ska ges. Ett beslut om hemlig dataavläsning kräver vidare att det ska pågå en förundersökning, vilket stämmer överens med övrig reglering av hemliga tvångsmedel i rättegångsbalken. De brott som räknas upp i bestämmelsen är desamma som hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning får användas för (27 kap. 18 § andra stycket och 27 kap. 20 a § RB). Förundersökningen ska beträffande alla typer av uppgifter utom rumsavlyssningsuppgifter (se 6 §) avse sådan brottslighet. Hemlig dataavläsning får således inte tillåtas för att utreda något annat brott än vad som anges i bestämmelsen.

Enligt *punkt 1* får det inte vara föreskrivet lindrigare straff än fängelse i två år för att ett tillstånd till hemlig dataavläsning ska få beviljas.

Enligt *punkt 2* får tillstånd till hemlig dataavläsning även beviljas vid förundersökning om sådana samhällsfarliga brott som anges i 27 kap. 2 § andra stycket 2–7 RB, trots att strafftröskeln i punkt 1 inte uppnås.

Enligt *punkt 3* får vidare tillstånd till hemlig dataavläsning beviljas vid förundersökning om försök, förberedelse eller stämpling till brott som avses i punkterna 1 eller 2. Detta förutsätter att en sådan gärning är belagd med straff.

Av *punkt 4* följer att tillstånd till hemlig dataavläsning får beviljas även vid annan brottslighet än vad som nämns i punkt 1–3 om det kan antas att det aktuella brottets straffvärde överstiger fängelse i två år.

I *andra stycket första meningen* anges att det som huvudregel ska finnas en skäligen misstänkt för att tillstånd till hemlig dataavläsning ska få beviljas. Misstankegraden motsvarar vad som gäller för övriga hemliga tvångsmedel. Skälig misstanke är en lägre misstankegrad än sannolika skäl, vilket som huvudregel krävs för t.ex. häktning (24 kap. 1 § RB), men en högre misstankegrad än kan misstänkas, vilket krävs för att hålla kvar en misstänkt för förhör längre tid än annars (23 kap. 9 § RB). För att

hemlig dataavläsning ska tillåtas under en förundersökning krävs att den person som är föremål för åtgärden är skäligen misstänkt för ett konkret brott. Frågan om misstanken är tillräckligt stark bedöms efter omständigheterna i det enskilda fallet. Prövningen av styrkan i misstankarna måste grunda sig på en objektiv och allsidig bedömning av utredningsmaterialet. För att beviskravet ska vara uppfyllt krävs att det föreligger konkreta omständigheter som med viss styrka talar för misstanken (se t.ex. JO 1993/94 s. 101). Ett beslut om tvångsmedel kan aldrig grunda sig enbart på allmänna kunskaper om en persons livsföring eller hans eller hennes tidigare brottslighet.

Det ska vidare finnas en koppling mellan det avläsningsbara informationssystemet och den misstänkte. Detta uttrycks genom att det anges att den misstänkte ska använda det avläsningsbara informationssystemet eller att det annars ska finnas särskild anledning att anta att denne har använt eller kommer att använda det. Ett avläsningsbart informationssystem används exempelvis när den misstänkte utnyttjar det för att ringa, skicka meddelanden eller spara elektroniska uppgifter. Dessutom används det om den misstänkte via en mobiltelefon eller dator kopplar upp sig mot internet eller använder informationssystemet på annat sätt, t.ex. spelar spel eller gör anteckningar.

Det krävs inte att den misstänkte äger informationssystemet och inte heller att han eller hon är den ende personen som använder det. Om flera personer t.ex. gemensamt använder ett konto till en tjänst kan bestämmelsen tillämpas om den misstänkte är en av dem som använder kontot.

Om den misstänkte inte använder informationssystemet men det finns misstankar om att han eller hon har använt det eller kommer att använda det måste det finnas särskild anledning att anta denna omständighet. Med detta menas att utredningsläget ska visa någon faktisk omständighet som med viss styrka talar för att den misstänkte har använt eller kommer att använda informationssystemet under tillståndstiden.

I *andra stycket andra meningen* görs undantag från huvudregeln om att informationssystemet måste användas av en misstänkt. Undantaget gäller endast beträffande kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter, dvs. uppgiftstyper som får hämtas in genom hemlig avlyssning eller övervakning av elektronisk kommunikation. Hemlig dataavläsning får tillåtas för avläsning eller upptagning av sådana uppgifter i ett annat avläsningsbart informationssystem än ett som den misstänkte använder, om det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta det andra informationssystemet. Kravet på synnerlig anledning att anta är detsamma som gäller vid hemlig avlyssning eller övervakning av elektronisk kommunikation under motsvarande förhållanden och har samma innebörd som anges där (27 kap. 20 § första stycket 2 RB). Det innebär att bestämmelsen ska tillämpas restriktivt och att det på grund av tillförlitliga uppgifter ska vara så gott som säkert att den misstänkte kommer att ta kontakt med informationssystemet (prop. 2002/03:74 s. 49).

Kravet på synnerlig vikt för utredningen gäller även i detta undantagsfall. Vid prövningen av om en åtgärd är av synnerlig vikt i dessa fall bör det framför allt beaktas vilken brottslighet som utreds, vem som är misstänkt och om brottet alls kan utredas om åtgärden inte vidtas. I en

utredning om terrorismrelaterad eller grovt organiserad brottslighet är en sådan åtgärd inte sällan av synnerlig vikt. När det är fråga om annan brottslighet torde det tillhöra undantagsfallen att en dataavläsning mot någon annan än den misstänkte är av synnerlig vikt för utredningen.

Uttrycket att kontakta ett annat informationssystem innebär dock inte att kontakt med en server vid sedvanligt internetanvändande omfattas. Den brottsbekämpande myndigheten kan därmed inte använda hemlig dataavläsning i en server som den misstänkte anropar för att till exempel göra en sökning på internet med en sökmotor. Bestämmelsen tar i stället sikte på en riktad kontakt mellan informationssystem som t.ex. telefon, datorer eller e-postkonto som den misstänkte skickar meddelanden eller ringer till.

I *tredje stycket* anges att hemlig dataavläsning som gäller kameraövervakningsuppgifter endast får användas på en plats där den misstänkte kan antas komma att uppehålla sig. Det måste finnas en direkt koppling mellan den misstänkte och platsen, vilket motsvarar vad som gäller för hemlig kameraövervakning (27 kap. 20 b § RB). Det kan röra sig om flera platser och antalet platser kan utökas genom domstolsbeslut. I tredje stycket anges också att tillstånd till hemlig dataavläsning för att läsa av eller ta upp kameraövervakningsuppgifter inte får beviljas avseende någons stadigvarande boende. Förbudet är detsamma som för hemlig kameraövervakning enligt rättegångsbalken. Hemlig dataavläsning avseende kameraövervakningsuppgifter skiljer sig dock från hemlig kameraövervakning. Vid den senare åtgärden består installationsmomentet av montering av kameror som övervakar den misstänkte. Vid hemlig dataavläsning består installationen eller åtgärden av att aktivera en redan befintlig kamera i det informationssystem som den misstänkte använder. Ett sådant informationssystem kan t.ex. vara en dator, mobiltelefon eller läsplatta. Dessa är som huvudregel rörliga och det ankommer därmed på den brottsbekämpande myndigheten som ska verkställa åtgärden att kontrollera var informationssystemet befinner sig när åtgärden vidtas. Den som prövar ansökan om hemlig dataavläsning bör försäkra sig om att det är möjligt att respektera platskravet. Det är möjligt att respektera platskravet genom t.ex. fysisk spaning.

5 § Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter får även beviljas för att utreda vem som skäligen kan misstänkas för ett brott som avses i 4 §. Avläsning eller upptagning av kommunikationsövervakningsuppgifter får då endast avse förfluten tid.

Hemlig dataavläsning enligt första stycket får endast avse ett avläsningsbart informationssystem som har använts vid ett brott eller i anslutning till en brottsplats vid brottstidpunkten eller som av någon annan anledning är av synnerlig vikt för utredningen.

I paragrafen regleras att tillstånd till hemlig dataavläsning i vissa fall får beviljas för att utreda vem som skäligen kan misstänkas för brott och under vilka förhållanden en sådan åtgärd får vidtas. Övervägandena finns i avsnitt 10.1.5.

Av *första stycket* framgår att tillstånd till hemlig dataavläsning får beviljas när det inte finns en skäligen misstänkt för ett brott som avses i 4 § men för att utreda vem som kan vara skäligen misstänkt för ett sådant brott. I dessa fall får åtgärden endast avse sådana uppgiftstyper som hemlig

övervakning av elektronisk kommunikation kan ge tillgång till (kommunikationsövervaknings- och platsuppgifter). Om åtgärden används för avläsning eller upptagning av kommunikationsövervakningsuppgifter får den endast avse meddelanden som redan har skickats, alltså förfluten tid. För platsuppgifter finns dock inte någon sådan begränsning. Åtgärden måste, som framgår av 4 §, i samtliga fall vara av synnerlig vikt för utredningen.

Andra stycket föreskriver att det ska vara fråga om ett avläsningsbart informationssystem som antingen har använts vid ett brott, i anslutning till en brottsplats vid brottstidpunkten eller av annan anledning är av synnerlig vikt för utredningen.

Att det avläsningsbara informationssystemet har använts vid ett brott innebär att det haft avgörande betydelse vid själva genomförandet av brottet eller använts för att understödja brottet. Om polisen inom ramen för en förundersökning om t.ex. grovt narkotikabrott upptäcker en viss ip-adress varifrån det har förmedlats stora mängder narkotika kan tillstånd till hemlig dataavläsning beviljas för att utreda vem som är skäligen misstänkt för brottet. Likaså kan tillstånd ges för att utreda vem som är skäligen misstänkt för kapning med tekniskt hjälpmedel enligt 13 kap. 5 a § brottsbalken och 3 § 11 lagen (2003:148) om straff för terroristbrott. Att informationssystemet använts i anslutning till en brottsplats vid brottstidpunkten innebär typiskt sett att det har använts på eller vid en brottsplats när ett brott har begåtts. Det finns dock ingen avgränsning för hur stort område kring brottsplatsen som åtgärden får vidtas inom. Detta måste bedömas från fall till fall. Storleken på det geografiska område inom vilket informationssystemet ska ha funnits och använts varierar t.ex. beroende på om brottet har begåtts i en storstad eller på landsbygden samt vilken typ av brott som utreds.

Att informationssystemet på annat sätt är av synnerlig vikt för utredningen omfattar de fall när det inte står klart att informationssystemet befunnit sig vid eller i närheten av brottsplatsen, men ändå kan ha en avgörande betydelse i utredningen. Som exempel kan nämnas att ett informationssystem befunnit sig längs en flyktväg från brottsplatsen eller när det finns skäl att tro att gärningspersonen kan tänkas förflytta sig medan brottet fortfarande pågår, t.ex. vid människorov eller grov narkotikasmuggling.

6 § Ett tillstånd till hemlig dataavläsning som gäller rumsavlyssningsuppgifter får endast beviljas vid en förundersökning om brott som avses i 27 kap. 20 d § andra stycket rättegångsbalken.

Hemlig dataavläsning enligt första stycket får användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Om platsen är någon annan stadigvarande bostad än den misstänktes, får tillstånd till hemlig dataavläsning beviljas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.

Hemlig dataavläsning enligt första stycket får aldrig användas på en plats dit tillträdestillstånd enligt 13 § inte får beviljas.

I bestämmelsen anges förutsättningarna för tillstånd till hemlig dataavläsning för avläsning eller upptagning av rumsavlyssningsuppgifter. Övervägandena finns i avsnitt 10.1.2, 10.1.4 och 10.3.2.

Av *första stycket* framgår att tillstånd till hemlig dataavläsning som avser rumsavlyssningsuppgifter endast kan beviljas för de brott som nämns i 27 kap. 20 d § andra stycket RB, t.ex. spionerі och mord. Åtgärden får, som framgår av 4 §, endast vidtas mot en person som är skäligen misstänkt och åtgärden måste vara av synnerlig vikt för utredningen.

I *andra stycket* anges att en åtgärd enligt första stycket endast får användas på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Det är samma platskrav som gäller för hemlig rumsavlyssning enligt rättegångsbalken. Särskild anledning att anta innebär att det ska finnas någon faktisk omständighet som med viss styrka talar för att den misstänkte verkligen kommer att uppehålla sig på platsen i vart fall någon gång under tillståndstiden. Om platsen är någon annan stadigvarande bostad än den misstänktes får hemlig dataavläsning dock tillgripas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. Det innebär att man måste vara så gott som säker på att den misstänkte kommer att uppehålla sig på platsen någon gång under den tid som tillståndet gäller. Ett exempel där rekvisitet kan anses uppfyllt är om det genom yttre spaning framkommit omständigheter som visar att en misstänkt vid en viss bestämd tidpunkt brukar besöka en bekants bostad. Detta strängare krav gäller endast annan stadigvarande bostad än den misstänktes egen. Därmed gäller kravet inte när tillståndet avser tillfälliga bostäder såsom hotellrum, möteslokaler eller andra tillfälliga övernattningslokaler.

Den praktiska verkställigheten av hemlig dataavläsning för avläsning eller upptagning av rumsavlyssningsuppgifter skiljer sig åt från hemlig rumsavlyssning enligt rättegångsbalken. I de senare fallen monteras avlyssningsutrustning på en plats där den misstänkte förväntas befinna sig. Vid hemlig dataavläsning måste en funktion i informationssystemet aktiveras, t.ex. en mikrofon i en dator, mobiltelefon eller läsplatta. Den som ska pröva förutsättningarna för tillstånd bör således förhöra sig om hur den brottsbekämpande myndigheten tänkt att det ska gå till att ha kontroll så att informationssystemet finns på den plats tillståndet gäller och, om nödvändigt, meddela de särskilda villkor i tillståndet som behövs (18 §).

Av *tredje stycket* framgår att hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter aldrig får avse sådana platser dit tillträdestillstånd inte får beviljas. Även detta krav motsvarar vad som gäller för hemlig rumsavlyssning enligt rättegångsbalken. Se vidare om vilka platser som avses i kommentaren till 13 §.

Hemlig dataavläsning utanför en förundersökning

Förhindrande av vissa särskilt allvarliga brott

7 § Ett tillstånd till hemlig dataavläsning får beviljas om

1. det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar brott som anges i 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, eller

2. det finns en påtaglig risk för att sådan brottslig verksamhet kommer att utövas inom en organisation eller grupp och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Ett tillstånd enligt första stycket får beviljas endast om åtgärden är av synnerlig vikt för att förhindra sådan brottslig verksamhet som anges i det stycket.

Hemlig dataavläsning som gäller kameraövervakningsuppgifter får användas endast på en plats där den person som anges i första stycket kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Ett tillstånd får inte avse rumsavlyssningsuppgifter.

I paragrafen finns bestämmelser om vad som gäller för tillstånd till hemlig dataavläsning vid sådana förhållanden som kan ligga till grund för tillstånd till hemliga tvångsmedel enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen). Övervägandena finns i avsnitt 10.2.2.

Av *första stycket* framgår att tillstånd till hemlig dataavläsning får beviljas under samma förutsättningar som kan ligga till grund för tillstånd till hemliga tvångsmedel enligt preventivlagen. Enligt *första punkten* får tillstånd till hemlig dataavläsning beviljas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva sådan brottslig verksamhet som anges i 1 § preventivlagen, t.ex. spionerі och terroristbrott. Tillstånd till hemlig dataavläsning får enligt *andra punkten* också beviljas om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas sådan brottslig verksamhet som avses i första punkten och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet. Även detta motsvarar vad som gäller för tillstånd till hemliga tvångsmedel i preventivlagen.

Prövningen av om rekvisiten är uppfyllda får normalt göras på grundval av den information som inhämtats genom bl.a. polisens underrättelse- och spaningsverksamhet samt det internationella polissamarbetet (prop. 2005/06:177 s. 83).

Enligt *andra stycket* får tillstånd beviljas endast om åtgärden är av synnerlig vikt för att förhindra sådan brottslig verksamhet som anges i första stycket. Vad som avses med begreppet synnerlig vikt utvecklas i kommentaren till 4 § andra stycket. Bortsett från att syftet med förevarande bestämmelse inte är att utreda brott utan i stället att förhindra brott ska rekvisitet synnerlig vikt tolkas på samma sätt som anges där.

I *tredje stycket* föreskrivs ett platskrav och en särskild begränsning avseende platser som är någons stadigvarande bostad för de tillfällen då hemlig dataavläsning ska användas för att läsa av eller ta upp kameraövervakningsuppgifter. Platskravet och begränsningen motsvarar vad som föreskrivs i 4 § tredje stycket, dock med skillnaden att en sådan person som kan antas uppehålla sig på platsen inte är misstänkt utan i stället en sådan person som anges i första stycket.

Av *fjärde stycket* framgår att tillstånd enligt första stycket inte får avse hemlig dataavläsning för att ta upp rumsavlyssningsuppgifter. Det innebär att hemlig dataavläsning i preventivlagsfallen aldrig får användas för att läsa av eller ta upp uppgifter som kan hämtas in genom hemlig rumsavlyssning. Detta motsvarar vad som gäller enligt preventivlagen.

8 § Hemlig dataavläsning enligt 7 § får avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en person som anges i den bestämmelsen.

Hemlig dataavläsning som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att en person som

anges i 7 § under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Paragrafen innehåller bestämmelser om krav på koppling mellan ett avläsningsbart informationssystem och den enskilde vid tillstånd som avses i 7 § (preventivlagsfallen). Övervägandena finns i avsnitt 10.2.3.

Enligt *första stycket* får hemlig dataavläsning enligt 7 § avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en person som anges där, se kommentaren till 7 § första stycket. Vad gäller kopplingen mellan denne person och det avläsningsbara informationssystemet gäller det som anges i kommentaren till 4 § andra stycket.

Paragrafens *andra stycke* motsvarar 4 § andra stycket andra meningen, se kommentaren till den bestämmelsen**.**

Särskild utlänningskontroll

9 § Ett tillstånd till hemlig dataavläsning får beviljas för att läsa av eller ta upp uppgifter i ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av en utlänning som omfattas av

1. ett utvisningsbeslut enligt 1 § 2 lagen (1991:572) om särskild utlänningskontroll, eller
2. ett avvisnings- eller utvisningsbeslut enligt 8 eller 8 a kap. utlänningslagen (2005:716) eller motsvarande äldre bestämmelser och det finns sådana omständigheter i fråga om utlänningen som avses i 1 § 2 lagen om särskild utlänningskontroll.

Ett tillstånd till hemlig dataavläsning får också beviljas för att läsa av eller ta upp uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Tillståndet får beviljas endast om Migrationsverket, regeringen eller en domstol har beslutat att 19–22 §§ lagen om särskild utlänningskontroll samt denna lag ska tillämpas på utlänningen. Det förfarande och de förutsättningar som gäller för ett beslut om att 19–22 §§ lagen om särskild utlänningskontroll ska tillämpas i fråga om utlänningen gäller också för ett beslut i fråga om hemlig dataavläsning.

Ett tillstånd får beviljas endast om det finns synnerliga skäl och det är av betydelse för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott.

Ett tillstånd får inte avse kameraövervaknings- eller rumsavlyssningsuppgifter.

I paragrafen regleras vad som gäller för tillståndsgivning till hemlig dataavläsning när det finns förhållanden som kan ligga till grund för beslut om hemliga tvångsmedel enligt lagen (1991:572) om särskild utlänningskontroll (LSU-fallen). Övervägandena finns i avsnitt 10.2.4 och 10.2.5.

Av *första stycket* framgår att en första förutsättning för att hemlig dataavläsning ska få användas i LSU-fallen är att det antingen finns ett utvisningsbeslut enligt lagen om särskild utlänningskontroll eller att det finns ett avvisnings- eller utvisningsbeslut enligt utlänningslagen (2005:716) eller motsvarande äldre bestämmelser. Den första situationen som anges i första punkten är att den utlänning som åtgärden ska avse omfattas av ett

utvisningsbeslut enligt 1 § 2 LSU. Ett beslut om utvisning får enligt nämnda lagrum beviljas om det med hänsyn till vad som är känt om utlänningens tidigare verksamhet och övriga omständigheter kan befaras att han eller hon kommer att begå eller medverka till terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller försök, förberedelse eller stämpling till sådant brott. Hemlig dataavläsning kan även, enligt den andra punkten, beviljas om den aktuella utlänningen omfattas av ett avvisnings- eller utvisningsbeslut enligt 8 eller 8 a kap. utlänningslagen (2005:716) eller motsvarande äldre bestämmelser och det finns sådana omständigheter i fråga om utlänningen som avses i 1 § 2 lagen om särskild utlänningskontroll.

I första stycket finns även ett krav på koppling mellan utlänningen och det avläsningsbara informationssystem som åtgärden ska avse. Bestämmelsen är utformad på motsvarande sätt som bestämmelsen i 4 § med den skillnaden att den enskilde som är föremål för åtgärden inte är en misstänkt person utan den utlänning som omfattas av ett avvisnings- eller utvisningsbeslut. Vad gäller kopplingen som sådan är ingen skillnad avsedd i förhållande till vad som gäller enligt 4 §, se kommentaren till den bestämmelsen.

I *andra stycket* finns ett undantag från den nu nämnda huvudregeln att informationssystemet ska användas av den utlänning som är föremål för tvångsmedlet. Ett tillstånd till hemlig dataavläsning får nämligen också beviljas för att läsa av eller ta upp uppgifter i ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att utlänningen har kontaktat eller kommer att kontakta. Kontakterna måste äga rum eller ha ägt rum inom den tid tillståndet löper. Bestämmelsen ska tolkas på samma sätt som motsvarande bestämmelse i 4 § , se kommentaren till den bestämmelsen.

