Hemlig dataavläsning

– ett viktigt verktyg i kampen mot allvarlig brottslighet

Delbetänkande av Utredningen om hemlig dataavläsning

Stockholm 2017

STATENS OFFENTLIGA UTREDNINGAR

SOU 2017:89

SOU och Ds kan köpas från Wolters Kluwers kundservice.
Beställningsadress: Wolters Kluwers kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@wolterskluwer.se
Webbplats: wolterskluwer.se/offentligapublikationer

För remissutsändningar av SOU och Ds svarar Wolters Kluwer Sverige AB
på uppdrag av Regeringskansliets förvaltningsavdelning.
Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
En kort handledning för dem som ska svara på remiss.
Häftet är gratis och kan laddas ner som pdf från eller beställas på regeringen.se/remisser

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2017

ISBN 978-91-38-24702-0
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 12 maj 2016 att tillkalla en särskild utredare med uppdrag att utreda om svenska brottsbekämpande myndigheter ska ges möjlighet att använda hemlig dataavläsning. Samma dag förordnades Petra Lundh, lagman vid Södertörns tingsrätt, att vara särskild utredare. Den 8 juni 2016 förordnades följande personer som experter att biträda utredaren: seniora strategiska rådgivaren Kurt Alavaara och chefsjuristen Per Lagerud vid Säkerhetspolisen, tidigare enhetschefen vid Säkerhets- och integritetsskyddsnämnden numera rådmannen Anna Backman vid Attunda tingsrätt, inspektören och gruppchefen Johan Dahl och it-teknikern Susanne Hedberg vid Nationella operativa avdelningen (NOA) inom Polismyndigheten, kanslirådet och tillförordnade enhetschefen Mikael Kullberg vid Justitiedepartementet, kammaråklagaren Mats Ljungqvist vid Riksenheten för säkerhetsmål och verksjuristen Lisbeth Tjärnkvist vid Tullverket. Den 22 juni 2016 förordnades ytterligare två experter; vice överåklagaren Bengt Lindholm vid Ekobrottsmyndigheten och generalsekreteraren Anne Ramberg i Sveriges advokatsamfund. Den 16 februari 2017 förordnades kammaråklagaren Hans Harding vid Åklagarmyndighetens Utvecklingscentrum Malmö som expert. Den 30 mars 2017 entledigades Mikael Kullberg från uppdraget som expert. Samma dag förordnades kanslirådet och tillförordnade enhetschefen Frida Göranson vid Justitiedepartementet som expert.

Som sekreterare anställdes från och med den 13 juni 2016 hovrättsassessorn David Caldevik.

Utredningen har antagit namnet Utredningen om hemlig dataavläsning. Utredningens experter har, i den mån inte annat framgår av de särskilda yttrandena, i allt väsentligt ställt sig bakom utred-

ningens överväganden och förslag. Betänkandet har därför skrivits i vi-form.

Härmed överlämnas delbetänkandet *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet* (SOU 2017:89).

Utredningen fortsätter nu sitt arbete i enlighet med tilläggsdirektiv som beslutades den 19 oktober 2017 om att analysera och ta ställning till om tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan knytas enbart till den misstänkte, i stället för till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning.

Stockholm i november 2017

Petra Lundh

/David Caldevik

Innehåll

Sammanfattning

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 effektiv metod 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 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. 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 dataavläsning 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 utrust-

ning, 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 dataavläsning 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 informationssäkerhets-, 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 rumsavlyssningsuppgifter. I underrättelsefallen ska motsvarande det som gäller för granskning, bevarande och förstörande av upptag-

ningar 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 preventivlagsfallen. De särskilda regler som gäller för hemlig kameraövervakning och hemlig rumsavlyssning ska tillämpas även för hemlig dataavläsning avseende kameraövervakningsuppgifter och rumsavlyssningsuppgifter.

Tillsynsfrågor

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.

1 Författningsförslag

1.1 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, psyko-

terapeuter 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 tvångs-

medel 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 2–8 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 för uppdraget.

Denna lag träder i kraft den 1 januari 2019 och gäller till utgången av 2023.

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

Härigenom föreskrivs 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.

1.3 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 hemlig övervakning 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 rättegångsbalken eller annan lag eller författning och enligt de särskilda bestämmelserna i denna lag.	Rättslig hjälp som avses i 1 kap. 2 § första stycket 1–6, 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.	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 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 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 dataavläsning.