Av *tredje stycket* framgår att innan Stockholms tingsrätt, som är ensam behörig domstol i dessa fall, fattar ett beslut om att tillåta hemlig dataavläsning i ett specifikt fall krävs att Migrationsverket, regeringen eller en domstol, på någon av de grunder som anges i lagen om särskild utlänningskontroll, har fattat ett generellt beslut om att tvångsmedel enligt 19–22 §§ LSU samt hemlig dataavläsning ska få tillämpas i fråga om utlänningen (jfr 11, 11 a, 14 och 15 §§ LSU). Av andra stycket framgår vidare att Migrationsverket, regeringen eller domstol ska följa samma förfaranderegler vid ett generellt beslut om att tillåta hemlig dataavläsning som vid ett generellt beslut om att tillåta andra tvångsmedel enligt lagen om särskild utlänningskontroll. Även samma förutsättningar ska gälla för beslutet om hemlig dataavläsning. Att samma förfaranderegler blir tillämpliga innebär t.ex. att ett generellt beslut om att tillåta hemlig dataavläsning går att överklaga till regeringen (11 § fjärde stycket LSU och 11 a § andra stycket LSU) och att domstol får besluta interimistiskt (15 § LSU).

Av *fjärde stycket* följer att ett tillstånd till hemlig dataavläsning i LSU-fallen endast får beviljas om det finns synnerliga skäl och det är av betydelse för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott. Det är således endast möjligt att ge tillstånd till hemlig dataavläsning i LSU-fallen för att utreda om en i första stycket angiven person eller en organisation eller grupp han eller hon tillhör planerar sådan brottslighet som anges i den lagen.

I *femte stycket* anges att ett tillstånd till hemlig dataavläsning i LSU-fallen inte får avse kameraövervaknings- eller rumsavlyssningsuppgifter. I den delen motsvarar bestämmelsen vad som gäller enligt lagen om särskild utlänningskontroll, vilken inte möjliggör hemlig kameraövervakning eller hemlig rumsavlyssning. Av det följer motsatsvis att hemlig dataavläsning får användas för att läsa av eller ta upp övriga uppgiftstyper enligt 2 § första stycket lagen om hemlig dataavläsning, om förutsättningarna enligt bestämmelsen är uppfyllda.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

10 § Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter får beviljas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i 2 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Vid hemlig dataavläsning enligt första stycket får meddelanden inte hindras att nå fram enligt 2 § andra stycket.

Ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervakningsuppgifter får endast avse uppgifter i förfluten tid.

I paragrafen regleras att tillstånd till hemlig dataavläsning i vissa fall får beviljas för avläsning eller upptagning av uppgifter i underrättelseverksamhet (inhämtningslagsfallen), motsvarande de som gäller för inhämtning av sådana uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Övervägandena finns i avsnitt 10.2.6 och 10.2.7.

Enligt *första stycket* får för det första hemlig dataavläsning i inhämtningslagsfallen endast avse kommunikationsövervakningsuppgifter och platsuppgifter. Det ställs vidare som krav att åtgärden ska vara av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i 2 § inhämtningslagen. Det är fråga om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller vissa särskilt angivna brott, t.ex. spionerі och kapning. Till skillnad från vad som gäller enligt inhämtningslagen ska åtgärden vara av synnerlig vikt för att tillstånd ska komma i fråga. Synnerlig vikt har samma innebörd som när uttrycket används i andra sammanhang i denna lag (se kommentaren till 4 § första stycket). Synnerlig vikt i detta sammanhang tar sikte på förebyggandet, förhindrandet eller upptäckandet av den brottsliga verksamheten i stället för utredningen, vilket är fallet under en förundersökning. Uttrycket förebygga, förhindra eller upptäcka brottslig verksamhet har samma betydelse som redovisats i förarbetena till inhämtningslagen (prop. 2011/12:55 s. 121). Enligt definitionen av hemlig dataavläsning (1 §) får åtgärder enligt förevarande bestämmelse endast avse uppgifter i ett avläsningsbart informationssystem. Det ställs inte några krav på att informationssystemet ska kunna kopplas till en viss person. Det innebär att det inte är nödvändigt att veta vem som använder informationssystemet men att det måste stå klart att avläsning eller upptagning sker ifrån ett visst avläsningsbart informationssystem.

I *andra stycket* finns en begränsning som innebär att när hemlig dataavläsning används i inhämtningslagsfallen får den brottsbekämpande

myndigheten inte hindra meddelanden från att nå fram enligt 2 § andra stycket. Det är inte heller tillåtet enligt inhämtningslagen.

Enligt *tredje stycket* får avläsning eller upptagning av kommunikationsövervakningsuppgifter endast avse uppgifter om meddelanden i förfluten tid, dvs. som har överförts, och alltså inte uppgifter om meddelanden i realtid. Det motsvarar vad som gäller enligt inhämtningslagen för sådana uppgifter (1 § 1 inhämtningslagen och prop. 2011/12:55 s. 120 och 129–130).

Förbud mot hemlig dataavläsning

11 § Ett tillstånd till hemlig dataavläsning får inte avse ett avläsningsbart informationssystem som stadigvarande används eller är särskilt avsett att användas

1. i verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,
2. i verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller
3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, i verksamhet för bikt eller enskild själavård.

I paragrafen anges begränsningar som innebär att hemlig dataavläsning aldrig får avse vissa avläsningsbara informationssystem. Övervägandena finns i avsnitt 10.3.2.

Bestämmelsen består av tre punkter som klargör att det finns ett absolut förbud mot hemlig dataavläsning avseende vissa avläsningsbara informationssystem. Bestämmelsen omfattar alla uppgiftstyper som hemlig dataavläsning kan ge tillgång till. För samtliga punkter gäller att informationssystemet stadigvarande ska användas eller vara särskilt avsett att användas i en i respektive punkt angiven verksamhet, vilket är detsamma som gäller för platser där hemlig rumsavlyssning inte får äga rum (27 kap. 20 e § tredje stycket RB). För att informationssystemet ska ha den i lagen angivna priviligierade ställningen krävs att det är en beständig del av verksamheten och används i något av dess syften eller att det är särskilt avsett att användas i verksamheten. Att ett informationssystem är särskilt avsett att användas i verksamheten kan omfatta fall då t.ex. en advokat ännu inte har startat sin verksamhet men har tagit med sig en klientdatabas från en annan arbetsgivare och lagrat denna i ett informationssystem.

Däremot omfattas typiskt sett inte anställdas privata mobiltelefoner eller datorer även om de vid enstaka fall används i verksamheten. Om det vid verkställighet av hemlig dataavläsning kommer fram uppgifter som enligt 27 § inte får läsas av eller tas upp gäller dock att verkställigheten ska avbrytas och upptagningar och uppteckningar förstöras i delar de omfattas av förbudet, se kommentaren till den bestämmelsen. Informationssystem som endast undantags- eller tillfälligtvis används i verksamheten eller är till för personer utanför verksamheten omfattas inte heller av förbudsregeln, t.ex. besöksdatorer på en läkarmottagning eller liknande inrättning. Stadigvarande användning behöver dock inte vara begränsad till att avse arbetsplatser inom den organisation som skyddas utan kan också omfatta t.ex. en arbetsplats i en journalists hem (prop. 2013/14:237 s. 180). Eftersom förbudet tar sikte på det avläsningsbara informationssystemet som

sådant och aldrig på vilken plats det befinner sig är den fysiska arbetsplatsen inte för någon av yrkesgrupperna avgörande för om informationssystemet kan bli föremål för hemlig dataavläsning. Inte heller har det betydelse om utrustningen befinner sig utanför arbetsplatsen, vilket inte sällan t.ex. en mobiltelefon eller en bärbar dator gör. Det avgörande är om informationssystemet stadigvarande används eller är särskilt avsett att användas i de angivna verksamheterna. Det innebär också att det inte är möjligt att undgå hemlig dataavläsning endast genom att tillfälligtvis använda ett informationssystem i sådan skyddad verksamhet som avses i bestämmelsen (jfr prop. 2005/06:178 s. 102).

När det gäller de enskilda punkterna och de verksamheter som anges i dessa är det samma verksamheter som anges i 27 kap. 20 e § tredje stycket RB, dvs. där rumsavlyssning inte får förekomma.

Punkt 1 avser verksamheter där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen. Här avses primärt medieföretag, t.ex. förlag eller nyhetsbyråer, som bedriver verksamhet för vilken det råder tystnadsplikt enligt reglerna i tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Punkt 2 avser verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen. Det innebär att hemlig dataavläsning inte får avse t.ex. digitala journalsystem hos läkare, tandläkare och annan sjukvårdspersonal eller klientinformation hos en advokat eller familjerådgivare hos socialtjänst. Begreppet advokat innefattar i detta sammanhang även den som är auktoriserad som advokat i någon annan stat inom Europeiska unionen, Europeiska ekonomiska samarbetsområdet eller i Schweiz när denne är verksam i Sverige (8 kap. 9 § RB).

Punkt 3 tar sikte på avläsningsbara informationssystem som används av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund. Punkten avser dock endast informationssystem som används i verksamhet för bikt eller enskild själavård.

Vid tillståndsprövningen ankommer det på den brottsbekämpande myndigheten att presentera uppgifter som tydliggör att informationssystemet inte omfattas av förbudsregeln, om det finns en sådan risk. Om det efter ett beviljat tillstånd visar sig att ett förbjudet informationssystem kommer att utsättas eller utsätts för hemlig dataavläsning måste åtgärden omedelbart avbrytas.

Tillträdestillstånd

12 § Vid hemlig dataavläsning får den verkställande myndigheten, efter särskilt tillstånd, i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd får endast avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller en sådan person som anges i 7 § första stycket eller 9 § första stycket, får tillstånd beviljas endast om det finns synnerlig anledning att anta att informationssystemet finns där.

I paragrafen regleras förutsättningarna för att en domstol eller, i förekommande fall, en åklagare ska kunna ge ett särskilt tillstånd för tillträde

(tillträdestillstånd) till annars skyddade platser. Övervägandena finns i avsnitt 10.4.

I paragrafen anges förutsättningarna för att bevilja ett tillträdestillstånd för att hemlig dataavläsning ska kunna verkställas. Det slås för det första fast att tillträdestillstånd får beviljas för att i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Med tekniskt hjälpmedel avses både hårdvara och programvara. Bestämmelsen innebär att installationen ska göras på plats och medger inte den verkställande myndigheten rätt att ta med sig informationssystemet därifrån. Bestämmelsen avser huvudsakligen de platser som skyddas genom bestämmelserna i 4 kap. 6 § brottsbalken om hemfridsbrott och olaga intrång. Det är således inte bara fråga om bostäder utan också om bl.a. arbetsplatser, föreningslokaler och bilar. Bestämmelsen innebär också att tillträdestillstånd får ges till plats som skyddas genom bestämmelsen i 8 kap. 8 § brottsbalken om egenmäktigt förfarande, vilket ger de brottsbekämpande myndigheterna rätt att, utan att behålla egendomen, fästa eller bryta lås eller på något annat sätt rubba någons egendom, t.ex. öppna en låst väska där det finns särskild anledning att anta att det eftersökta informationssystemet finns. I likhet med vad som gäller enligt bestämmelserna om husrannsakan och tillträdestillstånd vid hemlig rumsavlyssning får den brottsbekämpande myndigheten ta sig in i det skyddade utrymmet med våld. Den får alltså – om det anses nödvändigt – bryta eller dyrka sig in i t.ex. en bostad eller ett annat utrymme som tillståndet gäller för att genomföra installationen (eller avinstallationen, se 25 § fjärde stycket). Detta innefattar en befogenhet att tillfälligtvis sätta larmanordningar ur funktion (prop. 2005/06:178 s. 104–105).

Ett tillträdestillstånd är ett särskilt tillstånd som ges av den som beviljar beslut om hemlig dataavläsning och ska anges i beslutet (se kommentaren till 18 §). Som framgår av 14 och 17 §§ kan beslut beviljas av såväl rätten som åklagaren.

Av paragrafen framgår också att ett tillstånd endast får avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Kravet på att informationssystemet ska finnas tillgängligt innebär inte att det behöver finnas fysiskt tillgängligt på den plats där tillträdet äger rum. Det kan i vissa fall vara så att det tekniska hjälpmedlet kan installeras på distans, t.ex. via en kopplingsstation i källaren i ett flerbostadshus, i stället för att den verkställande myndigheten bryter sig in i bostaden där informationssystemet finns. Det följer då av proportionalitetsprincipen att den förra verkställighetsmetoden ska väljas. Det kan också vara så att avläsningen behöver göras genom en kopplingsstation men avse uppgifter i en misstänkts dator i en annan del av huset eller i ett annat hus (se kommentaren till 1 §). I båda dessa fall får tillträdestillstånd beviljas för att fysiskt få tillgång till kopplingsstationen.

Kravet på särskild anledning att anta innebär att det inte bara ska vara fråga om ett allmänt antagande om att informationssystemet kommer att finnas på platsen utan det ska finnas någon faktisk omständighet som med viss styrka talar för att det kommer att finnas där i vart fall någon gång under tillståndstiden.

Är platsen i fråga någon annan stadigvarande bostad än den misstänktes får tillträdestillstånd endast beviljas om det finns synnerlig anledning att

anta att informationssystemet finns där. Detta gäller även i preventivlagsfallen och LSU-fallen, om bostaden stadigvarande används av en annan person än den som är föremål för åtgärden. Med synnerlig anledning avses att man ska vara praktiskt taget säker på att informationssystemet finns på platsen. Det strängare kravet avser endast bostäder som stadigvarande används av någon annan än den som är föremål för hemlig dataavläsning. Därmed gäller inte kravet när åtgärden ska riktas mot den misstänktes bostad, en bostad som stadigvarande används av en person som är föremål för åtgärden i preventivlags- eller LSU-fallen eller mot tillfälliga bostäder, såsom hotellrum eller andra tillfälliga sovarrangemang i t.ex. möteslokaler eller andra liknande platser.

Vid tillträdestillstånd till en stadigvarande bostad i inhämtningslagsfallen gäller alltid det strängare kravet på att det ska finnas synnerlig anledning att anta att informationssystemet finns där, vilket framgår av att en person som omfattas av inhämtning enligt inhämtningslagen inte är misstänkt och inte heller en sådan person som nämns i 7 § första stycket eller 9 § första stycket.

Ett beslut om tillträdestillstånd gäller för hela tillståndstiden (om inte annat beslutas) och även efter tillståndstidens utgång till den del det avser borttagande eller avinstallation av det tekniska hjälpmedlet (25 § tredje stycket).

13 § Ett tillträdestillstånd enligt 12 § får inte avse en plats som stadigvarande används eller är särskilt avsedd att användas

1. för verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,
2. för verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller
3. av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, för bikt eller enskild själavård.

I bestämmelsen regleras vilka platser som alltid är fredade mot tillträdestillstånd enligt 12 §. Övervägandena finns i avsnitt 10.3.2 och 10.4.

Av paragrafen framgår att ett tillträdestillstånd aldrig får avse platser som stadigvarande används eller är särskilt avsedda att användas för sådana verksamheter som anges i 11 §, se kommentaren till den paragrafen. Kravet på att en plats stadigvarande används eller är särskilt avsedd att användas för det fredade ändamålet medför att det inte är möjligt att undvika ett tillträdestillstånd endast genom att tillfälligtvis upplåta eller inrätta en lokal för sådan skyddad verksamhet (prop. 2005/06:178 s. 102).

När det gäller platser som är fredade från hemlig dataavläsning på grund av att de används för bikt eller enskild själavård kan följande anföras. Det fredade utrymmet är endast det begränsade utrymme som är avsett för bikt eller själavård. Det förhållandet att en präst kan hålla ett själavårdande samtal i en kyrkbänk innebär inte att platsen är fredad från hemlig dataavläsning. Däremot bör aldrig ett biktbås eller ett rum särskilt inrättat för själavård kunna bli föremål för hemlig dataavläsning, jfr betänkandet Rättssäkerhetsgarantier och hemliga tvångsmedel (SOU 2018:61 s. 166).

Tillståndsprövning

14 § Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagare. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen eller Polismyndigheten.

I paragrafen finns regler om att rätten prövar ansökan om hemlig dataavläsning och om vem som ska göra ansökan. Övervägandena finns i avsnitt 11.1.1–11.1.2.

Av paragrafen följer att frågor om hemlig dataavläsning alltid ska prövas av rätten. Ordningen är densamma som för övriga hemliga tvångsmedel med det undantaget att rätten fattar beslut om hemlig dataavläsning även i inhämtningslagsfallen.

Bestämmelsen innebär att åklagaren ansöker om tillstånd i samtliga fall utom när ansökan avser hemlig dataavläsning i LSU-fallen. En sådan ansökan ska i stället göras av Säkerhetspolisen eller Polismyndigheten. Att åklagaren gör ansökan i övriga fall innebär att denne också ansöker om tillstånd till hemlig dataavläsning i inhämtningslagsfallen, vilket skiljer sig från ordningen i inhämtningslagen.

15 § Frågor om hemlig dataavläsning under en förundersökning prövas av den domstol som anges i 19 kap. rättegångsbalken. Om förundersökningen avser brott som anges i 27 kap. 2 § andra stycket 2–8 rättegångsbalken får frågan även prövas av Stockholms tingsrätt.

Frågor om hemlig dataavläsning enligt 7–10 §§ ska alltid prövas av Stockholms tingsrätt.

Paragrafen anger vilken domstol som är behörig att pröva frågor om tillstånd till hemlig dataavläsning. Övervägandena finns i avsnitt 11.1.1.

De forumregler som anges i bestämmelsen motsvarar befintliga forumregler, både under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll (dock ej inhämtning enligt inhämtningslagen som inte prövas av domstol).

Enligt *första stycket* ska den domstol som framgår av 19 kap. RB vara behörig att pröva frågor om hemlig dataavläsning när en förundersökning pågår. Som huvudregel är således rätten i den ort där brottet förövades behörig. Om det är lämpligt, får prövningen i stället göras där den misstänkte har hemvist eller mera varaktigt uppehåller sig. I vissa brådskande fall får frågor om tvångsmedel prövas även av domstol på annan ort (se 19 kap. 1 och 12 §§ RB). Om förundersökningen avser brottslighet som anges i 27 kap. 2 § andra stycket 2–8 RB (samhällsfarlig brottslighet) får frågan prövas av Stockholms tingsrätt. Det innebär att Stockholms tingsrätt alltid har behörighet att pröva dessa frågor och motsvarar vad som gäller om Stockholms tingsrätts behörighet för övriga hemliga tvångsmedel i 27 kap. 34 § RB.

Av *andra stycket* framgår att Stockholms tingsrätt är exklusivt forum för frågor om hemlig dataavläsning i underrättelseverksamhet och vid särskild utlänningskontroll. Bestämmelsen motsvarar 6 § preventivlagen och 21 § andra stycket LSU. Bestämmelsen avviker dock från vad som föreskrivs om beslutsordningen i inhämtningslagen, vilken aldrig kräver domstolsbeslut.

16 § När en ansökan eller anmälan om hemlig dataavläsning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet ska den som gjort ansökan och det offentliga ombudet närvara.

För offentliga ombud i ärenden om hemlig dataavläsning gäller 27 kap. 26 och 27 §§, 28 § andra stycket samt 29 och 30 §§ rättegångsbalken.

I paragrafen finns bestämmelser om sammanträde och offentliga ombud vid domstolsprövningen av hemlig dataavläsning samt om handläggningen i övrigt av ärenden om hemlig dataavläsning. Övervägandena finns i avsnitt 11.1.3.

Av *första stycket* framgår att när en ansökan eller anmälan (enligt 17 §) om hemlig dataavläsning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Bestämmelsen innebär att ett offentligt ombud alltid ska närvara vid domstolsprövningen av ansökan om hemlig dataavläsning. Bestämmelsen avviker därmed till viss del från andra bestämmelser om hemliga tvångsmedel, eftersom offentliga ombud annars inte deltar i ärenden som gäller hemlig övervakning av elektronisk kommunikation eller vid prövningen av inhämtning enligt inhämtningslagen. Vid hemlig dataavläsning finns emellertid inga undantag från det offentliga ombudets närvaroplikt. Det innebär att ett offentligt ombud ska närvara såväl vid grundbeslutet om hemlig dataavläsning som vid eventuella kompletterande beslut. Även den som gjort ansökan ska närvara vid sammanträdet. Den som gjort ansökan är åklagaren i alla fall utom i LSU-fallen. Då är det i stället Säkerhetspolisen eller Polismyndigheten som ansöker om tillstånd (14 § andra meningen).

I *andra stycket* anges att för offentliga ombud gäller rättegångsbalkens bestämmelser om offentliga ombud. Av dessa framgår det offentliga ombudets roll i förfarandet. Han eller hon ska således i enlighet med 27 kap. 26 § RB bevaka enskildas integritetsintressen i ärenden om hemlig dataavläsning och har rätt att ta del av det som förekommer i ärendet, yttra sig och överklaga rättens beslut. Vidare innebär hänvisningarna att den förordnandeprocedur som följer av 27 kap. 27 § RB gäller för offentliga ombud även enligt denna lag. Enligt 27 kap. 28 § andra stycket RB gäller ett uppdrag som offentligt ombud även i högre rätt. Även reglerna om ersättning till det offentliga ombudet och om tystnadsplikt i 27 kap. 29 och 30 §§ RB gäller för offentliga ombud enligt denna lag.

17 § Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens tillstånd i frågor om hemlig dataavläsning, får tillstånd ges av åklagaren i avvaktan på rättens beslut. Ett sådant tillstånd får dock aldrig avse hemlig dataavläsning som gäller rumsavlyssningsuppgifter eller hemlig dataavläsning vid särskild utlänningskontroll enligt 9 §.

Om åklagaren har gett ett tillstånd enligt första stycket, ska åklagaren utan dröjsmål skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de uppgifter som lästs av eller tagits upp inte

användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

I paragrafen finns bestämmelser om möjligheten för åklagaren att bevilja interimistiska beslut om hemlig dataavläsning och om rättens prövning av sådana beslut. Övervägandena finns i avsnitt 11.1.4.

Av *första stycket* framgår att åklagaren får bevilja ett interimistiskt beslut om hemlig dataavläsning. Förutsättningarna för detta är desamma som gäller för andra interimistiska beslut om hemliga tvångsmedel (27 kap. 21 a § RB och 6 a § preventivlagen).

En förutsättning för ett interimistiskt beslut är att det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga, förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens tillstånd. Med detta avses detsamma som i rättegångsbalken, inhämtningslagen och preventivlagen. Det innebär att det endast är i situationer när ändamålet med åtgärden riskerar att gå förlorat om rättens tillstånd skulle avvaktas som ett interimistiskt beslut får beviljas. Interimistiska beslut ska således beviljas endast i undantagsfall. Sådant undantag kan t.ex. aktualiseras vid tidpunkter då det inte går att få en domstolsprövning inom domstolarnas öppettider och åtgärden inte kan avvakta. På samma sätt kan det finnas behov av interimistiska beslut om behovet uppstår under domstolens öppettider men förfarandet befaras ta så lång tid att ändamålet med åtgärden riskerar att gå förlorat. Så kan vara fallet om sammanträdet (se 16 §) inte kan hållas tillräckligt snabbt, t.ex. om det tar lång tid att uppfylla kravet på att ett offentligt ombud ska medverka vid sammanträdet.

På åklagarens beslut ställs samma krav som på rättens beslut (18 §).

Åklagaren har samma möjlighet som rätten att bevilja grundbeslut om hemlig dataavläsning, beslut om tillträdestillstånd samt kompletterande beslut. Av första stycket framgår att interimistiska beslut inte får beviljas beträffande hemlig dataavläsning som gäller rumsavlyssningsuppgifter eller i LSU-fallen (9 §). Detsamma gäller för hemlig rumsavlyssning enligt 27 kap. 21 a § RB och för hemliga tvångsmedel enligt lagen om särskild utlänningskontroll. Interimistiska åklagarbeslut om hemlig dataavläsning får alltså beviljas under en förundersökning för samtliga uppgiftstyper utom rumsavlyssningsuppgifter samt i preventivlags- och inhämtningslagsfallen.

Andra stycket om rättens prövning motsvarar vad som anges i 27 kap. 21 a § andra stycket RB och 6 a § andra stycket preventivlagen och ska tillämpas på samma sätt som dessa bestämmelser. Om åklagaren har beviljat interimistiskt tillstånd till hemlig dataavläsning ska han eller hon utan dröjsmål skriftligt anmäla beslutet till rätten. Att anmälan ska göras utan dröjsmål innebär att den ska göras så snart någon hos domstolen kan ta emot den. Vid interimistiska beslut som beviljas under domstolens öppettider ska anmälan därmed normalt göras i samband med att beslutet beviljas, enligt propositionen Hemliga tvångsmedel mot allvarliga brott (prop. 2013/14:237 s. 183). Skälen för åtgärden ska anges i anmälan och rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet. Hemlig dataavläsning får då inte verkställas med stöd av åklagarens interimistiska beslut och eventuellt pågående avläsning ska omedelbart avbrytas.

Av *tredje stycket* framgår att rätten, om åklagarens beslut har verkställts innan rätten gjort en prövning enligt andra stycket, ska pröva om det funnits skäl för åtgärden. Vissa åtgärder inom hemlig dataavläsning kan vidtas tämligen omgående, t.ex. avläsning eller upptagning av lagrade uppgifter från ett avläsningsbart informationssystem. Rättens bedömning ska göras utifrån de förhållanden som förelåg vid tidpunkten för åklagarens beslut. Även om rätten finner att skäl för åtgärden saknades vid den tidpunkten, kan förhållandena ha ändrats så att förutsättningar för tvångsmedlet finns vid rättens prövning. Bestämmelsen hindrar i dessa fall inte att rätten, eller åklagaren i förekommande fall, fattar ett nytt beslut om tillstånd till hemlig dataavläsning. Inte heller hindrar bestämmelsen att uppgifter som på grund av rättens beslut inte får användas kan hämtas in på nytt med stöd av ett senare beviljat tillstånd (prop. 2013/14:237 s. 183–184).

Om rätten finner att det saknats skäl för tillstånd, t.ex. ett tillträdestillstånd, vid tidpunkten för åklagarens prövning, får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser. Med någon annan som uppgifterna avser menas t.ex. en person som nämns när två eller flera misstänkta talar om brottslig verksamhet utan att han eller hon själv utsatts för hemlig dataavläsning (prop. 2013/14:237 s. 183). På samma sätt skyddas en person som inte varit föremål för hemlig dataavläsning men t.ex. nämns i inhämtade dokument, syns på videor eller fotografier om sådana uppgifter har lästs av eller tagits upp. Att uppgifterna inte får användas i en brottsutredning avser användning både i en förundersökning och i en sådan utredning som avses i 23 kap. 22 § RB. Uppgifterna får däremot användas om de kan fria den berörde från brottsmisstankar eller på annat sätt användas till dennes fördel. Det finns inte heller något hinder mot att uppgifterna används i underrättelseverksamhet.

18 § I ett tillstånd till hemlig dataavläsning ska följande anges:

1. vilken tid tillståndet avser,
2. vilket avläsningsbart informationssystem tillståndet avser,
3. vilken typ av uppgift enligt 2 § första stycket som får läsas av eller tas upp,
4. villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, och
5. vem som är skäligen misstänkt för brottet, vid åtgärd som gäller rumsavlyssningsuppgifter.

Om tillståndet avser en plats enligt 4 § tredje stycket eller 6 § andra stycket ska även platsen anges i tillståndet. Om tillståndet är förenat med ett tillträdestillstånd enligt 12 §, ska det anges i beslutet.

Tiden för tillståndet får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet.

Paragrafen reglerar vad ett beslut om tillstånd till hemlig dataavläsning ska innehålla. Övervägandena finns i avsnitt 11.1.5.

I *första stycket* anges vad som ska framgå av ett beslut om hemlig dataavläsning.

Enligt *punkt 1* ska det av beslutet framgå vilken tid tillståndet avser. Vid bestämmande av tid måste begränsningen i tredje stycket beaktas.

Enligt *punkt 2* ska det i tillståndet anges vilket avläsningsbart informationssystem som tillståndet avser. Det betyder att det i tillståndet måste

anges vilket specifikt informationssystem tillståndet gäller för. Det kan ske genom att exempelvis ett visst serienummer, IMEI-nummer, MAC-adress eller andra uppgifter som möjliggör identifiering anges. Uppgifterna måste i vart fall vara så specificerade att det går att verkställa åtgärden och att det är möjligt att bedöma kopplingen mellan informationssystemet och den som åtgärden avser, när sådan prövning krävs, för att utesluta förväxlingsrisk med andra informationssystem. När tillståndet gäller icke-fysiska informationssystem anges lämpligen det användarkonto eller andra avgränsade delar av tjänsterna som åtgärden ska vidtas i. Det kan vara t.ex. en e-postadress, ett användarnamn till ett konto på sociala medier eller annan internetbaserad tjänst. Även i dessa fall måste uppgifterna vara så specificerade att det går att verkställa åtgärden och förhindra förväxlingsrisk.

Punkt 3 föreskriver att det ska anges i tillståndet vilken typ av uppgift enligt 2 § första stycket som tillståndet avser. Därmed klargörs vad åtgärden får användas för och vilka typer av uppgifter som får läsas av eller tas upp. Det har stor betydelse för vilka anpassningar av verkställighetstekniken som ska göras enligt 24 § första stycket. När hemlig dataavläsning får användas för avläsning eller upptagning av mer än en uppgiftstyp samtidigt ska samtliga uppgiftstyper som får läsas av eller tas upp framgå av tillståndet. Att det i tillståndet ska anges vilken uppgiftstyp som hemlig dataavläsning i det enskilda fallet får avse innebär i praktiken att den som ansöker om tillstånd måste ange vilken uppgiftstyp som ansökan avser.

Enligt *punkt 4* ska beslutet innehålla villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Villkoren kan vara av teknisk karaktär, t.ex. en föreskrift om att den brottsbekämpande myndigheten som ska verkställa en åtgärd på en viss utpekad plats (kameraövervaknings- eller rumsavlyssningsuppgifter) måste göra det tekniskt omöjligt att genomföra hemlig dataavläsning på annan plats än den som tillståndet avser. Villkoren kan också vara av annan karaktär, såsom att endast samtal med en viss person får vara föremål för hemlig dataavläsning eller att tillståndet endast får avse inkommande samtal. Vidare kan det uppställas villkor för att begränsa vilka uppgifter som får läsas av eller tas upp, exempelvis genom att det i tillståndet anges att endast lagrade uppgifter av viss filtyp, viss karaktär eller med viss beteckning omfattas.

Av *punkt 5* följer att, när avläsning eller upptagning avser rumsavlyssningsuppgifter, ska namnet på den som är skäligen misstänkt anges i tillståndet. Det motsvarar vad som gäller enligt 27 kap. 21 § femte stycket RB vid tillstånd till hemlig rumsavlyssning.

I *andra stycket* finns bestämmelser om att det ska anges en plats för tillståndet när hemlig dataavläsning ska användas för att läsa av eller ta upp kameraövervakningsuppgifter eller rumsavlyssningsuppgifter, se 4 § tredje stycket samt 6 § andra stycket. Kravet motsvarar vad som gäller för hemlig kameraövervakning och hemlig rumsavlyssning enligt 27 kap. 21 § fjärde stycket RB och, för hemlig kameraövervakning, enligt 8 § tredje stycket preventivlagen. Bestämmelsen ska tillämpas på motsvarande sätt. Av andra stycket framgår också att om ett tillträdestillstånd beviljas ska det framgå vilken plats det gäller för. Kravet på att ange en viss plats måste anpassas till vad tillträdestillståndet avser. Om det avser en bostad eller ett kontor ska den exakta adressen anges. Om tillträdestillståndet däremot avser ett förvaringsskåp bland många behöver inte det

specifika skåpet pekas ut utan det räcker att det i tillståndet anges att det avser ett förvaringsskåp i ett visst omklädningsrum eller liknande. För det fall tillträdestillståndet avser en bil behöver inte den geografiska platsen anges utan det räcker med att fordonet individualiseras.

Liksom för övriga hemliga tvångsmedel gäller enligt *tredje stycket* att tiden inte får bestämmas längre än nödvändigt. När rätten bestämmer vad som är en nödvändig tidsram, får hänsyn tas till den tid som kan behövas för att installation eller motsvarande ska kunna utföras och att åtgärden ska bli användbar. I flera fall kommer det finnas behov av att förbereda verkställigheten. Vissa åtgärder kommer inte kunna företas innan tillstånd har lämnats. Om det inte krävs några mera omfattande förberedelser kan det i vissa fall finnas skäl att begränsa tillståndet till tämligen kort tid. Så kan vara fallet när tillståndet avser åtgärd enligt 2 § första stycket 6 (lagrade uppgifter) eftersom målet med åtgärden då kan vara uppfyllt när själva avläsningen eller upptagningen av den lagrade informationen är utförd.

Enligt bestämmelsen gäller en bortre tidsgräns om en månad från dagen för tillståndsbeslutet. Det finns dock inte någon lagstadgad bortre tidsgräns för tiden innan tillståndet beviljades. Detta kan få betydelse när lagrade uppgifter ska läsas av eller tas upp samt när historiska meddelanden, historiska uppgifter om meddelanden och historiska platsuppgifter får läsas av eller tas upp enligt tillståndet. En tidsgräns avseende meddelanden är tämligen enkelt att ställa upp, t.ex. genom att inskränka tillståndet till att avse meddelanden som skickats eller tagits emot endast efter en viss tidpunkt. När det däremot gäller lagrade filer, t.ex. textdokument kan saken vara svårare. Sådana kan vara skapade vid en viss tidpunkt och ändrade vid en eller flera andra tidpunkter. Ett tillstånd bör då uttryckas som att det avser filer som skapats eller ändrats efter en viss given tidpunkt. Avläsningen ska då få avse uppgifter i filer som ändrats efter den givna tidpunkten, även om de skapats före. Vid tillståndsgivningen bör rätten dock, t.ex. av integritetsskäl, begränsa de uppgifter som får tas upp även såvitt avser tiden före beslutet, eftersom tiden inte får vara längre än vad som är nödvändigt i det enskilda fallet. När det gäller tillståndstiden är det möjligt att förlänga ett tillstånd till hemlig dataavläsning enligt samma principer som gäller för övriga hemliga tvångsmedel, dvs. att den sökande före tillståndstidens utgång kommer in med en ny ansökan. Även en sådan ansökan om förlängning av tillståndet prövas av rätten enligt samma förfarande som vid den första ansökan.

19 § På förfarandet enligt denna lag i övrigt tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte något annat anges i denna lag. Handläggningen ska ske skyndsamt.

Enligt paragrafen ska reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor tillämpas på förfarandet enligt denna lag, om inte annat anges i lagen. Övervägandena finns i avsnitt 11.1.3

Ärenden om hemlig dataavläsning ska således hanteras på samma sätt i domstol som övriga hemliga tvångsmedelsärenden. Det innebär bl.a. att domstolens beslut om hemlig dataavläsning är ett slutligt beslut som kan överklagas enligt 49 kap. 3 § första stycket RB. Även inskränkande villkor

kan överklagas. Det offentliga ombudet kan också överklaga ett tillståndsbeslut på den grunden att det inte är förenat med tillräckliga villkor i syfte att förhindra onödigt intrång i enskildas integritet. Av 52 kap. 7 § tredje stycket RB framgår att hovrätten kan inhibera verkställigheten vid ett överklagande. Handläggningen av ärenden om hemlig dataavläsning ska ske skyndsamt.

20 § Ett beslut i frågor om hemlig dataavläsning får verkställas omedelbart.

Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, ska den som ansökt om åtgärden eller rätten omedelbart upphäva beslutet.

I paragrafen finns bestämmelser om omedelbar verkställighet och omedelbart upphävande av beslut om tillstånd till hemlig dataavläsning. Övervägandena finns i avsnitt 11.1.6.

Av *första stycket* följer att beslut i frågor om hemlig dataavläsning får verkställas omedelbart. Bestämmelsen har samma innebörd som 30 kap. 12 § RB, som föreskriver omedelbar verkställighet av tvångsmedelsåtgärder i 24–28 kap. RB.

I *andra stycket* anges att om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning ska beslutet om tillstånd omedelbart upphävas. Det är rätten eller den som ansökt om åtgärden som ska upphäva beslutet. Med den som ansökt menas åklagaren eller, i förekommande fall, Säkerhetspolisen eller Polismyndigheten (se kommentaren till 14 §). Åtgärden ska också avbrytas om det efter tillståndsprövningen visar sig att uppgifter i det avläsningsbara informationssystem som tillståndet avser inte får läsas av eller tas upp enligt 11 §, eftersom det då inte längre finns skäl för åtgärden.

21 § När rätten har beslutat i frågor om hemlig dataavläsning ska den underrätta Säkerhets- och integritetsskyddsnämnden om beslutet.

I paragrafen föreskrivs en skyldighet för domstol att underrätta Säkerhets- och integritetsskyddsnämnden vid beslut i fråga om hemlig dataavläsning. Övervägandena finns i avsnitt 12.2.1.

Rätten ska, efter att den beslutat i frågor om hemlig dataavläsning, underrätta Säkerhets- och integritetsskyddsnämnden om beslutet. Underrättelseskyldigheten omfattar alla rättens beslut och gäller således såväl bifall som avslag samt kompletterande beslut. I bestämmelsen anges att underrättelsen ska lämnas när rätten har beslutat. Underrättelse bör äga rum i nära anslutning till beslutstillfället och görs lämpligen samma dag eller följande arbetsdag.

Genomförande av hemlig dataavläsning

Tillåtna tekniska metoder

22 § När ett tillstånd till hemlig dataavläsning har beviljats får de tekniska hjälpmedel som behövs för avläsningen och upptagningen användas. Om det är nödvändigt får systemskydd brytas eller kringgås och tekniska sårbarheter utnyttjas.

I paragrafen finns regler om verkställighet av hemlig dataavläsning. Övervägandena finns i avsnitt 11.2.1.

När ett tillstånd till hemlig dataavläsning har beviljats, får de tekniska hjälpmedel som behövs för avläsningen och upptagningen användas. Bestämmelsen motsvarar vad som gäller vid verkställighet av hemlig avlyssning eller övervakning av elektronisk kommunikation enligt 27 kap. 25 § RB. Med tekniska hjälpmedel avses både hårdvara och mjukvara (se prop. 1994/95:227 s. 29). Den verkställande myndigheten får själv bestämma vilken teknik som ska användas i det enskilda fallet. Verkställighetstekniken omfattas inte formellt av domstolens prövning, även om rätten kan ställa villkor om hur verkställigheten ska utföras för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan (18 § första stycket 4). Hemlig dataavläsning kan genomföras på flera olika sätt. Om det är nödvändigt får systemskydd brytas eller kringgås och tekniska sårbarheter utnyttjas. Det kan exempelvis vara fråga om inloggning på en tjänst genom användande av inloggningsuppgifter som blivit kända för den brottsbekämpande myndigheten eller om mer tekniskt avancerade åtgärder. Verkställighet kan bland annat ske genom installation av programvara i eller installation av ett fysiskt föremål på ett avläsningsbart informationssystem. Den verkställande myndigheten får också använda tekniska hjälpmedel som redan finns i det avläsningsbara informationssystem som tillståndet avser. Det kan behövas för att kunna verkställa beslut om hemlig dataavläsning som avser upptagning av plats-, kameraövervaknings- eller rumsavlyssningsuppgifter. I sådana fall kan det vara nödvändigt att aktivera t.ex. GPS-, kamera- eller mikrofonfunktion i det avläsningsbara informationssystemet. Bestämmelsen medger såväl aktivering av programvara som finns i informationssystemet som installation av annan programvara, t.ex. den som ska användas för verkställigheten.

Paragrafen utesluter inte att flera olika tekniker eller metoder används vid samma verkställighet. Det ska dock noteras att det aktsamhetskrav som anges i 25 § kan begränsa vilka tekniska hjälpmedel som får användas.

Skyldighet att medverka

23 § Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation är på begäran av den verkställande myndigheten skyldig att medverka i samband med verkställighet av hemlig dataavläsning.

Den som medverkar enligt första stycket har rätt till ersättning för kostnader som uppstår vid sådan medverkan. Ersättningen ska betalas av den verkställande myndigheten.

I bestämmelsen regleras medverkansskyldighet för vissa privaträttsliga aktörer. Övervägandena finns i avsnitt 12.2.2.

I *första stycket* slås fast att det på begäran av den verkställande myndigheten finns en skyldighet för den som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation att medverka i samband med verkställighet av hemlig dataavläsning. Det innebär att det är aktörer som tillhandahåller allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster som träffas av regeln, t.ex. operatörer av mobiltelefoni och internet.

Det är inte reglerat närmare vad medverkan ska avse. Vilka specifika uppgifter en operatör ska bistå den verkställande myndigheten med beror

på hur den verkställande myndigheten formulerar sin begäran. Det kan t.ex. röra sig om att en operatör identifierar vilka tjänster en specifik användare har och vilka förbindelser den använder, ger råd avseende vilka tekniska hjälpmedel som kan användas, tillhandahåller möjlighet att installera tekniska hjälpmedel i operatörens nät för verkställighet eller bistår med andra liknande stödåtgärder.

Av *andra stycket* framgår att den som medverkar i samband med verkställighet har rätt till ersättning från den verkställande myndigheten för de kostnader som uppstår vid sådan medverkan. De kostnader som avses är främst nedlagd tid hos den medverkande. Kostnader kan också uppstå för att t.ex. upplåta utrymme, dvs. kostnader som inte är hänförliga till tidsåtgång utan till själva upplåtandet. Det är direkta kostnader, som nedlagd tid och upplåtande av utrymme, som kan ersättas enligt bestämmelsen. Även kostnader som kan ha uppstått vid medverkan som inte leder till en genomförd verkställighet omfattas av bestämmelsen. Däremot ersätts inte kostnader som uppstår hos operatören för att generellt anpassa sina system för att möjliggöra medverkan. Kostnadsfördelningen överensstämmer således med den modell som förekommer inom datalagringen, se propositionen Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG (prop. 2010/11:46 s. 65–68).

Teknikanpassning och otillåten tilläggsinformation

24 § Den teknik som används i samband med hemlig dataavläsning ska anpassas efter det tillstånd som beviljats. Tekniken får inte göra det möjligt att läsa av eller ta upp någon annan typ av uppgift än vad som anges i tillståndet. Om sådana uppgifter har lästs av eller tagits upp ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas.

Uppgifter som anges i första stycket får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

I paragrafen finns bestämmelser om anpassning av verkställighetstekniken och vad som gäller om anpassningen varit otillräcklig. Övervägandena finns i avsnitt 11.2.2.

I *första stycket* anges att den teknik som används i samband med hemlig dataavläsning ska anpassas efter det tillstånd som beviljats. Det är den verkställande myndigheten som ansvarar för det. I bestämmelsen regleras inte hur anpassningen ska gå till. Det blir en fråga för den verkställande myndigheten att se till att de anpassningar som gjorts är tillräckliga. Brister i det avseendet kan även påtalas av tillsynsmyndigheten i efterhand.

Tekniken som används i samband med verkställighet får inte möjliggöra avläsning eller upptagning av någon annan typ av uppgift än sådan som tillståndet tillåter. Det innebär att om tillståndet exempelvis tillåter hemlig dataavläsning för att läsa av eller ta upp kommunikationsavlyssningsuppgifter ska det inte vara möjligt att med den teknik som används läsa av eller ta upp kameraövervakningsuppgifter. Om ett tekniskt hjälpmedel är konstruerat på så sätt att det i och för sig är möjligt att använda det för att läsa av eller ta upp olika uppgiftstyper krävs att hjälpmedlet är inställt på ett sådant sätt att det inte är möjligt att utan ändringar av inställningarna i hjälpmedlet komma åt andra uppgiftstyper än de som tillståndet avser.

Om den verkställande myndigheten, trots skyldigheten att anpassa tekniken efter tillståndet, har läst av eller tagit upp en annan typ av uppgift än tillståndet medger är det fråga om s.k. otillåten tilläggsinformation. Om otillåten tilläggsinformation har lästs av eller tagits upp ska upptagningar och uppteckningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. Hur nämnden ska förfara när den mottagit sådan information regleras inte i lagen. Det står nämnden fritt att rikta sin tillsyn mot det aktuella fallet eller vidta de andra åtgärder den finner nödvändiga.