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 med-

delanden 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.

1.4 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,	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.	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 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.	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.

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.

1.5 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

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.

2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *eller hemlig dataavläsning*, eller

I avvaktan på domstolens beslut 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 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 11 § lagen (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 verkställbarhetsför-

klaring, 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.

1.6 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Härigenom föreskrivs att 3 § offentlighets- och sekretessförordningen (2009:641) ska ha följande lydelse

Nuvarande lydelse

3 § Följande myndigheter ska i den utsträckning som framgår nedan inte tillämpa 5 kap. 2 § andra stycket offentlighets- och sekretesslagen (2009:400).

Myndigheter	Register
allmänna domstolar	diarier över ärenden om kvarhållande av försändelser på befordringsanstalt och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning
Polismyndigheten	diarier över ärenden om kvarhållande av försändelse på befordringsanstalt och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning
Säkerhetspolisen	diarier över underrättelser inom den särskilda polisverksamheten för att hindra och uppdaga brott mot rikets säkerhet m.m. och diarier över ärenden om kvarhållande av försändelse på befordringsanstalt och om hemlig avlyss-

	ning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning
Tullverket	diarier över ärenden om kvarhållande av försändelse på befordringsanstalt och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning
åklagarmyndigheter	diarier över ärenden om kvarhållande av försändelse på befordringsanstalt och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning samt diarier över förundersökningar som rör brott mot rikets säkerhet

Föreslagen lydelse

3 § Följande myndigheter ska i den utsträckning som framgår nedan inte tillämpa 5 kap. 2 § andra stycket offentlighets- och sekretesslagen (2009:400).

Myndigheter	Register
allmänna domstolar	diarier över ärenden om kvarhållande av försändelser på befordringsanstalt och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraöver-

	vakning, hemlig rumsavlyssning *och hemlig dataavläsning*
Polismyndigheten	diarier över ärenden om kvarhållande av försändelse på befordringsanstalt och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *och hemlig dataavläsning*
Säkerhetspolisen	diarier över underrättelser inom den särskilda polisverksamheten för att hindra och uppdaga brott mot rikets säkerhet m.m. och diarier över ärenden om kvarhållande av försändelse på befordringsanstalt och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *samt hemlig dataavläsning*
Tullverket	diarier över ärenden om kvarhållande av försändelse på befordringsanstalt och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *samt hemlig dataavläsning*

åklagarmyndigheter	diarier över ärenden om kvarhållande av försändelse på befordringsanstalt och om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning *och hemlig dataavläsning* samt diarier över förundersökningar som rör brott mot rikets säkerhet

---

Denna förordning träder i kraft den 1 januari 2019.

2 Utredningens uppdrag och arbete

2.1 Utredningsuppdraget

Regeringen beslutade den 12 maj 2016 att ge en särskild utredare i uppdrag att utreda om svenska brottsbekämpande myndigheter ska ges möjlighet att använda arbetsmetoden hemlig dataavläsning. Direktiven finns bifogade som bilaga 1.

Enligt utredningsdirektiven ska utredaren undersöka om bestämmelser om hemlig dataavläsning bör införas i svensk rätt för att säkerställa att de brottsbekämpande myndigheterna kan upprätthålla sin förmåga att bekämpa brott. Utredaren ska enligt direktiven bland annat

- ta reda på vilket behov de brottsbekämpande myndigheterna har av att hemligt i realtid bereda sig tillgång till information i datorer och andra tekniska utrustningar för att effektivt kunna fullgöra sin uppgift, bl.a. i förhållande till övriga metoder för att bekämpa brott inklusive övriga (hemliga) tvångsmedel, och vid analysen särredovisa Åklagarmyndighetens, Ekobrottsmyndighetens, Polismyndighetens, Säkerhetspolisens och Tullverkets behov,
- undersöka vilka möjligheter som modern teknik kan ge de brottsbekämpande myndigheterna att i realtid i hemlighet läsa information i datorer och andra tekniska utrustningar och vilka begränsningar som följer av tekniken och av möjligheten att använda motmedel mot en sådan åtgärd,
- kartlägga och med beaktande av eventuell sekretess beskriva hur en sådan metod kan förväntas verkställas och avbrytas eller avslutas inklusive de operativa svårigheterna med detta,