Av *andra stycket* framgår att uppgifter som kommit fram vid sådan avläsning eller upptagning som avses i första stycket, dvs. otillåten tilläggsinformation, inte får användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser. Det innebär t.ex. att det inte får beslutas husrannsakan eller inledas utredning om nya brott på grundval av uppgifter som utgör otillåten tilläggsinformation. Bestämmelsen motsvarar vad som gäller enligt 17 § tredje stycket när hemlig dataavläsning har verkställts efter ett interimistiskt tillstånd från åklagare som rätten sedan anser inte borde ha beviljats. Det som anges i kommentaren till 17 § tredje stycket gäller på motsvarande sätt för otillåten tilläggsinformation.

Aktsamhetskrav

25 § När ett beslut om hemlig dataavläsning verkställs får någon olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser får dock inte åsidosättas, minskas eller skadas till följd av verkställigheten.

När verkställigheten avslutas ska den verkställande myndigheten vidta de åtgärder som behövs för att informationssäkerheten i det avläsningsbara informationssystem som tillståndet avser ska hålla åtminstone samma nivå som vid verkställighetens början.

Ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet har gått ut eller tillståndet upphävts.

I paragrafen föreskrivs aktsamhetsregler som tar sikte på bl.a. informationssäkerhet. Övervägandena redovisas i avsnitt 11.2.3.

I *första stycket* anges att vid genomförande av hemlig dataavläsning får olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Bestämmelsen är en generellt utformad aktsamhetsregel som alltid gäller vid verkställighet av hemlig dataavläsning. Den motsvarar vad som föreskrivs vid hemlig rumsavlyssning i 27 kap. 25 a § femte stycket RB och vid husrannsakan i 28 kap. 6 § första stycket RB. Bestämmelsen får betydelse t.ex. i fråga om tillträde till den plats där hemlig dataavläsning ska genomföras och på vilket sätt utrustningen ska installeras (jfr prop. 2005/06:178 s. 107). Bestämmelsen är tillämplig i såväl det fysiska rummet som i de virtuella eller digitala rum där hemlig dataavläsning verkställs. Den gäller såväl i förhållande till den som ska bli föremål för hemlig dataavläsning som i förhållande till andra som kan drabbas av åtgärden. Bestämmelsen förbjuder inte att skada eller olägenhet uppstår, men föreskriver att den i så fall måste vara absolut nödvändig. Detta innebär att det vid verkställigheten behöver övervägas om det finns några

alternativ till den åtgärd som planeras om åtgärden kommer att innebära skada eller olägenhet för en person, t.ex. åverkan på dennes dator eller mobiltelefon vid installation av hårdvara.

I *första stycket andra meningen* anges att informationssäkerheten i andra avläsningsbara informationssystem än det tillståndet avser inte får åsidosättas, minskas eller skadas till följd av verkställigheten. Det är en mer specifikt inriktad aktsamhetsregel än den i första meningen och tar sikte på informationssäkerheten i andra informationssystem än det som tillståndet avser. När ett tillstånd till hemlig dataavläsning avser en viss elektronisk kommunikationsutrustning är exempel på andra informationssystem än det som omfattas av tillståndet det nät som utrustningen är ansluten till eller informationssystem som är sammankopplade med det som tillståndet gäller, t.ex. angränsande datorer i ett och samma nätverk. Om tillstånd till hemlig dataavläsning däremot avser användarkonton eller på motsvarande sätt avgränsade delar av kommunikationstjänster, lagringstjänster eller liknande tjänster är allt vid sidan av den definitionen att se som utanför informationssystemet. Det innebär exempelvis att allt innehåll på den tjänst som användarkontot tillhör men som inte kan tillgängliggöras genom användarkontot, t.ex. andras användarkonton och den fysiska infrastrukturen för tjänsten, omfattas av aktsamhetskravet.

I *andra stycket* föreskrivs att när verkställigheten avslutas ska den verkställande myndigheten vidta de åtgärder som behövs för att informationssäkerheten i det avläsningsbara informationssystem som tillståndet avser ska hålla åtminstone samma nivå som vid verkställighetens början. Bestämmelsen tar sikte på informationssäkerheten i det avläsningsbara informationssystem som tillståndet avser. Redan av den generella aktsamhetsregeln i första stycket följer att skada eller olägenhet inte ska orsakas informationssystemet om det inte är absolut nödvändigt. Vid verkställighet av hemlig dataavläsning kan det förekomma att informationssäkerheten i det informationssystem tillståndet avser minskas, bl.a. eftersom det är tillåtet att bryta eller kringgå systemskydd och utnyttja tekniska sårbarheter (22 §). Eventuella skador av detta utesluts alltså inte, men måste vara absolut nödvändiga i enlighet med första stycket. När verkställighet av hemlig dataavläsning avslutas ska dock inte informationssystemet lämnas i sämre, dvs. mindre säkert, skick än när verkställigheten påbörjades. Detta uttrycks genom att den verkställande myndigheten åläggs en skyldighet att se till att informationssäkerheten i informationssystemet ska hålla åtminstone samma nivå som vid verkställighetens början. Den brottsbekämpande myndigheten är alltså oförhindrad att öka säkerheten i systemet.

Av *tredje stycket* framgår att ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter det att tiden för tillståndet gått ut eller tillståndet hävts. Det är således inte möjligt för den verkställande myndigheten att efter det att tillståndstiden har löpt ut kunna utnyttja samma verktyg igen vid ett senare tillfälle utan att installera eller aptera utrustningen på nytt efter ett nytt tillstånd.

26 § Den verkställande myndigheten ska utse en eller flera personer som får verkställa hemlig dataavläsning. Sådana personer ska vara särskilt lämpade för uppdraget och ha särskilda kunskaper om informationssäkerhet samt den särskilda kompetens, utbildning och erfarenhet som i övrigt är nödvändig.

I paragrafen anges att den verkställande myndigheten ska utse personer som får verkställa hemlig dataavläsning och vilka krav som ska ställas på sådana personer. Övervägandena finns i avsnitt 12.2.4.

Av *första meningen* framgår att det är den verkställande myndigheten som utser personer som får ansvara för den praktiska verkställigheten av hemlig dataavläsning. De myndigheter som kan komma i fråga för sådan verkställighet är Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket. Myndighetschefen eller den som myndighetschefen utser får utse dem som verkställer hemlig dataavläsning.

Den som utses ska vara särskilt lämpad för uppdraget. Han eller hon ska också ha de särskilda kunskaper om informationssäkerhet samt den särskilda kompetens, utbildning och erfarenhet som i övrigt är nödvändig. Den verkställande myndigheten ansvarar för att tillse att den ansvarige personen uppfyller dessa krav.

Förbud att läsa av eller ta upp vissa uppgifter

27 § Hemlig dataavläsning enligt 2 § första stycket 6 eller 7 får inte avse uppgifter som enligt 27 kap. 2 § första stycket rättegångsbalken hindrar beslag.

Hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram.

Om det under verkställigheten kommer fram uppgifter som omfattas av första eller andra styckena ska verkställigheten omedelbart avbrytas och upptagningar och uppteckningar omedelbart förstöras i de delar som de omfattas av förbudet.

I paragrafen regleras förbud att i vissa fall läsa av eller ta upp vissa uppgifter. Övervägandena finns i avsnitt 10.3.3 och 10.3.4.

Av *första stycket* framgår att hemlig dataavläsning avseende lagrade uppgifter eller uppgifter som visar hur ett informationssystem används inte får avse uppgifter som enligt 27 kap. 2 § första stycket RB hindrar beslag. Bestämmelsen knyter således an till det s.k. beslagsförbudet i rättegångsbalken som innebär ett förbud mot att ta vissa skriftliga handlingar i beslag. Dess utformning innebär att uppgifter som är en del av en fil eller annan informationsenhet som inte skulle ha fått tas i beslag inte heller får läsas av eller tas upp genom hemlig dataavläsning (se NJA 2015 s. 631 p. 25 och 26). De uppgifter det kan vara fråga om är sådana som en befattningshavare eller någon annan som avses i 36 kap. 5 § RB inte får höras som vittne om och som innehas av honom eller henne eller av den som tystnadsplikten gäller till förmån för. Det kan t.ex. vara en advokat, läkare eller tandläkare. Det innebär motsatsvis att i den mån tystnadsplikt enligt 36 kap. 5 § RB inte gäller för uppgiften, t.ex. i vissa fall när det är fråga om grövre brott eller vid medgivande enligt det lagrummet, finns det normalt inte hinder mot beslag. I de fallen finns det inte heller något förbud mot att läsa av eller ta upp uppgifterna.

Av *andra stycket* framgår att hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter inte får avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte

styckena RB, inte skulle ha kunnat höras som vittne om det som har sagts eller som på annat sätt kommit fram. I sak har förbudet samma innebörd som avlyssningsförbudet i 27 kap. 22 § RB och, såvitt avser hemlig avlyssning av elektronisk kommunikation, i 11 § preventivlagen. Det kan t.ex. vara fråga om samtal där uppgifter från en advokat, läkare eller tandläkare förekommer.

Av *tredje stycket* framgår att om det under verkställigheten kommer fram uppgifter som omfattas av första eller andra styckena ska verkställigheten omedelbart avbrytas och upptagningar och uppteckningar omedelbart förstöras i de delar som de omfattas av förbudet.

Överskottsinformation, granskning och underrättelse till enskilda

Förundersökning

28 § När hemlig dataavläsning används eller har använts under en förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 23 a och 24 §§ rättegångsbalken tillämpas för åtgärden. Det som gäller för hemlig rumsavlyssning ska dock tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

För underrättelse till en enskild vid hemlig dataavläsning under förundersökning gäller 27 kap. 31–33 §§ rättegångsbalken. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning som gäller rumsavlyssningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

I paragrafen anges vad som gäller bl.a. beträffande hur överskottsinformation får användas vid hemlig dataavläsning under en förundersökning. Övervägandena finns i avsnitt 12.1.2–12.1.4.

Genom *första stycket* blir de regler som gäller för hemlig avlyssning av elektronisk kommunikation under en förundersökning i frågor som rör användning av överskottsinformation, granskning och bevarande tillämpliga även för hemlig dataavläsning genom hänvisningar till rättegångsbalkens regler (27 kap. 23 a § och 27 kap. 24 § RB). För hemlig dataavläsning som gäller rumsavlyssningsuppgifter gäller dock i stället reglerna i rättegångsbalken om användning av överskottsinformation och behandling av uppgifter vid hemlig rumsavlyssning.

I *andra stycket* finns bestämmelser om underrättelse till enskild. Genom en hänvisning blir rättegångsbalkens regler om vad som gäller vid användning av hemliga tvångsmedel under en förundersökning tillämpliga (27 kap. 31–33 §§). När kameraövervakningsuppgifter eller rumsavlyssningsuppgifter har lästs av eller tagits upp med hemlig dataavläsning ska det som gäller för hemlig kameraövervakning respektive hemlig rumsavlyssning i nämnda bestämmelser tillämpas för underrättelsen. Det innebär bl.a. att innehavaren av den plats som tillståndet avsett typiskt sett ska underrättas. Det som anges om hemlig avlyssning av elektronisk kommunikation ska tillämpas vid hemlig dataavläsning i övrigt, dvs. samtliga uppgiftstyper utom kameraövervaknings- och rumsavlyssningsuppgifter.

Vid tillämpning av bestämmelserna om underrättelse till enskild ska en annan nomenklatur användas än den som anges i rättegångsbalken. När en enskild ska underrättas om hemlig dataavläsning ska nämligen underrättelsen riktas till användaren av det avläsningsbara informationssystemet i stället för till innehavaren av ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning.

Förhindrande av vissa särskilt allvarliga brott

29 § När hemlig dataavläsning används eller har använts i fall som anges i 7 § ska 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas.

För underrättelse till en enskild vid hemlig dataavläsning i fall som anges i 7 § gäller 16–18 §§ lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som anges där om

– hemlig kameraövervakning ska tillämpas för hemlig dataavläsning som gäller kameraövervakningsuppgifter

– hemlig avlyssning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning i övrigt

– telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska avse avläsningsbart informationssystem.

I paragrafen anges vad som ska gälla bl.a. beträffande hur överskottsinformation får användas vid hemlig dataavläsning i preventivlagsfallen. Övervägandena finns i avsnitt 12.1.2–12.1.4.

Genom *första stycket* blir de regler som gäller enligt preventivlagen i frågor som rör användning av överskottsinformation, granskning och bevarande genom hänvisningar tillämpliga även för hemlig dataavläsning i preventivlagsfallen.

I *andra stycket* finns regler om underrättelse till enskild vid hemlig dataavläsning i preventivlagsfallen. Genom en hänvisning blir samma regler som används vid annan tvångsmedelsanvändning enligt preventivlagen tillämpliga även vid hemlig dataavläsning (16–18 §§). När kameraövervakningsuppgifter har lästs av eller tagits upp med hemlig dataavläsning ska det som gäller för hemlig kameraövervakning i nämnda bestämmelser gälla såvitt avser underrättelse till enskild. Det innebär bl.a. att innehavaren av den plats som tillståndet i den delen avsett typiskt sett ska underrättas. Det som anges om hemlig avlyssning av elektronisk kommunikation ska för övriga uppgiftstyper, dvs. alla uppgiftstyper utom kameraövervakningsuppgifter, tillämpas vid hemlig dataavläsning i preventivlagsfallen. Underrättelseskyldigheten enligt preventivlagen är emellertid begränsad genom att det endast är när åtgärd vidtas för att förhindra vissa allvarliga brott mot person i systemhotande syfte som underrättelse ska lämnas (1 § 7 och 16 § preventivlagen). Detsamma ska gälla vid hemlig dataavläsning i dessa fall. I bestämmelsen förtydligas, på samma sätt som i 28 §, att det vid tillämpning av paragrafen ska användas en annan nomenklatur än den som anges i rättegångsbalken. När en enskild ska underrättas om hemlig dataavläsning ska nämligen underrättelsen riktas till användaren av det avläsningsbara informationssystemet i stället för till innehavararen av ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning.

Särskild utlänningskontroll

30 § När hemlig dataavläsning används eller har använts i fall som anges i 9 § ska 21 a § och 22 § första och andra styckena lagen (1991:572) om särskild utlänningskontroll tillämpas. Det som anges där om hemlig avlyssning och övervakning av elektronisk kommunikation ska tillämpas för hemlig dataavläsning.

I paragrafen anges vad som ska gälla bl.a. beträffande hur överskottsinformation får användas vid hemlig dataavläsning i LSU-fallen. Övervägandena finns i avsnitt 12.1.2–12.1.3.

Genom paragrafen blir de regler som gäller enligt lagen (1991:572) om särskild utlänningskontroll i frågor som rör användning av överskottsinformation, granskning och bevarande tillämpliga även för hemlig dataavläsning i LSU-fallen.

Det finns inte några regler om underrättelseskyldighet i lagen om särskild utlänningskontroll. Därför finns inte heller någon bestämmelse som reglerar underrättelse till enskild vid hemlig dataavläsning i LSU-fallen.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

31 § När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska 6–8 §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet tillämpas. Det som anges där om inhämtning av uppgifter ska tillämpas för hemlig dataavläsning.

I paragrafen anges vad som ska gälla för bl.a. överskottsinformation när hemlig dataavläsning används i inhämtningslagsfallen. Övervägandena finns i avsnitt 12.1.2–12.1.3.

Genom paragrafen blir de regler som gäller enligt inhämtningslagen i frågor som rör användning av överskottsinformation, granskning och bevarande tillämpliga även för hemlig dataavläsning i inhämtningslagsfallen.

Det finns inte några regler om underrättelseskyldighet enligt inhämtningslagen. Därför finns inte heller någon bestämmelse som reglerar underrättelse till enskild vid hemlig dataavläsning i inhämtningslagsfallen.

Tystnadsplikt

32 § Den som i samband med verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation har fått del av eller tillgång till en uppgift som hänför sig till användning av hemlig dataavläsning, får inte obehörigen föra vidare eller utnyttja det han eller hon fått del av eller tillgång till.

I paragrafen föreskrivs tystnadsplikt för personer som i viss verksamhet fått del av uppgifter om hemlig dataavläsning. Övervägandena finns i avsnitt 12.2.3.

I paragrafen anges att den som i samband med verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation har fått del av eller tillgång till en uppgift som hänför sig till användning av hemlig dataavläsning, inte obehörigen får föra vidare eller utnyttja det han eller hon fått del av eller tillgång till. Bestämmelsen innebär att vem som helst kan omfattas av tystnadsplikten, så länge han

eller hon har fått del av eller tillgång till uppgifterna i samband med sådan tillståndspliktig verksamhet som avses i bestämmelsen. Den tillståndspliktiga verksamhet som avses är t.ex. mobiloperatörers och nätägares tillhandahållande av allmänna kommunikationsnät. Typiskt sett avses personer som är eller har varit verksamma i sådan verksamhet, antingen genom anställning eller genom uppdrag av eller hos företaget. För att omfattas av tystnadsplikt enligt bestämmelsen ska en sådan person ha fått del av eller tillgång till uppgift som hänför sig till angelägenhet som avser användning av hemlig dataavläsning. Uppgifterna som kan bli föremål för tystnadsplikten kan vara hänförliga till bl.a. tekniken som används vid verkställighet, personen som ska bli föremål för åtgärden, informationssystemet som innehåller uppgifterna som ska läsas av eller den brottsbekämpande myndigheten som ansvarar för verkställighet. Bestämmelsen omfattar varje uppgift som direkt eller indirekt gäller användning av hemlig dataavläsning.

Innebörden av tystnadsplikten är att den som tystnadsplikten gäller för inte obehörigen får föra vidare eller utnyttja det som han eller hon har fått del av eller tillgång till. Han eller hon får varken genom tal eller i skrift föra uppgifterna vidare eller exempelvis utnyttja uppgifter om verkställighetstekniken som han eller hon fått kännedom om.

I 44 kap. 5 § 5 OSL införs en bestämmelse som innebär att den grundlagsstadgade rätten att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som föreskrivs i förevarande bestämmelse, se kommentaren till den bestämmelsen.

I 20 kap. brottsbalken finns straffbestämmelser för den som bryter mot tystnadsplikten.

Rätt att meddela föreskrifter

33 § Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om

1. medverkan och ersättning enligt 23 §, och
2. underrättelser enligt 24 §.

I paragrafen upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela verkställighetsföreskrifter om medverkan och ersättning vid verkställighet av hemlig dataavläsning och om de underrättelser som i vissa fall ska skickas till Säkerhets- och integritetsskyddsnämnden. Övervägandena finns i avsnitt 12.2.6.

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

28 § Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § rättegångsbalken *eller hemlig dataavläsning enligt 2 § första*

stycket 5 lagen (2019:000) om hemlig dataavläsning, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.

Om åklagaren har gett ett sådant tillstånd, ska han eller hon utan dröjsmål skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

I paragrafen regleras åklagarens interimistiska beslutanderätt. Övervägandena finns i avsnitt 12.2.5.

I *första stycket* görs ett tillägg som innebär att åklagaren får bevilja ett interimistiskt beslut om hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter enligt 2 § första stycket 5 lagen om hemlig dataavläsning om förutsättningarna i övrigt är uppfyllda.

16.3 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 Polismyndigheten 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 Polismyndigheten 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.

I lagen (2019:000) om hemlig dataavläsning finns bestämmelser om att rätten kan meddela Säkerhetspolisen eller Polismyndigheten tillstånd enligt den lagen.

I paragrafen finns bestämmelser om tillstånd till hemlig dataavläsning vid särskild utlänningskontroll. Övervägandena finns i avsnitt 10.2.4.

I *fjärde stycket* införs en upplysningsbestämmelse om att rätten enligt lagen om hemlig dataavläsning kan meddela Säkerhetspolisen eller Polismyndigheten tillstånd enligt den lagen (se 9 och 14 §§ lagen om hemlig dataavläsning). I övrigt är paragrafen oförändrad.

16.4 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. *hemlig kameraövervakning,*
8. *hemlig rumsavlyssning,*
9. *hemlig dataavläsning,*
10. *tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning,*
11. *tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning,*
12. *överförande av frihetsberövade för förhör m.m., och*
13. *rättsmedicinsk undersökning av en avliden person.*

Lagen hindrar inte att hjälp lämnas med *någon* 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, som i *första stycket* innehåller en uttömmande uppräkning av de åtgärder som omfattas av rättslig hjälp enligt lagen, kompletteras med hemlig dataavläsning, tekniskt bistånd med hemlig dataavläsning och tillstånd till gränsöverskridande hemlig dataavläsning. Tekniskt bistånd och tillstånd till gränsöverskridande hemlig dataavläsning avser enbart hemlig dataavläsning för kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter. Övriga ändringar är endast redaktionella. Övervägandena finns i avsnitt 13.2.1 och 13.2.2.

2 kap.

1 § Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–9 och 13* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.

Rättslig hjälp som avses i 1 kap. 2 § första stycket *10–12* lämnas enligt de särskilda bestämmelserna i denna lag.

I 5 kap. 2 § finns bestämmelser om att den rättsliga hjälpen får förenas med villkor i vissa fall.

I paragrafen regleras vilka förutsättningar som ska gälla för tillämpning av åtgärderna i 1 kap. 2 §. Övervägandena finns i avsnitt 13.2.1.

En hänvisning till rättslig hjälp i form av hemlig dataavläsning införs i *första stycket*. Det innebär att rättslig hjälp med hemlig dataavläsning ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning. Således ska både förutsättningarna enligt lagen om hemlig dataavläsning och förevarande lag vara uppfyllda för att åtgärden ska tillåtas.

Vissa åtgärder som avses i 1 kap. 2 § första stycket saknar motsvarigheter i nationella förfaranden, bl.a. tekniskt bistånd med och tillstånd till gränsöverskridande hemlig dataavläsning. Förutsättningarna för att bistå med dessa åtgärder framgår av paragrafens *andra stycke*. I detta stycke görs ett tillägg beträffande tekniskt bistånd med och tillstånd till gränsöverskridande hemlig dataavläsning (1 kap. 2 § första stycket 10 och 11). Särskilda bestämmelser beträffande förutsättningarna att lämna tekniskt bistånd med respektive tillstånd till gränsöverskridande hemlig dataavläsning finns i 4 kap. 28 e–h §§.

Övriga ändringar är endast redaktionella.

2 § Rättslig hjälp som avses i 1 kap. 2 § första stycket *1–4, 10 och 12* får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket *5–9, 11* och *13* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan och beslag.

I paragrafen regleras när dubbel straffbarhet uppställs som krav för att rättslig hjälp ska få lämnas. Övervägandena finns i avsnitt 13.2.1.

Ändringen innebär att rättslig hjälp med hemlig dataavläsning får lämnas endast om den gärning som ansökan avser motsvarar ett brott enligt både svensk lag och lagen i den stat där åtgärden behövs. Kravet på dubbel straffbarhet uppställs även i fråga om tillstånd till gränsöverskridande hemlig dataavläsning (1 kap. 2 § första stycket 11) men inte beträffande tekniskt bistånd med hemlig dataavläsning (1 kap. 2 § första stycket 10).

Övriga ändringar är endast redaktionella.

4 § En ansökan om rättslig hjälp i Sverige enligt denna lag bör innehålla
– uppgift om den utländska domstol eller myndighet som handlägger ärendet,
– en beskrivning av det rättsliga förfarande som pågår,
– uppgift om den aktuella gärningen, tid och plats för *den*,
samt *uppgift om* de bestämmelser som är tillämpliga i den ansökande staten,
– uppgift om vilken åtgärd som begärs och, i förekommande fall, i vilken egenskap en person ska höras,
– namn på och adress till de personer som är aktuella i ärendet.

I 4 kap. 8, 11, 14, 24 a, 25, 25 b, 25 c, 26 a, *28 c*, 29 och 29 a §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.

Om ärendet är brådskande eller om *verkställigheten* önskas inom *en* viss tidsfrist, ska detta anges och motiveras.

En ansökan om rättslig hjälp ska göras skriftligen genom post, bud eller telefax. Den får även, efter överenskommelse i det enskilda fallet, översändas på annat sätt.

Paragrafen innehåller regler om bl.a. vad en ansökan om rättslig hjälp i Sverige bör innehålla. Övervägandena finns i avsnitt 13.2.2.

I *andra stycket* görs ett tillägg i den uppräkning av paragrafer som innehåller särskilda bestämmelser om vad en ansökan ska innehålla. Tillägget avser den paragraf som reglerar vad en ansökan om rättslig hjälp i Sverige med hemlig dataavläsning ska innehålla (4 kap. 28 c §).

Övriga ändringar är endast språkliga.

4 kap.

Hemlig dataavläsning i Sverige

Rättslig hjälp i Sverige med hemlig dataavläsning

28 c § *En ansökan om hemlig dataavläsning 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 det får ske enligt 17 § lagen (2019:000) om hemlig dataavläsning, själv besluta om åtgärden.*

Upptagningar och uppteckningar behöver inte granskas enligt 28 § första stycket lagen om hemlig dataavläsning.

Om åklagaren har fattat beslut enligt första stycket, ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om hemlig dataavläsning. Upptagningar och uppteckningar får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning skett enligt 2 kap. 17 § endast om det är tillåtet enligt 28 § första stycket lagen om hemlig dataavläsning.

I fråga om underrättelse till en enskild enligt 28 § andra stycket lagen om hemlig dataavläsning ska bestämmelserna i 25 § tredje stycket detta kapitel tillämpas.

I paragrafen, som är ny, finns bestämmelser om rättslig hjälp med hemlig dataavläsning i Sverige. Övervägandena finns i avsnitt 13.2.2.

Paragrafen motsvarar i allt väsentligt vad som gäller för rättslig hjälp med andra hemliga tvångsmedel enligt lagen. Enligt *första stycket* första meningen ska en ansökan handläggas av åklagare. Detta motsvarar vad som gäller för övriga hemliga tvångsmedel enligt lagen. I andra meningen framgår de krav som ställs på en ansökan. Motsvarande krav gäller vid ansökan om rättslig hjälp i Sverige med hemlig avlyssning eller övervakning av elektronisk kommunikation enligt 25 §. Med sådana uppgifter som behövs för att åtgärden ska kunna genomföras avses de uppgifter som enligt lagen om hemlig dataavläsning krävs för att domstol ska kunna pröva om åtgärden ska tillåtas, t.ex. uppgifter om vilket brott som avses, vem som ska bli föremål för åtgärden, omständigheter som gör att åtgärden är av synnerlig vikt för utredningen och vilket informationssystem som tillståndet avser. Det kan också vara lämpligt att det uttryckligen framgår att det är fråga om en ansökan om hemlig dataavläsning avseende en viss typ av uppgift, t.ex. kommunikationsavlyssningsuppgifter, eftersom vissa åtgärder som enligt svensk rätt utgör hemlig dataavläsning i andra länder anses vara en metod för att verkställa ett hemligt tvångsmedel, t.ex. hemlig avlyssning av elektronisk kommunikation. Tredje meningen reglerar åklagarens handläggning och möjligheten att fatta interimistiska beslut. Bestämmelsen motsvarar vad som gäller enligt bestämmelserna om rättslig hjälp i Sverige med övriga hemliga tvångsmedel förutom hemlig rumsavlyssning. Genom hänvisningen till 17 § lagen om hemlig dataavläsning klargörs att åklagarens interimistiska beslutanderätt bestäms genom den bestämmelsen.

I *andra stycket* anges att granskning inte behöver ske av upptagningar och uppteckningar. Motsvarande gäller för övriga hemliga tvångsmedel. Den hänvisning som i dessa fall görs till 27 kap. 24 § RB ersätts med en hänvisning till 28 § lagen om hemlig dataavläsning.

I *tredje stycket* första meningen anges att ett interimistiskt åklagarbeslut ska underställas domstolens prövning innan upptagna eller uppteckнade uppgifter från en hemlig dataavläsning får lämnas över till den andra staten. Kravet överensstämmer med det som gäller för övriga hemliga tvångsmedel enligt lagen när det föreligger en möjlighet för åklagaren att fatta interimistiskt beslut. I andra meningen upplyses om att sådana upptagningar eller uppteckningar som finns kvar i Sverige efter att ärendet återredovisats till den andra staten endast får bevaras i Sverige om det är tillåtet enligt 28 § första stycket lagen om hemlig dataavläsning. Samma sak gäller för övriga hemliga tvångsmedel.

I *fjärde stycket* regleras vad som gäller avseende underrättelse till enskild vid rättslig hjälp i Sverige med hemlig dataavläsning. Där framgår att samma sak som gäller vid underrättelse till enskild vid hemlig avlyssning eller övervakning av elektronisk kommunikation enligt 25 § tredje stycket ska tillämpas. I den angivna bestämmelsen anpassas de bestämmelser om underrättelse i 27 kap. 31–33 §§ RB, till vilka den angivna regeln hänvisar, till de förhållanden som gäller i det internationella rättsliga samarbetet. Det innebär bl.a. att tidpunkten för underrättelse inte utgår ifrån den tidpunkt då förundersökningen avslutades. I stället knyts underrättelseskyldigheten till den tidpunkt då åtgärden avslutades. Bestämmelserna blir tillämpliga vid hemlig dataavläsning genom en hänvisning till 28 § andra stycket lagen om hemlig dataavläsning. Det innebär bl.a. att när en enskild ska underrättas om hemlig dataavläsning ska underrättelsen ta sikte på användaren av det avläsningsbara informationssystemet i stället för ett telefonnummer, en annan adress eller en viss elektronisk kommunikationsutrustning.

28 d § *Om en ansökan avser hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning får rättens beslut enligt 28 c § att tillåta hemlig dataavläsning verkställas med tillämpning av 25 a §.*

I paragrafen, som är ny, regleras att hemlig dataavläsning, när åtgärden avser avläsning eller upptagning av kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter- får ske genom omedelbar överföring av bl.a. meddelanden. Övervägandena finns i avsnitt 13.2.2.

Hänvisningarna i bestämmelsen innebär att den får samma innebörd som motsvarande bestämmelse om hemlig avlyssning och övervakning av elektronisk kommunikation i 25 a §.

Tekniskt bistånd i Sverige med hemlig dataavläsning

28 e § *Tekniskt bistånd med hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning i form av omedelbar överföring av meddelanden eller uppgifter om meddelanden får lämnas i Sverige enligt de förutsättningar som gäller enligt 25 b § andra, tredje och femte styckena. Vid hemlig dataavläsning i en annan stat än den som ansökt om tekniskt bistånd ska ett tillstånd enligt 28 f § ha lämnats.*

Ansökan ska prövas av åklagare. För beslutet om tekniskt bistånd tillämpas 1 §, 18 § första stycket 1–3 och tredje stycket och 20 § andra stycket lagen om hemlig dataavläsning.

I paragrafen, som är ny, regleras frågan om tekniskt bistånd genom omedelbar överföring av meddelanden eller uppgifter om meddelanden när hemlig dataavläsning avser avläsning eller upptagning av kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter. Övervägandena finns i avsnitt 13.2.2.

I *första stycket* regleras frågan om tekniskt bistånd med omedelbar överföring av meddelanden eller uppgifter om meddelanden. Genom hänvisning till vissa delar av 25 b § blir det som gäller enligt den paragrafens andra, tredje och femte stycken tillämpligt även för hemlig dataavläsning. Det innebär bl.a. att reglerna om vilka förutsättningar som gäller för tekniskt bistånd med hemlig avlyssning och hemlig övervakning av elektronisk kommunikation blir tillämpliga även på tekniskt bistånd med hemlig dataavläsning avseende kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter. Tillämpningsområdet för bestämmelsen är begränsat till ansökningar från medlemsstater i EU eller från Island eller Norge. Av andra meningen följer att vid hemlig dataavläsning i en annan stat än den som ansökt om tekniskt bistånd krävs tillstånd enligt 28 f §, se kommentaren till den bestämmelsen.

Enligt *andra stycket* prövas en ansökan av åklagare. Vid prövningen tillämpas det som föreskrivs i 1 §, 18 § första stycket 1–3 och tredje stycket och 20 § andra stycket lagen om hemlig dataavläsning. Det innebär bl.a. att tiden för ett tillstånd inte får bestämmas längre än nödvändigt och högst en månad från tidpunkten för beslutet samt att ett tillstånd omedelbart ska upphävas om det inte längre finns skäl för beslutet. Bestämmelserna motsvarar det som anges om tekniskt bistånd för hemlig avlyssning och övervakning av elektronisk kommunikation i 25 b § fjärde stycket.

Tillstånd från Sverige till gränsöverskridande hemlig dataavläsning

28 f § *Om ansökan avser tillstånd till gränsöverskridande hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning tillämpas det som gäller för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation enligt 26 a § första och andra styckena och 26 b §. De förutsättningar som gäller enligt 1–6, 11, 14 och 18 §§ lagen om hemlig dataavläsning tillämpas vid tillståndsprövningen. Rätten ska även tillämpa motsvarande förfarande som anges i 16 § den lagen. Tingsrättens beslut får inte överklagas.*

I paragrafen, som är ny, regleras frågor om tillstånd till gränsöverskridande hemlig dataavläsning av kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter. Övervägandena finns i avsnitt 13.2.2.

Enligt bestämmelsens *första mening* ska det som gäller för hemlig avlyssning och övervakning av elektronisk kommunikation vid gränsöverskridande åtgärder tillämpas på motsvarande sätt när ansökan avser hemlig dataavläsning för kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter, vilket framgår av hänvisningarna till 26 a § första och andra styckena samt 26 b §. Det innebär bl.a. att ett beslut som huvudregel ska fattas inom 96 timmar från det att ansökan kom in. Hänvisningarna i *andra meningen* till bestämmelserna i lagen om hemlig

dataavläsning motsvarar de hänvisningar som görs till rättegångsbalken för hemlig avlyssning och övervakning av elektronisk kommunikation i 26 a § tredje stycket. Hänvisningen medför bl.a. att reglerna om förbud mot hemlig dataavläsning och tillståndsprövning ska tillämpas vid en ansökan om hemlig dataavläsning. Av *tredje meningen* framgår att reglerna om offentliga ombud i 16 § lagen om hemlig dataavläsning ska tillämpas. Av *fjärde meningen* framgår att tingsrättens beslut inte får överklagas.

Hemlig dataavläsning i utlandet

Rättslig hjälp och tekniskt bistånd i utlandet med hemlig dataavläsning

28 g § *Vid rättslig hjälp och tekniskt bistånd med hemlig dataavläsning i en annan stat tillämpas 26 §.*

Tekniskt bistånd får endast avse hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning.

Om en underrättelse ska lämnas till en enskild tillämpas 28 § andra stycket lagen om hemlig dataavläsning.

I paragrafen, som är ny, regleras vad som ska gälla vid rättslig hjälp och tekniskt bistånd med hemlig dataavläsning i utlandet. Övervägandena finns i avsnitt 13.2.3.

I *första stycket* framgår att vid rättslig hjälp och tekniskt bistånd med hemlig dataavläsning i en annan stat tillämpas 26 §. Det innebär bl.a. att det är åklagare som får ansöka hos en utländsk myndighet om rättslig hjälp och tekniskt bistånd med hemlig dataavläsning 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 åtgärden. Ansökan ska då innehålla en bekräftelse på att ett sådant tillstånd har meddelats. Domstolsprövningen görs enligt lagen om hemlig dataavläsning, dvs. domstolen ska bedöma om förutsättningarna för att vidta en motsvarande åtgärd i en svensk förundersökning är uppfyllda. Om den person som åtgärden avser inte befinner sig i den stat där rättslig hjälp eller tekniskt bistånd söks, ska det av ansökan framgå att den stat där personen befinner sig har lämnat tillstånd till åtgärden.

I *andra stycket* framgår att tekniskt bistånd endast får avse hemlig dataavläsning som avser kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter.

I *tredje stycket* framgår att underrättelse till enskild inte alltid aktualiseras. När åtgärden verkställs i en annan stat ska den statens regler om underrättelse tillämpas (prop. 2006/07:133 s. 59). Det är endast när avläsning eller upptagning sker i Sverige som 28 § andra stycket lagen om hemlig dataavläsning om underrättelse till enskild ska tillämpas. Detta blir aktuellt om åtgärden verkställs genom omedelbar överföring av meddelanden eller uppgifter om meddelanden (jfr 28 d §) eller genom tekniskt bistånd med hemlig dataavläsning.

Tillstånd från en annan stat till gränsöverskridande hemlig dataavläsning

28 h § *När ett tillstånd till hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning beslutats i en brottsutredning i Sverige och avläsningen eller upptagningen kommer att göras i en medlemsstat i Europeiska unionen, Island eller Norge utan hjälp från den andra staten, tillämpas 26 c §.*

I paragrafen, som är ny, regleras när hemlig dataavläsning får verkställas gränsöverskridande utan hjälp från den andra staten. Övervägandena finns i avsnitt 13.2.3.

Bestämmelsen reglerar situationen då den person som är föremål för hemlig dataavläsning avseende kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter i en svensk brottsutredning befinner sig i ett annat EU-land eller i Island eller Norge. Om avläsningen eller upptagningen i ett sådant fall kan ske utan hjälp från den andra staten ska samma regler som gäller för gränsöverskridande hemlig avlyssning och övervakning av elektronisk kommunikation tillämpas även för hemlig dataavläsning (prop. 2004/05:144 s. 208–209 och prop. 2011/12:55 s. 141). Det innebär bl.a. att ansökan om ett sådant tillstånd görs av åklagare. Vidare finns bestämmelser om när en ansökan ska göras och vad den ska innehålla.

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

18 kap.

19 § Den tystnadsplikt som följer av 5–8, 9 och 10 §§, 11 § första stycket och 12 och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ 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, hemlig rumsavlyssning *eller hemlig dataavläsning* på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av uppgifter enligt lagen (2012:278) 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, hemlig kameraövervakning, *hemlig rumsavlyssning eller hemlig dataavläsning* 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 det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

I paragrafen regleras vilka tystnadsplikter enligt 18 kap. OSL som har företräde framför rätten att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 12.2.3.

I *andra* och *tredje styckena* införs hemlig dataavläsning i uppräkningen av åtgärder där tystnadsplikten inskränker rätten att meddela och offentliggöra uppgifter. I tredje stycket införs också hemlig rumsavlyssning som en sådan åtgärd.

44 kap.

5 § Rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer

1. av beslut som har meddelats med stöd av 7 § lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet,
2. av 7 kap. 1 § 1 lagen (2006:544) om kommuners och regioners, åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,
3. av 4 kap. 16 § försäkringsrörelselagen (2010:2043),
4. av 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige, *och*
5. *av 32 § lagen (2019:000) om hemlig dataavläsning.*

I paragrafen regleras vilka tystnadsplikter enligt särskilda regler i annan lagstiftning som har företräde framför rätten att meddela och offentliggöra uppgifter. Övervägandena finns i avsnitt 12.2.3.

I uppräkningen införs en ny punkt, 5. Ändringen innebär att den som har tystnadsplikt enligt 32 § lagen om hemlig dataavläsning inte får meddela eller offentliggöra uppgifter som han eller hon har fått del av eller tillgång till och som hänför sig till angelägenhet som avser användning av hemlig dataavläsning.

16.6 Förslaget till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

1 kap.

4 § En utredningsåtgärd enligt denna lag ska avse eller motsvara

1. förhör under förundersökning,
2. bevisupptagning vid domstol,
3. förhör genom ljudöverföring eller ljud- och bildöverföring,
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller en åtgärd enligt 27 kap. 15 § samma balk,
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning*,* hemlig rumsavlyssning och *hemlig dataavläsning,*
7. tillfälligt överförande av en frihetsberövad person,
8. rättsmedicinsk undersökning av en avliden person,
9. kontrollerad leverans,
10. bistånd i en brottsutredning med användning av en skyddsidentitet,
11. inhämtande av bevis som finns hos en myndighet, eller
12. andra åtgärder som inte innebär användning av tvångsmedel eller någon annan tvångsåtgärd.

Paragrafen innehåller en uppräkning av de utredningsåtgärder som en europeisk utredningsorder ska avse eller motsvara. Övervägandena finns i avsnitt 13.3.1.

Genom ett tillägg i *punkt 6* inkluderas hemlig dataavläsning i uppräkningen av möjliga utredningsåtgärder enligt lagen.

2 kap.

5 § Innan åklagaren utfärdar en utredningsorder ska åklagaren ansöka om domstolens tillstånd till att utfärda utredningsordern, om utredningsåtgärden avser

1. kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken,
2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *eller hemlig dataavläsning*, eller
3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m.

I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken *eller 17 § lagen (2019:000) om hemlig dataavläsning* utfärda en utredningsorder för kvarhållande av försändelse, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning *eller hemlig dataavläsning*. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

Innan en utredningsorder för husrannsakan, kroppsvisitation eller kroppsbesiktning utfärdas, får åklagaren enligt 28 kap. 4 § första stycket och 13 § första stycket rättegångsbalken ansöka om domstolens tillstånd till att utfärda utredningsordern.

För domstolens handläggning gäller vad som är föreskrivet i rättegångsbalken eller annan författning för den åtgärd som avses.

I paragrafen föreskrivs domstolsprövning av vissa utredningsåtgärder. Övervägandena finns i avsnitt 13.3.1.

I *första stycket punkt 2* läggs hemlig dataavläsning till bland de utredningsåtgärder som kräver domstolsprövning innan åklagaren får utfärda en utredningsorder. Det klargörs alltså att huvudregeln för att en utredningsorder om hemlig dataavläsning ska få utfärdas är att domstolen har lämnat tillstånd till åtgärden.

I *andra stycket* regleras undantag från första stycket. Genom en hänvisning till 17 § lagen om hemlig dataavläsning framgår att när det är tillåtet med ett interimistiskt beslut om tillstånd till hemlig dataavläsning enligt den lagen är det också på motsvarande sätt tillåtet med ett sådant beslut för att utfärda en utredningsorder om hemlig dataavläsning. Det innebär att åklagaren interimistiskt kan utfärda en utredningsorder om hemlig dataavläsning enligt 2 § första stycket 1–4 samt 6 och 7 lagen om hemlig dataavläsning men inte beträffande avläsning eller upptagning av rumsavlyssningsuppgifter.

Hemlig dataavläsning

19 a § *En utredningsorder får utfärdas för hemlig dataavläsning i Sverige eller i en annan medlemsstat.*

En utredningsorder för hemlig dataavläsning i Sverige eller i en annan medlemsstat än den stat till vilken ordern översänds enligt 7 § första stycket får endast avse en åtgärd enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning.

Om dataavläsningen enligt andra stycket ska ske i en annan medlemsstat än den stat till vilken ordern översänds enligt 7 § första stycket ska det av utredningsordern framgå att en underrättelse enligt 4 kap. 12 § har lämnats.

I paragrafen, som är ny, anges under vilka förutsättningar en utredningsorder för hemlig dataavläsning får utfärdas. Övervägandena finns i avsnitt 13.3.2.

Enligt *första stycket* får en utredningsorder utfärdas för hemlig dataavläsning i Sverige eller i en annan medlemsstat. En utredningsorder kan således sändas över till en annan medlemsstat för hemlig dataavläsning i den staten eller i en annan tredje medlemsstat. Ett skäl till det kan vara att den förstnämnda staten har de bästa tekniska förutsättningarna för att genomföra hemlig dataavläsning.

I *andra stycket* anges att en utredningsorder för hemlig dataavläsning i Sverige eller i en annan medlemsstat än den stat till vilken ordern översänds enligt 7 § första stycket endast får avse en åtgärd enligt 2 § första stycket 1–3 lagen om hemlig dataavläsning. Det innebär att en utredningsorder som har utfärdats för hemlig dataavläsning avseende avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får ske i Sverige eller i en annan medlemsstat än den stat till vilken ordern översänds. I övriga fall av hemlig dataavläsning, dvs. enligt 2 § första stycket 4–7 lagen om hemlig dataavläsning, gäller att åtgärden endast får ske i den medlemsstat dit utredningsordern har sänts. Detta omfattar avläsning eller upptagning av kameraövervakningsuppgifter, rumsavlyssningsuppgifter, elektroniskt lagrade uppgifter och uppgifter som visar hur ett avläsningsbart informationssystem används.

Av *tredje stycket* följer att om dataavläsning ska göras i en annan medlemsstat än dit utredningsordern sänts, ska det av utredningsordern framgå att en underrättelse enligt 4 kap. 12 § har lämnats. Bestämmelsen avser endast hemlig dataavläsning som sker enligt andra stycket, dvs. avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter. Den medlemsstat som ska verkställa den utredningsorder som utfärdats av en svensk åklagare ska således få information om att den medlemsstat där hemlig dataavläsning görs, t.ex. där ett telefonnummer används, har underrättats om åtgärden. Bestämmelsen är inte tillämplig om den hemliga dataavläsningen ska äga rum i Sverige eftersom den svenske åklagaren som har utfärdat utredningsordern är medveten om att avläsningen kommer att utföras här.

19 b § *När en utredningsorder för hemlig dataavläsning har utfärdats, ska 20 § andra stycket, 27 § och 28 § första stycket lagen (2019:000) om hemlig dataavläsning tillämpas. I de fall där upptagningen eller upptecknin*gen *görs i Sverige ska 28 § andra stycket lagen om hemlig dataavläsning tillämpas.*

I paragrafen som är ny, anges vilka regler i lagen om hemlig dataavläsning som ska tillämpas när en utredningsorder för hemlig dataavläsning har utfärdats i Sverige. Övervägandena finns i avsnitt 13.3.2.

Enligt paragrafen ska bestämmelserna i 20 § andra stycket, 27 § och 28 § första stycket lagen om hemlig dataavläsning tillämpas när en utredningsorder har utfärdats för hemlig dataavläsning i en annan medlemsstat. Bestämmelsen motsvarar i princip vad som gäller enligt 19 § för hemlig kameraövervakning och hemlig rumsavlyssning och innebär bl.a. att avlyssningsförbudet och reglerna om överskottsinformation är tillämpliga även i nu aktuella fall (prop. 2016/17:218 s. 256). Andra meningen innebär

att om upptagningen eller uppteckningen görs i Sverige ska reglerna om underrättelse till enskild i 28 § andra tycket lagen om hemlig dataavläsning tillämpas.

3 kap.

10 § I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken *eller 17 § lagen (2019:000) om hemlig dataavläsning*, besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation*,* hemlig kameraövervakning *eller hemlig dataavläsning.*

I paragrafen anges att åklagare i vissa fall kan meddela en verkställbarhetsförklaring i avvaktan på domstolens beslut. Övervägandena finns i avsnitt 13.2.1.

I bestämmelsen görs ett tillägg som innebär att åklagaren, i likhet med vad som gäller vid övriga hemliga tvångsmedel förutom hemlig rumsavlyssning, får ge ett interimistiskt beslut att erkänna en utredningsorder för hemlig dataavläsning. Genom hänvisningen till 17 § lagen om hemlig dataavläsning framgår att erkännande och verkställighet av en utredningsorder får göras interimistiskt för hemlig dataavläsning, som gäller alla typer av uppgifter som anges i 2 § andra stycket lagen om hemlig dataavläsning utom rumsavlyssningsuppgifter.

Hemlig dataavläsning

37 a § *Vid verkställighet av en utredningsorder för hemlig dataavläsning som gäller en åtgärd enligt 2 § första stycket 1 och 2 lagen (2019:000) om hemlig dataavläsning tillämpas 34 § detta kapitel.*

Vid verkställighet enligt 34 § 1 tillämpas 35 § andra stycket. I dessa fall får någon upptagning eller uppteckning inte göras i Sverige, och 28 § andra stycket lagen om hemlig dataavläsning ska inte tillämpas.

I paragrafen, som är ny, regleras vad som gäller för verkställighet av en utredningsorder när det är fråga om hemlig dataavläsning för kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter enligt 2 § första stycket 1–2 lagen om hemlig dataavläsning. Övervägandena finns i avsnitt 13.3.3.

Genom hänvisningen i *första stycket* till 34 § framgår att vid verkställighet av en utredningsorder i fråga om hemlig dataavläsning för kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter ska motsvarande tillämpas som vid verkställighet av en utredningsorder för hemlig avlyssning och övervakning av elektronisk kommunikation (prop. 2016/17:218 s. 284–285). Det innebär att åklagaren efter samråd med behörig myndighet i den andra medlemsstaten ska besluta om verkställighet ska genomföras genom omedelbar överföring eller genom upptagning eller uppteckning i Sverige.

I *andra stycket* regleras vad som ska gälla när verkställigheten sker genom omedelbar överföring till den andra medlemsstaten av meddelanden eller uppgifter om meddelanden enligt 34 § 1. Vid sådan verkställighet

får någon upptagning eller uppteckning inte göras i Sverige och bestämmelsen om underrättelse till enskild i 28 § andra stycket lagen om hemlig dataavläsning ska inte tillämpas. Genom hänvisningen till 35 § andra stycket gäller att om åklagaren har meddelat en interimistisk verkställbarhetsförklaring enligt 10 § får verkställighet ske först efter det att domstolen har fastställt förklaringen. Motsvarande gäller vid verkställighet av en utredningsorder för hemlig avlyssning och övervakning av elektronisk kommunikation (prop. 2016/17:218 s. 285–286).

37 b § *Vid verkställighet av en utredningsorder för hemlig dataavläsning som sker med stöd av 34 § 2 eller i andra fall av verkställighet av en utredningsorder för hemlig dataavläsning behöver upptagningar eller uppteckningar inte granskas enligt 28 § första stycket lagen (2019:000) om hemlig dataavläsning. Upptagningar och uppteckningar, som finns kvar i Sverige efter det att ärendet har avslutats hos åklagaren och bevismaterialet har överlämnats med stöd av 38 eller 40 §, får bevaras endast om detta är tillåtet enligt 28 § första stycket lagen om hemlig dataavläsning.*

I fråga om underrättelse till en enskild enligt 28 § andra stycket lagen om hemlig dataavläsning ska bestämmelserna i 36 § andra stycket detta kapitel tillämpas.

Paragrafen, som är ny, innehåller bestämmelser om hanteringen av inhämtat material och om underrättelseskyldighet gentemot en enskild eller enskilda när upptagning eller uppteckning sker i Sverige. Övervägandena finns i avsnitt 13.3.3.

Paragrafen omfattar hemlig dataavläsning avseende kommunikationsavlyssnings- och kommunikationsövervakningsuppgifter som ska verkställas genom upptagning eller uppteckning i Sverige av meddelanden eller uppgifter om meddelanden. Paragrafen omfattar också hemlig dataavläsning enligt 2 § första stycket 3–7 lagen om hemlig dataavläsning, dvs. platsuppgifter, kameraövervakningsuppgifter, rumsavlyssningsuppgifter, elektroniskt lagrade uppgifter och uppgifter som visar hur ett avläsningsbart informationssystem används.

Av *första stycket* följer att upptagningar eller uppteckningar inte behöver granskas enligt 28 § första stycket lagen om hemlig dataavläsning. Undantaget från granskningsskyldigheten gäller emellertid inte sådan granskning som t.ex. avser att avbryta åtgärden om avläsningsförbud råder eller uppgifterna är skyddade enligt beslagsförbudsregeln, se 27 § lagen om hemlig dataavläsning. Upptagningar och uppteckningar som finns kvar i Sverige efter det att ärendet har avslutats hos åklagaren och bevismaterialet har överlämnats med stöd av 38 eller 40 § förevarande lag, får bevaras endast om detta är tillåtet enligt 28 § första stycket lagen om hemlig dataavläsning. Motsvarande gäller för övriga hemliga tvångsmedel.

Av *andra stycket* framgår att i fråga om underrättelse till enskild enligt 28 § andra stycket lagen om hemlig dataavläsning ska 36 § andra stycket i denna lag tillämpas beträffande hemlig dataavläsning (prop. 2016/17:218 s. 286–287). I sistnämnda paragraf hänvisas till 27 kap. 31–33 §§ RB med vissa nödvändiga förändringar som t.ex. att tidpunkten då underrättelse ska lämnas inte räknas från dagen då förundersökningen avslutas utan från då åtgärden avslutades. Vidare följer av bestämmelsen att när en enskild ska underrättas om hemlig dataavläsning ska underrättelsen ta sikte på använd-

aren av det avläsningsbara informationssystemet i stället för ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning.

4 kap.

15 a § *Det som anges om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation i 12–15 §§ tillämpas även för hemlig dataavläsning enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning.*

I paragrafen, som är ny, finns bestämmelser om underrättelse till en annan medlemsstat och om underrättelse till Sverige. Övervägandena finns i avsnitt 13.3.4.

Enligt bestämmelsen ska det som gäller för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation avseende underrättelse till en annan medlemsstat när avlyssning eller övervakning ska genomföras på den andra statens territorium (12 §) även gälla för hemlig dataavläsning när åtgärden avser avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter enligt 2 § första stycket 1–3 lagen om hemlig dataavläsning. I bestämmelsen anges också att det som gäller när en annan medlemsstat underrättar Sverige om hemlig avlyssning och övervakning av elektronisk kommunikation i Sverige utan bistånd av en svensk myndighet (13–15 §§) också ska gälla för hemlig dataavläsning när åtgärden avser avläsning eller upptagning av kommunikationsavlyssnings, kommunikationsövervaknings- eller platsuppgifter (prop. 2016/17:218 s. 299–303).

Sammanfattning av betänkandet Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89)

Vårt uppdrag

Vi har haft i uppdrag att överväga om de brottsbekämpande myndigheterna bör få möjlighet att använda hemlig dataavläsning för att bekämpa terroristbrott och andra allvarliga brott. I uppdraget har bland annat ingått att

- ta reda på vilket behov de brottsbekämpande myndigheterna har av hemlig dataavläsning,
- undersöka om hemlig dataavläsning skulle vara en effektivmetod för att bekämpa terroristbrottslighet och andra allvarliga brott,
- klargöra om intresset av att upprätthålla ett starkt skydd för den personliga integriteten ger utrymme för att tillåta hemlig dataavläsning,
- analysera om det är lämpligt att införa hemlig dataavläsning som ett nytt straffprocessuellt tvångsmedel, och
- lämna fullständiga förslag till författningsändringar eller andra
- förändringar oavsett vad analysen föranleder.

Vad är hemlig dataavläsning?

Eftersom hemlig dataavläsning inte finns som metod i Sverige saknas en definition av vad åtgärden innebär. Vår utgångspunkt i analysen av behovs-, effektivitets- och integritetsaspekter har varit att hemlig data-avläsning är en metod för de brottsbekämpande myndigheterna att med någon form av tekniskt hjälpmedel i hemlighet bereda sig tillgång till en dator eller annan teknisk utrustning som kan användas för kommunikation och därigenom få besked om hur utrustningen används eller har använts och vilken information som finns i den. Med metoden kan man komma åt både uppgifter som i dag får hämtas in med nuvarande hemliga tvångsmedel, t.ex. innehåll i meddelanden (som får hämtas in efter tillstånd till hemlig avlyssning av elektronisk kommunikation), och uppgifter som i dag inte får hämtas in med hemliga tvångsmedel, t.ex. uppgifter som finns lagrade i en dator eller telefon (som dock får hämtas in med öppna tvångsmedel, exempelvis vid undersökning av beslag).

Internationell utblick

I många andra länder finns lagstiftning som möjliggör hemlig data-avläsning eller en motsvarighet till metoden.

Danmark var det första av de nordiska länderna att införa tvångsmedlet när landet år 2002 införde en regel om dataaflæsning i retsplejeloven. Även Finland har lagstiftning, bland annat i tvångsmedelslagen och polislagen, som i praktiken motsvarar hemlig dataavläsning. Sedan hösten 2016 används metoden också i Norge, där regler om dataavlesing införts i straffeprosessloven.

Våra bedömningar och förslag

Vilket behov av hemlig dataavläsning har de brottsbekämpande myndigheterna?

Under de senaste åren har den tekniska utvecklingen liksom brotts- och samhällsutvecklingen i övrigt lett till att de brottsbekämpande myndigheterna inte längre kan ta del av många av de uppgifter som man tidigare fick del av genom användande av straffprocessuella tvångsmedel som hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation. Framför allt är det den kraftigt ökade användningen av kryptering i förening med att en mycket stor andel av kommunikationen i dag sker via internet som är orsaken till detta. I dag är till exempel mer än 90 procent av den avlyssnade internettrafiken krypterad. Det innebär alltså att de brottsbekämpande myndigheterna faktiskt bara kan läsa av mindre än tio procent av den datakommunikation som får avlyssnas eller övervakas. Även utrustning, till exempel datorer och mobiltelefoner, krypteras eller lösenordskyddas i allt högre utsträckning. En annan orsak till utvecklingen är anonymisering. Anonymisering sker till exempel då någon använder ett WiFi-nätverk eller särskilda anonymiseringstjänster som medför att det i princip blir omöjligt att upptäcka och identifiera en persons aktiviteter på internet med dagens verkställighetsmetoder.

Vår bedömning är att det mot denna bakgrund finns ett tungt vägande behov av nya och bättre metoder för att de brottsbekämpande myndigheterna i hemlighet ska kunna komma åt uppgifter som redan i dag får hämtas in samt vissa andra uppgifter. Till grund för den bedömningen ligger också de kriminellas medvetenhet om hur nuvarande metoder fungerar liksom andra svårigheter att i vissa fall verkställa hemliga tvångsmedel.

Det konstaterade behovet är lika tungt vägande i brottsutredande verksamhet som i underrättelseverksamhet.

Är hemlig dataavläsning en effektiv metod för att bekämpa terroristbrottslighet och annan allvarlig brottslighet?

Hemlig dataavläsning kan användas som metod för att komma åt sådana uppgifter som de brottsbekämpande myndigheterna har ett starkt behov av. Metoden kommer dock inte att kunna användas i alla de fall där det finns behov av den. När hemlig dataavläsning kan genomföras förväntas den leda till betydligt bättre information än vad dagens metoder gör. Metoden är dock resurskrävande och kommer att medföra kostnadsökningar. Den bör därför i första hand användas i kampen mot den allra allvarligaste brottsligheten. I de fallen förväntas hemlig dataavläsning vara en effektiv åtgärd.

Ger intresset av att upprätthålla ett starkt skydd för den personliga integriteten utrymme för att tillåta hemlig dataavläsning?

Vår integritetsriskanalys har utgått från i vilken utsträckning hemlig dataavläsning kan medföra ökade risker för den personliga integriteten jämfört med dagens ordning. Slutsatsen är att hemlig dataavläsning i flera avseenden innebär att riskerna för enskildas personliga integritet ökar. De tre allvarligaste riskerna som vi har identifierat är att hemlig dataavläsning

- kan medföra en närmast fullständig kartläggning och övervakning av den person som utsätts för åtgärden om inte tydliga begränsningar görs
- om metoden används för att optiskt övervaka eller avlyssna personer kan medföra en mycket långtgående övervakning om inte tydliga begränsningar görs
- kan innebära att informationssäkerheten utanför den tekniska utrustning som åtgärden avser minskar om inte särskilda krav ställs upp.

Proportionalitetsavvägningen

Vi har vägt de risker som metoden för hemlig dataavläsning i sig innebär och riskerna som finns med att alls tillåta hemlig inhämtning av de olika typer av uppgifter som hemlig dataavläsning kan ge tillgång till mot intresset av en effektiv brottsbekämpning och det starka behov som finns av nya och bättre metoder för att samla in betydelsefull information. Vår slutsats är att det är proportionerligt att införa regler om hemlig data-avläsning under förutsättning att reglerna balanserar de ökade integritetsriskerna och riskerna för informationssäkerheten som kan uppstå med hemlig dataavläsning.

En ny lag om hemlig dataavläsning införs

Vi föreslår att en ny lag med bestämmelser om hemlig dataavläsning införs. Lagen tidsbegränsas till att gälla i fem år efter införandet för att en utvärdering av tvångsmedlet ska kunna göras när lagen har tillämpats en tid.

Enligt definitionen i den nya lagen innebär hemlig dataavläsning en avläsning eller upptagning som sker i hemlighet med ett tekniskt hjälpmedel, av uppgifter avsedda för automatiserad behandling i ett informationssystem. Med informationssystem avses antingen

- elektronisk kommunikationsutrustning (till exempel datorer och mobiltelefoner) eller
- ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst.

Ett tillstånd till hemlig dataavläsning får beslutas endast om det är proportionerligt, dvs. om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Vilka uppgifter ska de brottsbekämpande myndigheterna få läsa av?

Vi föreslår att hemlig dataavläsning får användas för att läsa av eller ta upp följande uppgiftstyper.

1. Uppgifter om innehållet i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress (kommunikationsavlyssningsuppgifter),
2. uppgifter om annat än innehållet i sådana meddelanden som anges i första punkten (kommunikationsövervakningsuppgifter),
3. uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits (lokaliseringsuppgifter),
4. uppgifter som innebär optisk personövervakning (kameraövervakningsuppgifter),
5. uppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till (rumsavlyssningsuppgifter),
6. uppgifter som finns lagrade i ett informationssystem men som inte avses i 1–5 eller
7. uppgifter som visar hur informationssystemet används men som inte kan läsas av eller tas upp enligt 1–6.

När det är fråga om att använda hemlig dataavläsning för att läsa av eller ta upp uppgifter enligt punkterna 1 eller 2 får meddelanden också hindras från att nå fram.

Bestämmelsen om uppgiftstyper reglerar endast vilka sådana som hemlig dataavläsning kan få användas för att läsa av eller ta upp. Vilken typ av uppgift som ett tillstånd sedan faktiskt avser i ett enskilt fall bestäms av domstolen utifrån ändamålet med åtgärden.

När ska hemlig dataavläsning få användas?

Utgångspunkter

Som framgår av förteckningen över vilka uppgiftstyper hemlig dataavläsning bör få användas för motsvarar dessa i hög utsträckning uppgifter som i dag får hämtas in med andra tvångsmedel, både öppna och hemliga. En utgångspunkt för oss har varit att när hemlig dataavläsning ska få användas för att läsa av eller ta upp uppgifter som får hämtas in efter tillstånd till andra hemliga tvångsmedel bör motsvarande möjligheter och krav gälla för hemlig dataavläsning som gäller för de ”bakomliggande” tvångsmedlen. Metoden blir i de fallen i praktiken ett sätt att verkställa dessa hemliga tvångsmedel (punkterna 1–5).

Vid hemlig dataavläsning för att läsa av eller ta upp uppgifter som i dag inte är möjliga att hämta in genom hemliga tvångsmedel (lagrade uppgifter och uppgifter som visar hur ett informationssystem används, punkterna 6 och 7) har vår utgångspunkt varit att motsvarande krav för tillstånd till hemlig dataavläsning som gäller för tillstånd till hemlig avlyssning av elektronisk kommunikation ska gälla.

Utgångspunkterna är dock inte utan undantag. I de fall informations-, integritets-, rättssäkerhets- eller andra intressen föranleder strängare krav vid hemlig dataavläsning bör sådana införas.

De angivna utgångspunkterna gör sig gällande både i den brottsutredande verksamheten då de bakomliggande tvångsmedlen regleras i rättegångsbalken (förundersökningsfallen) och i sådan underrättelseverksamhet där det i dag är möjligt att få tillstånd till hemliga tvångsmedel (underrättelsefallen). Underrättelsefallen används som samlingsbeteckning då de bakomliggande tvångsmedlen regleras i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen), lagen om särskild utlänningskontroll (LSU) och lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen).

Hemlig dataavläsning i förundersökningsfallen

Som ett grundläggande krav gäller att hemlig dataavläsning aldrig får användas vid en förundersökning om något annat brott än ett sådant som kan föranleda tillstånd till hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § rättegångsbalken (normalt brott med ett minimistraff på två års fängelse). Om hemlig dataavläsning ska användas för att läsa av eller ta upp rumsavlyssningsuppgifter krävs dock i stället att det är fråga om brott som kan föranleda tillstånd till hemlig rumsavlyssning (normalt brott med ett minimistraff på fyra års fängelse).

Hemlig dataavläsning får som utgångspunkt användas endast om någon är skäligen misstänkt för brottet. Det enda undantag som finns är när hemlig dataavläsning behövs för att utreda vem som skäligen kan misstänkas för brottet. Undantaget motsvarar vad som gäller i dag enligt 27 kap. 20 § andra stycket rättegångsbalken, dock med något strängare krav för hemlig dataavläsning. Åtgärden ska alltid vara av synnerlig vikt för utredningen.

Motsvarande platskrav (och förbud avseende vissa platser) som gäller vid hemlig kameraövervakning och hemlig rumsavlyssning ska gälla när hemlig dataavläsning avser kameraövervaknings- respektive rumsavlyssningsuppgifter. Möjligheten att med hemlig dataavläsning skaffa sig tillgång till sådana uppgifter sträcker sig således inte längre än dagens hemliga tvångsmedel.

Hemlig dataavläsning i preventivlagsfallen

Motsvarande förutsättningar som gäller för tillstånd till hemlig avlyssning av elektronisk kommunikation enligt preventivlagen ska gälla för tillstånd till hemlig dataavläsning i preventivlagsfallen. Vid avläsning eller upptagning av kameraövervakningsuppgifter ska dessutom krav motsvarande de som uppställs i preventivlagen för hemlig kameraövervakning tillämpas. Hemlig dataavläsning får i preventivlagsfallen inte användas för att läsa av eller ta upp rumsavlyssningsuppgifter. Det bör understrykas att möjligheterna att i dag använda hemliga tvångsmedel enligt preventivlagen är starkt begränsade till allvarlig brottslighet under vissa särskilda

förhållanden. Samma gäller alltså vid hemlig dataavläsning i preventivlagsfallen.

Hemlig dataavläsning i LSU-fallen

Motsvarande förutsättningar som gäller för tillstånd till hemlig avlyssning av elektronisk kommunikation enligt LSU ska gälla för att tillstånd till hemlig dataavläsning ska kunna meddelas i LSU-fallen. Hemlig dataavläsning får i LSU-fallen inte avse avläsning eller upptagning av kameraövervaknings- eller rumsavlyssningsuppgifter.

Hemlig dataavläsning i inhämtningslagsfallen

Hemlig dataavläsning i inhämtningslagsfallen får endast avse historiska kommunikationsövervakningsuppgifter och lokaliseringsuppgifter, såväl historiska som i realtid, och motsvarar därför helt vad som gäller beträffande vilka uppgifter som får hämtas in enligt inhämtningslagen. Åtgärden får endast avse uppgifter i ett identifierbart informationssystem, dock inte i sådant system som tillhör någon som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

Förbud mot hemlig dataavläsning

Hemlig dataavläsning får aldrig avse uppgifter i informationssystem som stadigvarande används i verksamheter som tystnadsplikt gäller för och som anges i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, exempelvis advokatverksamheter och medieverksamheter.

Om det vid genomförande av hemlig dataavläsning kommer fram att uppgifter som läses av eller tas upp skyddas enligt reglerna om beslagsförbudet i 27 kap. 2 § första stycket rättegångsbalken ska avläsningen omedelbart avbrytas och upptagningarna omedelbart förstöras i de delar som de omfattas av skyddet.

Motsvarande avlyssningsförbud som i dag gäller vid hemlig avlyssning av elektronisk kommunikation och hemlig rumsavlyssning införs beträffande avläsning av kommunikationsavlyssnings- och rumsavlyssningsuppgifter.

Tillträdestillstånd

Vid tillstånd till hemlig dataavläsning får rätten meddela särskilt tillstånd för den brottsbekämpande myndigheten att i hemlighet installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Det krävs dock att det finns särskild anledning att anta att informationssystemet som tillståndet avser finns där. Om ansökan om sådant tillstånd gäller stadigvarande bostad som inte är en misstänkts krävs i stället att det finns synnerlig anledning att anta att informationssystemet finns där. Ett tillträdestillstånd får dock aldrig avse platser där hemlig rumsavlyssning inte får ske.

Tillståndsprövning

Frågor om tillstånd till hemlig dataavläsning ska alltid prövas av allmän domstol. I förundersökningsfallen ska samma forumregler gälla som i rättegångsbalken medan det i underrättelsefallen alltid är Stockholms tingsrätt som ska pröva ansökan. Som utgångspunkt är åklagaren den som ansöker om tillstånd, men undantag gäller i LSU-fallen där, liksom i dag, antingen Polismyndigheten eller Säkerhetspolisen ska ansöka.

I ett tillstånd till hemlig dataavläsning ska anges vilken tid (aldrig längre än en månad framåt i tiden), vilket informationssystem, vilken typ av uppgift och, i förekommande fall, vilken plats tillståndet avser. Det ska också anges vem som är misstänkt för brottet när åtgärden avser avläsning eller upptagning av rumsavlyssningsuppgifter.

Om tillståndet till hemlig dataavläsning har förenats med tillträdestillstånd ska platsen för det anges. Därtill ska särskilda villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan anges i tillståndet.

Åklagaren får fatta interimistiska beslut om hemlig dataavläsning i vissa fall, dock inte när hemlig dataavläsning avser rumsavlyssningsuppgifter eller i LSU-fallen.

Vid alla ärenden i domstol om hemlig dataavläsning ska det hållas sammanträde där ett offentligt ombud och den som gjort ansökan närvarar. I övrigt är ordningen vid hemlig dataavläsning densamma som gäller enligt rättegångsbalken beträffande offentliga ombud och sammanträdet. På förfarandet enligt lagen i övrigt ska reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor tillämpas. Handläggningen ska ske skyndsamt.

När ett beslut om tillstånd till hemlig dataavläsning fattats är det möjligt att verkställa omedelbart. Om det inte längre finns skäl för åtgärden ska den som gjort ansökan eller rätten omedelbart häva beslutet.

Genomförande av hemlig dataavläsning

När ett tillstånd till hemlig dataavläsning har lämnats får de tekniska hjälpmedel som behövs för avläsning eller upptagning användas. Den verkställande myndigheten får, om det är nödvändigt för att verkställighet ska kunna ske, bryta eller kringgå skydd och utnyttja sårbarheter för att bereda sig tillgång till informationssystemet samt använda tekniska hjälpmedel i informationssystemet. Sådana åtgärder får endast vidtas efter att tillstånd till hemlig dataavläsning har lämnats.

En särskild regel om att den teknik som används för verkställighet ska anpassas efter det tillstånd som meddelats införs så att det inte ska vara möjligt att läsa av eller ta upp någon annan uppgiftstyp än den som tillståndet avser. Om andra typer av uppgifter än tillståndet avser ändå läses av eller tas upp ska dels upptagningarna av de felaktigt inhämtade uppgifterna omedelbart förstöras, dels Säkerhets- och integritetsskyddsnämnden underrättas. Uppgifter som har kommit fram vid avläsning eller upptagning av en uppgiftstyp som inte avses i tillståndet får inte heller användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

En allmän aktsamhetsregel införs som innebär att det vid genomförande av hemlig dataavläsning inte får förorsakas olägenhet eller skada utöver vad som är absolut nödvändigt. Med hänsyn till risker för informationssäkerheten föreskrivs också att en särskilt utsedd person ska ansvara för verkställigheten av hemlig dataavläsning och att denne ska vidta nödvändiga och tillräckliga åtgärder för att informationssäkerheten utanför det informationssystem tillståndet avser inte åsidosätts, minskas eller skadas till följd av åtgärden. Den verkställande myndigheten ska dessutom vidta de åtgärder som behövs för att säkerheten i det informationssystem som tillståndet avser, när verkställigheten avslutas, ska hålla åtminstone samma nivå som vid verkställighetens början. I lagen tas också in en bestämmelse om att ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet gått ut eller tillståndet hävts.

Vissa andra rättssäkerhetsgarantier

Användning av överskottsinformation

Under förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation beträffande användning av överskottsinformation gälla för hemlig dataavläsning. När det är fråga om att läsa av eller ta upp rumsavlyssningsuppgifter ska dock i stället det som gäller för användning av överskottsinformation vid hemlig rumsavlyssning enligt rättegångsbalken gälla. I underrättelseverksamhet ska motsvarande det som gäller för användning av överskottsinformation enligt preventivlagen, LSU och inhämtningslagen gälla även för hemlig dataavläsning.

Granskning, bevarande och förstörande av upptagningar och uppteckningar vid hemlig dataavläsning

Under förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation beträffande granskning, bevarande och förstörande av upptagningar och uppteckningar gälla för hemlig dataavläsning. I de fall särreglering av hemlig rumsavlyssning görs ska dock motsvarande gälla när hemlig dataavläsning avser eller har avsett rums avlyssningsuppgifter. I underrättelsefallen ska motsvarande det som gäller för granskning, bevarande och förstörande av upptagningar och uppteckningar enligt preventivlagen, LSU och inhämtningslagen gälla även för hemlig dataavläsning.

Underrättelse till enskild om hemlig dataavläsning

Motsvarande regler som gäller för underrättelse till enskild vid hemlig avlyssning av elektronisk kommunikation enligt rättegångsbalken och preventivlagen ska gälla enligt lagen om hemlig dataavläsning när hemlig dataavläsning använts i förundersökningsfallen och preventiv-lagsfallen. De särskilda regler som gäller för hemlig kameraövervakning och hemlig rumsavlyssning ska tillämpas även för hemlig dataavläsning avseende kameraövervakningsuppgifter och rumsavlyssningsuppgifter.

Det som gäller för Säkerhets- och integritetsskyddsnämndens utövande av tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel enligt lagen om tillsyn över viss brottsbekämpande verksamhet och förordningen med instruktion för Säkerhets- och integritetsskyddsnämnden kommer att gälla även användning av hemlig dataavläsning enligt den föreslagna lagen. Det krävs inte några kompletterande bestämmelser för att nämnden ska kunna utöva sin tillsyn.

Mot bakgrund av vikten av en aktiv tillsyn införs dock en bestämmelse i lagen om hemlig dataavläsning som innebär att när en domstol har meddelat beslut att tillåta hemlig dataavläsning ska den underrätta Säkerhets- och integritetsskyddsnämnden om beslutet. På så vis får nämnden tidigt kännedom om ärendet och kan inleda ett tillsynsärende redan under pågående verkställighet.

Medverkan vid verkställighet

Den som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § lagen om elektronisk kommunikation får bistå den verkställande myndigheten i samband med verkställighet av hemlig dataavläsning. Den operatör som medverkar har rätt till ersättning för de kostnader som uppstår. Ersättning för medverkan betalas av den verkställande myndigheten.

Sekretess-, tystnadsplikts-, och partsinsynsfrågor

Hemlig dataavläsning läggs till i de uppräkningar av hemliga tvångsmedel som görs i 18 kap. 19 § andra och tredje styckena offentlighets- och sekretesslagen för att klargöra att tystnadsplikten ska ha företräde framför rätten att meddela och offentliggöra uppgifter när det gäller intresset av att förebygga eller beivra brott.

En särskild sekretessregel införs för den som i samband med verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen om elektronisk kommunikation har fått del av eller tillgång till uppgift som hänför sig till angelägenhet som avser användning av hemlig dataavläsning. Tystnadsplikten enligt den bestämmelsen ska ha företräde framför rätten att meddela och offentliggöra uppgifter.

Kvalifikationskrav på den som ansvarar för verkställighet

Myndighetschefen vid den myndighet som ska verkställa hemlig dataavläsning utser den som får ansvara för verkställighet av hemlig dataavläsning. Den som utses måste ha de särskilda kunskaper om informationssäkerhet som behövs och den särskilda kompetens, utbildning och erfarenhet som är nödvändig samt i övrigt vara särskilt lämpad för uppdraget.

Frågor om det internationella samarbetet

Regler om hemlig dataavläsning införs i både lagen om internationell rättslig hjälp i brottmål och i den föreslagna lagen om europeisk utredningsorder. I lagen om internationell rättslig hjälp i brottmål tas tvångsmedlet upp som en åtgärd som rättslig hjälp omfattar och nya bestämmelser om tvångsmedlet införs. I den föreslagna lagen om europeisk utredningsorder tas hemlig dataavläsning upp i förteckningen som anger vad en utredningsåtgärd avser eller motsvarar. Nya bestämmelser om hemlig dataavläsning tas också in i den föreslagna lagen.

Våra synpunkter beträffande exekutiv jurisdiktion och elektroniskt lagrade uppgifter

Sveriges hållning när det gäller exekutiv jurisdiktion vid tvångsmedelsanvändning är att svenska brottsbekämpande myndigheter inte har rätt att ta del av elektroniskt lagrade uppgifter om de är lagrade i andra stater, oavsett om ägaren eller innehavaren av informationen finns i Sverige och om andra faktorer anknyter till Sverige. Inte heller om det är oklart var uppgifterna lagras har de svenska brottsbekämpande myndigheterna ansetts ha rätt att bereda sig tillgång till dem. Detta är ett utflöde av den svenska tolkningen av territorialitetsprincipen vid exekutiv jurisdiktion.

Det finns enligt vår uppfattning starka skäl att nyansera denna hittillsvarande officiella svenska hållning. Detta gäller särskilt i de fall då det inte är känt och inte kan klarläggas i vilket eller vilka länder som de elektroniska uppgifterna lagras (loss of location). Frågan bör dock inte nu bli föremål för nationell lagstiftning utan den bör prövas i rättstillämpningen.

Sverige bör också aktivt arbeta för att få till stånd internationella överenskommelser i aktuella frågor. Ett första steg bör vara att så snart som möjligt ratificera it-brottskonventionen för att få delta i de samtal och diskussioner som för närvarande förs på området i Europarådet.

Ekonomiska konsekvenser och genomförande av våra förslag

Förslaget om hemlig dataavläsning bedöms leda till ökade kostnader, särskilt för de brottsbekämpande myndigheter som ska kunna verkställa hemlig dataavläsning (dvs. Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket). Kostnadsökningarna för dessa brottsbekämpande myndigheter bör fördelas mellan dem och bör huvudsakligen rymmas inom befintliga anslag eller i vart fall genom omfördelning av befintliga anslag. Anskaffning av teknisk utrustning som utgör anläggningstillgångar ska finansieras med lån i Riksgäldskontoret. Det kan kräva utvidgade låneramar.

Förslaget om hemlig dataavläsning bedöms också leda till ökade kostnader för Säkerhets- och integritetsskyddsnämnden. Nämndens anslag bedöms endast till en mindre del kunna täcka kostnadsökningarna. Dess anslag bör höjas i motsvarande mån som nu varande anslag inte förslår.

Ramhöjningen bör finansieras genom omfördelningar inom rättsväsendets anslag.

De kostnadsökningar som kan förväntas för andra myndigheter inom rättsväsendet och för offentliga ombud bedöms rymmas inom befintliga anslag.

Vi föreslår att lagen om hemlig dataavläsning ska träda i kraft den 1 januari 2019 och tidsbegränsas att gälla till och med den 31 december 2023. Det finns inte behov av några särskilda övergångsbestämmelser.

Betänkandets lagförslag

Förslag till lag (2019:000) om hemlig dataavläsning

Härigenom föreskrivs följande.

Definitioner

1 § Med hemlig dataavläsning avses avläsning eller upptagning som sker i hemlighet med ett tekniskt hjälpmedel, av uppgifter avsedda för automatiserad behandling i ett informationssystem.

Med informationssystem avses i denna lag antingen

1. elektronisk kommunikationsutrustning, eller
2. ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst.

Uppgiftstyper som får läsas av eller tas upp

2 § Hemlig dataavläsning får användas, endast efter tillstånd enligt denna lag, för att läsa av eller ta upp uppgifter

1. om innehåll i meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress,
2. om annat än innehållet i sådana meddelanden som anges i 1,
3. om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits,
4. som innebär optisk personövervakning,
5. som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till
6. som finns lagrade i ett informationssystem men inte avses i 1–5 eller
7. som visar hur ett informationssystem används men inte avses i 1–6.

Vid hemlig dataavläsning enligt första stycket 1 eller 2 får meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts även hindras från att nå fram.

Grundläggande förutsättningar för hemlig dataavläsning

3 § Ett tillstånd till hemlig dataavläsning får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktas mot eller för något annat motstående intresse.

Hemlig dataavläsning under en förundersökning

4 § Hemlig dataavläsning får, om inte annat anges i andra eller tredje stycket, användas vid en förundersökning om brott som anges i 27 kap. 18 § andra stycket rättegångsbalken om någon är skäligen misstänkt för

brottet och åtgärden är av synnerlig vikt för utredningen. En åtgärd enligt 2 § första stycket 4 får användas endast på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Hemlig dataavläsning enligt 2 § första stycket 2 och 3 får också användas för att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Om åtgärden innebär att uppgifter om meddelanden enligt 2 § första stycket 2 läses av eller tas upp får uppgifterna dock endast avse förfluten tid.

Hemlig dataavläsning enligt 2 § första stycket 5 får endast användas vid en förundersökning om brott som anges i 27 kap. 20 d § andra stycket rättegångsbalken om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Är platsen någon annan stadigvarande bostad än den misstänktes, får hemlig dataavläsning enligt 2 § första stycket 5 användas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. På en plats som anges i 12 § tredje stycket får hemlig dataavläsning enligt 2 § första stycket 5 aldrig användas.

5 § Hemlig dataavläsning får, om inte annat anges i andra eller tredje stycket, endast avse uppgifter i ett identifierbart informationssystem som används av eller som det finns särskild anledning att anta har använts eller kommer att användas av den misstänkte.

Hemlig dataavläsning enligt 2 § första stycket 1–3 får avse uppgifter i ett identifierbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Hemlig dataavläsning i fall som anges i 4 § andra stycket får avse uppgifter i ett identifierbart informationssystem som har använts vid ett brott eller i anslutning till en brottsplats vid brottstidpunkten eller som av annan anledning är av synnerlig betydelse för att utreda vem som skäligen kan misstänkas för brottet. Åtgärden får inte avse uppgifter i informationssystem som tillhör någon som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

Hemlig dataavläsning utanför en förundersökning

Förhindrande av vissa särskilt allvarliga brott

6 § Tillstånd till hemlig dataavläsning får meddelas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar brott som anges i 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Ett sådant tillstånd får också meddelas om det finns en påtaglig risk för att det inom en organisation eller grupp kommer att utövas sådan brottslig verksamhet och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet.

Tillstånd enligt första stycket får meddelas endast om åtgärden är av synnerlig vikt för att förhindra sådan brottslig verksamhet som anges i

första stycket. En åtgärd enligt 2 § första stycket 4 får användas endast på en plats där den person som anges i första stycket kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Ett tillstånd enligt första stycket får inte avse hemlig dataavläsning enligt 2 § första stycket 5.

7 § Hemlig dataavläsning i fall som anges i 6 § får, om inte annat anges i andra stycket, endast avse uppgifter i ett identifierbart informationssystem som används av eller som det finns särskild anledning att anta har använts eller kommer att användas av en person som anges där.

När det är fråga om hemlig dataavläsning enligt 2 § första stycket 1–3 får åtgärden avse uppgifter i ett identifierbart informationssystem som det finns synnerlig anledning att anta att en person som anges i 6 § under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Särskild utlänningskontroll

8 § Tillstånd till hemlig dataavläsning får meddelas om

1. ett beslut enligt 1 § 2 lagen (1991:572) om särskild utlänningskontroll om utvisning av en utlänning har fattats på grund av att det med hänsyn till vad som är känt om utlänningens tidigare verksamhet och övriga omständigheter kan befaras att han eller hon kommer att begå eller medverka till terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller försök, förberedelse eller stämpling till sådant brott,
2. en myndighet eller en domstol som enligt 11 §, 11 a, 14 § eller 15 § lagen (1991:572) om särskild utlänningskontroll får besluta att 19–22 §§ den lagen ska tillämpas på utlänningen, av skäl som gäller för ett sådant beslut och med tillämpning av motsvarande förfarande, har bestämt att denna lag ska tillämpas på utlänningen som utvisningsbeslutet avser,
3. det är av betydelse för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för, planlägger eller förbereder brott som anges i 1 och
4. det finns synnerliga skäl.

Ett tillstånd enligt första stycket får inte avse hemlig dataavläsning enligt 2 § första stycket 4 eller 5.

9 § Hemlig dataavläsning i fall som anges i 8 § får endast avse uppgifter i ett identifierbart informationssystem som används av eller som det finns särskild anledning att anta har använts eller kommer att användas av en person som anges i 8 § första stycket 1.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

10 § Tillstånd till hemlig dataavläsning enligt 2 § första stycket 2 och 3 får meddelas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år eller brott som anges i 3 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. 2 § andra stycket tillämpas inte vid hemlig dataavläsning enligt denna bestämmelse.

Om hemlig dataavläsning i fall som anges i första stycket innebär att uppgifter om meddelanden enligt 2 § första stycket 2 läses av eller tas upp får uppgifterna endast avse förfluten tid.

Hemlig dataavläsning i fall som anges i första stycket får endast avse uppgifter i ett identifierbart informationssystem. Åtgärden får inte avse uppgifter i informationssystem som tillhör någon som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

Förbud mot hemlig dataavläsning

11 § Tillstånd till hemlig dataavläsning får inte avse uppgifter i ett informationssystem

1. som stadigvarande används i verksamhet som tystnadsplikt gäller för enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,
2. som stadigvarande används i verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller
3. som stadigvarande används av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, i verksamhet för bikt eller enskild själavård.

Tillträdestillstånd

12 § Vid hemlig dataavläsning får särskilt tillstånd meddelas den verkställande myndigheten att i hemlighet installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd får endast avse en plats där det finns särskild anledning att anta att informationssystemet finns. Om platsen är någon annan stadigvarande bostad än den misstänktes får tillstånd meddelas endast om det finns synnerlig anledning att anta att informationssystemet finns där.

Med den misstänkte enligt första stycket jämställs en person som avses i 7 § första stycket och en person som avses i 8 § första stycket 1.

Tillstånd enligt första stycket får inte avse

1. en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet som tystnadsplikt gäller för enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen,
2. en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen (2001:453), eller
3. en plats som stadigvarande används eller är särskilt avsedd att användas av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund, för bikt eller enskild själavård.

Tillståndsprövning m.m.

13 § Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagaren. En ansökan om en åtgärd i fall som anges i 8 § ska dock göras av Säkerhetspolisen eller Polismyndigheten.

I ett tillstånd till hemlig dataavläsning ska det anges

1. vilken tid tillståndet avser,
2. vilket informationssystem tillståndet avser,
3. vilken typ av uppgift enligt 2 § första stycket tillståndet avser,
4. i förekommande fall, den plats tillståndet gäller, och
5. vid åtgärd enligt 2 § första stycket 5 vem som är skäligen misstänkt för brottet.

Tiden för tillståndet får inte bestämmas längre än nödvändigt. När det gäller tid som infaller efter beslutet får tiden inte överstiga en månad från dagen för beslutet.

När tillståndet ska förenas med särskilt tillstånd enligt 12 §, ska det anges särskilt i beslutet.

I tillståndet ska också i övrigt anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.

14 § Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller möjligheterna att förhindra den brottsliga verksamheten att inhämta rättens tillstånd till hemlig dataavläsning, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut. Sådant tillstånd får dock inte avse hemlig dataavläsning enligt 2 § första stycket 5 eller hemlig dataavläsning i fall som anges i 8 §.

Om åklagaren har gett ett sådant tillstånd, ska han eller hon utan dröjsmål skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.

Om åklagarens beslut har verkställts innan rätten gjort en prövning som avses i andra stycket, ska rätten pröva om det funnits skäl för åtgärden. Om rätten finner att det saknats sådana skäl, får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

15 § När ansökan om hemlig dataavläsning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet ska den som gjort ansökan och det offentliga ombudet närvara.

För offentliga ombud i ärenden om hemlig dataavläsning gäller 27 kap. 26 och 27 §§, 28 § andra stycket samt 29 och 30 §§ rättegångsbalken.

På förfarandet enligt denna lag i övrigt tillämpas reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor, om inte annat anges i denna lag. Handläggningen ska ske skyndsamt.

16 § Beslut i frågor om hemlig dataavläsning får verkställas omedelbart.

Om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning, ska den som ansökt om åtgärden eller rätten omedelbart upphäva beslutet.

Genomförande av hemlig dataavläsning

Tillåtna tekniska metoder

17 § När tillstånd till hemlig dataavläsning har lämnats, får de tekniska hjälpmedel som behövs för avläsning och upptagning användas.

Om det är nödvändigt för att verkställighet ska kunna ske får den som ska verkställa åtgärden, när tillstånd har lämnats, bryta eller kringgå systemskydd och utnyttja tekniska sårbarheter. Den som ska verkställa åtgärden får då också, om det är nödvändigt, använda tekniska hjälpmedel i det informationssystem tillståndet avser.

Medverkan

18 § Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation får bistå den verkställande myndigheten i samband med verkställighet av hemlig dataavläsning.

Den som medverkar enligt första stycket har rätt till ersättning för kostnader som uppstår vid sådan medverkan. Ersättningen ska betalas av den verkställande myndigheten.

Teknikanpassning och otillåten tilläggsinformation

19 § Den teknik som används i samband med verkställighet ska anpassas efter det tillstånd som meddelats så att det inte är möjligt att läsa av eller ta upp någon annan typ av uppgift än sådan som tillståndet avser.

Om det, trots vad som anges i första stycket, kommer fram att någon annan typ av uppgift än sådan som tillståndet avser har lästs av eller tagits upp ska upptagningar av dessa uppgifter omedelbart förstöras och tillsynsmyndigheten underrättas.

Uppgifter som framkommit vid sådan avläsning eller upptagning som anges i andra stycket får inte användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

Aktsamhetskrav

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

Den som ansvarar för verkställighet av hemlig dataavläsning ska vidta nödvändiga och tillräckliga åtgärder för att informationssäkerheten utanför det informationssystem tillståndet avser inte åsidosätts, minskas eller skadas till följd av verkställigheten.

När verkställighet av hemlig dataavläsning avslutas ska den verkställande myndigheten vidta de åtgärder som behövs för att säkerheten i det informationssystem som tillståndet avser ska hålla åtminstone samma nivå som vid verkställighetens början.

Ett tekniskt hjälpmedel som har använts ska tas bort, avinstalleras eller annars göras obrukbart så snart det kan ske efter att tiden för tillståndet har gått ut eller tillståndet hävts.

Förbud avseende vissa uppgifter

Beslagsförbudet

21 § Om det vid genomförande av hemlig dataavläsning kommer fram att uppgifter som läses av är skyddade enligt 27 kap. 2 § första stycket rättegångsbalken ska avläsningen omedelbart avbrytas.

Upptagningar ska omedelbart förstöras i de delar som de omfattas av skyddet enligt första stycket.

Avlyssningsförbudet

22 § Hemlig dataavläsning enligt 2 § första stycket 1 får inte avse uppgifter i telefonsamtal eller andra meddelanden där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram. Om det under avläsningen kommer fram att det är fråga om sådana uppgifter, ska den omedelbart avbrytas.

Hemlig dataavläsning enligt 2 § första stycket 5 får inte avse uppgifter i samtal eller annat tal där någon som angetts i första stycket talar. Om det under avläsningen kommer fram att det är fråga om sådana uppgifter, ska den omedelbart avbrytas.

Upptagningar och uppteckningar ska omedelbart förstöras i de delar som de omfattas av förbud enligt första eller andra stycket.

Bestämmelser om överskottsinformation, granskning och underrättelse till enskild

Förundersökning

23 § När hemlig dataavläsning används eller har använts under förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 23 a och 24 §§ rättegångsbalken tillämpas för åtgärden. När hemlig dataavläsning används eller har använts enligt 2 § första stycket 5 ska dock i stället det som enligt de bestämmelserna gäller för hemlig rumsavlyssning tillämpas.

För underrättelse till enskild vid hemlig dataavläsning under förundersökning gäller det som anges i 27 kap. 31–33 §§ rättegångsbalken. Det som där anges om hemlig avlyssning av elektronisk kommunikation ska alltid tillämpas för hemlig dataavläsning. Det som anges om hemlig kameraövervakning ska tillämpas för hemlig dataavläsning enligt 2 § första stycket 4 och det som anges om hemlig rumsavlyssning ska tillämpas för hemlig dataavläsning enligt 2 §första stycket 5.

Förhindrande av vissa särskilt allvarliga brott

24 § När hemlig dataavläsning används eller har använts i fall som anges i 6 § ska det som gäller enligt 12 och 13 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott tillämpas för åtgärden.

För underrättelse till enskild vid hemlig dataavläsning i fall som anges i 6 § gäller det som anges i 16–18 §§ lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Det som där anges om hemlig avlyssning av elektronisk kommunikation ska alltid tillämpas för hemlig dataavläsning. Det som anges om hemlig kameraövervakning ska tillämpas för hemlig dataavläsning enligt 2 § första stycket 4.

Gemensam bestämmelse avseende 23 och 24 §§

25 § Vid tillämpning av 23 och 24 §§ ska begreppet informationssystem användas i stället för telefonnummer eller annan adress eller en

viss elektronisk kommunikationsutrustning när något av dessa begrepp används i de hänvisade bestämmelserna.

Särskild utlänningskontroll

26 § När hemlig dataavläsning används eller har använts i fall som anges i 8 § ska det som gäller enligt 21 a och 22 §§ lagen (1991:572) om särskild utlänningskontroll tillämpas för åtgärden.

Förebyggande, förhindrande och upptäckande av brottslig verksamhet

27 § När hemlig dataavläsning används eller har använts i fall som anges i 10 § ska det som gäller för inhämtning enligt 7–9 §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet tillämpas för åtgärden.

Behörig domstol

28 § Frågor om tillstånd till hemlig dataavläsning prövas, om förundersökning pågår, av domstol som föreskrivs i 19 kap. rättegångsbalken. Vid förundersökning om brott som anges i 27 kap. 2 § andra stycket 28 rättegångsbalken får sådana frågor också prövas av Stockholms tingsrätt.

Frågor om tillstånd till hemlig dataavläsning i fall som anges i 6–10 §§ prövas av Stockholms tingsrätt.

Underrättelse till Säkerhets- och integritetsskyddsnämnden

29 § När ett tillstånd till hemlig dataavläsning har lämnats ska rätten underrätta Säkerhets- och integritetsskyddsnämnden om beslutet.

Tystnadsplikt

30 § Den som i samband med verksamhet som är anmälningspliktig enligt 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation har fått del av eller tillgång till uppgift som hänför sig till angelägenhet som avser användning av hemlig dataavläsning får inte obehörigen föra vidare eller utnyttja det han eller hon fått del av eller tillgång till.

Bestämmelser om ansvar för den som bryter mot tystnadsplikten enligt första stycket finns i brottsbalken.

Övriga bestämmelser

31 § Den verkställande myndigheten fattar beslut om att utse den som enligt 20 § andra stycket får ansvara för verkställighet av hemlig dataavläsning.

Till ansvarig person för verkställighet av hemlig dataavläsning får endast utses den som har de särskilda kunskaper om informationssäkerhet som behövs och därtill den särskilda kompetens, utbildning och erfarenhet som är nödvändig samt i övrigt är särskilt lämpad föruppdraget.

Bilaga 2

Denna lag träder i kraft den 1 januari 2019 och gäller till utgången av 2023.

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

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

Nuvarande lydelse	*Föreslagen lydelse*
28 §	
Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § rättegångsbalken, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.	Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § rättegångsbalken *eller hemlig dataavläsning enligt 2 § första stycket 5 lagen (2019:000) om hemlig dataavläsning,* får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.
Om åklagaren har gett ett sådant tillstånd, ska han eller hon utan dröjsmål skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet. Om rätten finner att det inte finns skäl för åtgärden, ska den upphäva beslutet.	

Denna lag träder i kraft den 1 januari 2019.

Bilaga 2

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 2 kap. 1, 2 och 4 § ska ha följande lydelse,

dels att det ska införas fyra nya paragrafer, 4 kap. 28 c-f §§, och närmast före 4 kap. 28 c och e §§ nya rubriker av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
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 hemligövervakning av elektronisk kommunikation,	
7. tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation, 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	*11. hemlig dataavläsning*,
12. rättsmedicinsk undersökning av en avliden person.	12. överförande av frihetsberövade för förhör m.m., och
	13. 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.	
2 kap.	
1 §	
Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–6, 9, 10 och 12 ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–6, 9–*11 och 13* ska lämnas under de förutsättningar som gäller för en motsvarande åtgärd under en svensk förundersökning eller rättegång enligt

rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 7, 8 och 11 lämnas enligt de särskilda bestämmelserna i denna lag.	rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 7, 8 och *12* lämnas enligt de särskilda bestämmelserna i denna lag.

I 5 kap. 2 § finns bestämmelser om att den rättsliga hjälpen får förenas med villkor i vissa fall.

2 §

Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 7 och 11 får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5, 6, 8–10 och 12 får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan och beslag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–4, 7 *och 12* får lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag. Rättslig hjälp som avses i 1 kap. 2 § första stycket 5, 6, 8–*11 och 13* får endast lämnas om den gärning som ansökan avser motsvarar ett brott enligt svensk lag (dubbel straffbarhet), om inte annat följer av 4 kap. 20 § beträffande husrannsakan och beslag.

4 §

En ansökan om rättslig hjälp i Sverige enligt denna lag bör innehålla

– uppgift om den utländska domstol eller myndighet som handlägger ärendet,

– en beskrivning av det rättsliga förfarande som pågår,

– uppgift om den aktuella gärningen med tid och plats för denna, samt de bestämmelser som är tillämpliga i den ansökande staten,

– uppgift om vilken åtgärd som begärs och, i förekommande fall, i vilken egenskap en person ska höras,

– namn på och adress till de personer som är aktuella i ärendet.

I 4 kap. 8, 11, 14, 24 a, 25, 25 b, 25 c, 26 a, 29 och 29 a §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.	I 4 kap. 8, 11, 14, 24 a, 25, 25 b, 25 c, 26 a, *28 c*, 29 och 29 a §§ finns särskilda bestämmelser om vad en ansökan ytterligare ska innehålla vid vissa slag av åtgärder.

Om ärendet är brådskande eller om verkställighet önskas inom viss tidsfrist, ska detta anges och motiveras.

En ansökan om rättslig hjälp ska göras skriftligen genom post, bud eller telefax. Den får även, efter överenskommelse i det enskilda fallet, översändas på annat sätt.

4 kap.

Hemlig dataavläsning

Hemlig dataavläsning avseende någon i Sverige

28 c §

En ansökan om hemlig dataavläsning avseende 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 genom-föras. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd till åtgärden eller, när det får ske enligt 14 § lagen (2019:000) om hemlig dataavläsning, själv besluta om åtgärden.

Upptagningar och uppteckningar behöver inte granskas enligt 23 § första stycket lagen (2019:000) om hemlig dataavläsning.

Om åklagaren har fattat beslut enligt första stycket, ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om hemlig dataavläsning. 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 23 § första stycket lagen (2019:000) om hemlig data-avläsning.

I fråga om underrättelse till en enskild enligt 23 § andra stycket lagen (2019:000) om hemlig dataavläsning ska bestämmelserna i 4 kap. 25 § tredje stycket denna lag tillämpas.

28 d §

Om en ansökan avser hemlig dataavläsning enligt 2 § 1–3 lagen (2019:000) om hemlig

dataavläsning får rättens beslut enligt 28 c § att tillåta hemlig dataavläsning verkställas genom omedelbar överföring med tillämpning av 25 a §.

Tekniskt bistånd i form av omedelbar överföring av meddelanden eller uppgifter om meddelanden får lämnas i Sverige enligt de förutsättningar som gäller för tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation enligt 25 b § andra, tredje och femte styckena. Ansökan ska prövas av åklagare. För beslutet om tekniskt bistånd tillämpas 1 §, 13 § andra stycket 1–3 och tredje stycket samt 16 § andra stycket lagen (2019:000) om hemlig dataavläsning.

Om ansökan avser tillstånd till gränsöverskridande hemlig dataavläsning enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning tillämpas det som gäller för hemlig avlyssning av elektronisk kommunikation i 26 a § första och andra styckena och 26 b §. De förutsättningar som gäller enligt 1–5 och 11–13 §§ lagen om hemlig dataavläsning tillämpas vid tillståndsprövningen. Rätten ska även tillämpa motsvarande förfarande som anges i 15 § den lagen. Tingsrättens beslut får inte överklagas.

Hemlig dataavläsning avseende någon i utlandet

28 e §

Om hemlig dataavläsning ska äga rum avseende någon som befinner sig i en annan stat och den andra staten kräver att ansökan först ska prövas av domstol i Sverige, får rätten på begäran av svensk åklagare besluta att tillåta avläsningen.

Bestämmelsen om underrättelse till enskild enligt 23 § andra stycket

lagen (2019:000) om hemlig dataavläsning ska tillämpas endast när avläsning eller upptagning sker i Sverige.

När det är fråga om hemlig dataavläsning enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning tillämpas det som anges i 26 § om tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation också för hemlig dataavläsning.

28 f §

Har ett tillstånd till hemlig dataavläsning enligt 2 § första stycket 1–3 i en brottsutredning beslutats i Sverige och befinner sig den person som tillståndet avser i en annan stat som är medlem i Europeiska unionen eller i Island eller Norge samt avläsning eller upptagning kan ske utan hjälp från den andra staten tillämpas det som anges i 26 c § om hemlig avlyssning av elektronisk kommunikation också för hemlig dataavläsning.

Denna lag träder i kraft den 1 januari 2019.

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

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400) att 18 kap. 19 § och 44 kap. 5 § ska ha följande lydelse.

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 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 (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	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, hemlig rumsavlyssning eller *hemlig dataavläsning* på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av uppgifter enligt lagen (2012:278) 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.	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, hemlig kameraövervakning, *hemlig rumsavlyssning eller hemlig dataavläsning* på grund av beslut av domstol eller åklagare.
Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker	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.	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.

44 kap.

5 §

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. förordnande med stöd av 7 § lagen (1999:988) om förhör m.m. hos kommissionen för granskning av de svenska säkerhetstjänsternas författningsskyddande verksamhet,
2. 7 kap. 1 § 1 lagen (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap,
3. 4 kap. 16 § försäkringsrörelselagen (2010:2043), och
4. 5 kap. 15 § lagen (1998:293) om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige.

5. 30 § första stycket lagen (2019:000) om hemlig dataavläsning.

Denna lag träder i kraft den 1 januari 2019.

Förslag till lag om ändring i lagen (2017:000) om europeisk utredningsorder

Härigenom föreskrivs i fråga om den föreslagna lagen (2017:000) om europeisk utredningsorder

dels att 1 kap. 4 §, 2 kap. 5 § och 3 kap. 10 § ska ha följande lydelse,

dels att det ska införas två nya paragrafer, 2 kap. 19 a § och 3 kap. 37 a §, samt närmast före dessa nya rubriker av följande lydelse.

Lydelse enligt prop. 2016/17:218	*Föreslagen lydelse*
1 kap.	
4 §	
En utredningsåtgärd enligt denna lag ska avse eller motsvara	
1. förhör under förundersökning,	
2. bevisupptagning vid domstol,	
3. förhör genom ljudöverföring eller ljud- och bildöverföring,	
4. beslag, kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken	
eller en åtgärd enligt 27 kap. 15 § samma balk,	
5. husrannsakan och andra åtgärder enligt 28 kap. rättegångsbalken,	
6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning,	6. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *och hemlig dataavläsning*,
7. tillfälligt överförande av en frihetsberövad person,	
8. rättsmedicinsk undersökning av en avliden person,	
9. kontrollerad leverans,	
10. bistånd i en brottsutredning med användning av en skyddsidentitet,	
11. inhämtande av bevis som finns hos en myndighet, eller	
12. andra åtgärder som inte innebär användning av tvångsmedel	
eller någon annan tvångsåtgärd.	
2 kap.	
5 §	
Innan åklagaren utfärdar en utredningsorder ska åklagaren ansöka om domstolens tillstånd till att utfärda utredningsordern, om utredningsåtgärden avser	
1. kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken,	
2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning eller hemlig rumsavlyssning, eller	2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *eller hemlig dataavläsning*, eller
3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m.	
I avvaktan på domstolens beslut	I avvaktan på domstolens beslut

får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken utfärda en utredningsorder för kvarhållande av försändelse, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation eller hemlig kameraövervakning. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.	får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ *eller 14 § lagen (2019:000) om hemlig dataavläsning* rättegångsbalken utfärda en utredningsorder för kvarhållande av försändelse, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning *eller hemlig dataavläsning*. Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.

Innan en utredningsorder för husrannsakan, kroppsvisitation eller kroppsbesiktning utfärdas, får åklagaren enligt 28 kap. 4 § första stycket och 13 § första stycket rättegångsbalken ansöka om domstolens tillstånd till att utfärda utredningsordern.

För domstolens handläggning gäller vad som är föreskrivet i rättegångsbalken eller annan författning för den åtgärd som avses.

Hemlig dataavläsning

19 a §

När en utredningsorder för hemlig dataavläsning har utfärdats, ska 16 § andra stycket, 22 § och 23 § första stycket lagen (2019:000) om hemlig dataavläsning tillämpas.

Om en utredningsorder enligt första stycket avser hemlig dataavläsning enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning gäller det som anges i 17 § om hemlig avlyssning av elektronisk kommunikation också för hemlig dataavläsning.

I de fall upptagningen sker i Sverige ska 23 § andra stycket lagen (2019:000) om hemlig dataavläsning tillämpas.

3 kap.

10 §

I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken, besluta att er-	I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken *eller 11 § lagen*

känna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation eller hemlig kameraövervakning.	*(2019:000) om hemlig dataavläsning,* besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning *eller hemlig dataavläsning.*
	Hemlig dataavläsning
	37 a § *Vid verkställighet av en utredningsorder för hemlig dataavläsning behöver upptagningar eller uppteckningar inte granskas enligt 23 § första stycket lagen (2019:000) om hemlig dataavläsning. Upptagningar och uppteckningar som finns kvar i Sverige efter det att ärendet har avslutats hos åklagaren och bevismaterialet har överlämnats med stöd av 38 eller 40 §, får bevaras endast om detta är tillåtet enligt 23 § första stycket lagen (2019:000) om hemlig dataavläsning.* *I fråga om underrättelse till enskild gäller 36 § andra stycket med tillämpning av 23 § andra stycket lagen (2019:000) om hemlig dataavläsning.* *När en utredningsorder för hemlig dataavläsning avser en åtgärd enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning tillämpas vid verkställighet vad som föreskrivs om hemlig avlyssning av elektronisk kommunikation i 34 §.* *Vid verkställighet av hemlig dataavläsning enligt 34 § 1 får upptagning eller uppteckning inte göras i Sverige och 23 § andra stycket lagen (2019:000) om hemlig dataavläsning ska inte tillämpas. Om åklagaren med stöd av 10 § har meddelat en verkställ-*

barhetsförklaring, får verkställighet ske först efter det att domstolen har fastställt förklaringen. Vid verkställighet enligt 34 § 2 tillämpas första och andra styckena.

4 kap.

15 a §

Det som anges om hemlig avlyssning av elektronisk kommunikation i 12–15 §§ tillämpas även för hemlig dataavläsning enligt 2 § första stycket 1–3 lagen (2019:000) om hemlig dataavläsning.

Denna lag träder i kraft den 1 januari 2019.

Förteckning över remissinstanserna

Remissyttranden har lämnats av följande instanser. Riksdagens ombudsmän (JO), Svea hovrätt, Stockholms tingsrätt, Göteborgs tingsrätt, Malmö tingsrätt, Luleå tingsrätt, Justitiekanslern, Domstolsverket, Domarnämnden, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Brottsförebyggande rådet, Datainspektionen, Försvarsmakten, Försvarets radioanstalt, Statens inspektion för försvarsunderrättelseverksamheten, Försvarsunderrättelsedomstolen, Migrationsverket, Tullverket, Skatteverket, Statskontoret, Riksarkivet, Post- och telestyrelsen, Myndigheten för samhällsskydd och beredskap, Lunds universitet (juridiska fakulteten), Stockholms universitet (juridiska fakulteten), Uppsala universitet (juridiska fakulteten), Kungl. Tekniska högskolan, Diskrimineringsombudsmannen, Sveriges advokatsamfund, Civil Rights Defenders, Dataskydd.net Sverige, Föreningen för Digitala fri- och rättigheter, IT&Telekomföretagen, Stiftelsen för Internetinfrastruktur, Svenska stadsnätsföreningen, Sveriges läkarförbund, Svenska Journalistförbundet (SJF), Svenska kyrkan, Sveriges kristna råd, Com Hem AB, Google Sweden AB, Hi3G Access AB och Telia Sverige AB.

Yttrande har också inkommit från Privacy International.

Följande instanser har inbjudits att yttra sig men har avstått eller inte hörts av. Luleå tekniska universitet, Amnesty International, Centrum för rättvisa, Dataspelsbranschen, ECPAT Sverige, IFPI Sverige, Institutet för Juridik och Internet, Polisförbundet, Rättighetsalliansen, Svenska avdelningen av Internationella Juristkommissionen, Sveriges domareförbund, Sveriges psykologförbund, Sveriges muslimska råd, Judiska centralrådet i Sverige, Apple Aktiebolag, Bahnhof AB, Facebook Sweden AB, IP-Only AB, Net at Once Sweden AB, Samsung Electronics Nordic AB, Tele2 Sverige AB, Telenor Sverige AB och SNUS Swedish network users society.