- analysera i vilken utsträckning det kan bidra till en effektiv brottsbekämpning att ge brottsbekämpande myndigheter befogenhet att i realtid i hemlighet läsa information i datorer och andra tekniska utrustningar,
- undersöka vilket integritetsintrång detta skulle medföra för enskilda och beskriva vilka avgränsningar som behövs,
- utifrån en avvägning mellan effektivitets- och integritetsskäl ta ställning till om de brottsbekämpande myndigheterna bör ges möjlighet att använda hemlig dataavläsning för att bekämpa terroristbrottslighet och andra allvarliga brott, som i dag ger möjlighet till hemlig avlyssning av elektronisk kommunikation,
- avgöra de närmare förutsättningarna för en sådan användning bl.a. i fråga om syfte, tillämpningsområde och rättssäkerhetsgarantier i enlighet med Europakonventionen och den praxis som Europeiska domstolen för de mänskliga rättigheterna har utvecklat,
- ta ställning till i vilken utsträckning åtgärden ska kunna användas i det internationella rättsliga samarbetet, och
- lämna förslag till författningsändringar eller andra förändringar oavsett vad analysen föranleder.

I uppdraget ingår också att redovisa gällande rätt och eventuellt pågående arbete i övriga nordiska länder samt de övriga länder som bedöms vara relevanta för utredningsuppdraget och i övrigt göra de internationella jämförelser som utredaren bedömer befogade. Vidare ska utredaren hålla sig informerad om och beakta sådant arbete inom Regeringskansliet samt inom EU och andra internationella forum som är relevant för uppdraget. Utredaren ska särskilt uppmärksamma det pågående arbetet inom ramen för utredningen om moderna regler om beslag och husrannsakan (dir. 2016:20) och samordna sina bedömningar med den utredningen i den utsträckning det behövs.

2.2 Utredningsarbetet

Uppdraget har inrymt överväganden inom ett mycket komplext område, både juridiskt och tekniskt. En stor del av utredningstiden har gått åt till att förstå vad hemlig dataavläsning skulle kunna vara

och att klarlägga de behov som föreligger i de brottsbekämpande myndigheternas verksamhet liksom att avgöra i vilken utsträckning hemlig dataavläsning skulle kunna möta behoven.

Utredningen har haft flera sammanträden med de förordnade experterna. Därutöver har utredningen haft separata möten med enskilda experter i syfte att förstå enskilda frågor, huvudsakligen av teknisk karaktär. Utredningen har vidare genomfört studiebesök hos Polismyndigheten, Tullverket och Säkerhetspolisen. Representanter för de brottsbekämpande myndigheterna har också i olika omgångar beretts möjlighet att komma in med behovsbeskrivningar.

Vidare har utredningen besökt brottsbekämpande myndigheter (och säkerhetstjänster) i Norge, Nederländerna, Storbritannien och Tyskland för att få en uppfattning om hur åtgärder motsvarande hemlig dataavläsning tillämpas där. Därtill har utredningen, utan att besök gjorts, haft kontakter med personer verksamma vid brottsbekämpande myndigheter i Danmark och Finland.

Utredningen har under utredningsarbetet också haft löpande kontakter och samrått med Beslagsutredningen, där den särskilde utredaren också är förordnad som expert. Därtill har utredningen genomfört ett möte med den utredningen och representanter för Justitiedepartementet för att klargöra vissa gränsdragningsfrågor mellan utredningarna. Visst samråd har också skett med Utredningen om datalagring och EU-rätten. Vidare har utredningen träffat representanter för Post- och telestyrelsen samt IT&Telekomföretagen och Comhem, Telenor och Telia.

Utredningen har därutöver löpande tagit del av synpunkter från enskilda personer och organisationer, särskilt från företrädare för den ideella föreningen Dataskydd.net och från Journalistförbundet.

2.3 Några avgränsningar

I utredningsdirektiven har, som utgångspunkt för en analys, hemlig dataavläsning definierats som ”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 används för kommunikation och därigenom få besked om hur utrustningen används i realtid och vilken information som finns i

den". Metoden kan enligt direktiven verkställas t.ex. genom att hårdvara eller programvara placeras i en användares tekniska utrustning.

Enligt den angivna definitionen skulle hemlig dataavläsning kunna användas för att genomföra en husrannsakan eller beslag av uppgifter i datormiljö på distans. Detta synsätt förutsätter bland annat dels att uppgifter kan tas i beslag (jfr rättsfallet NJA 2015 s. 631), dels att så kan ske utan att den dator eller annan tekniska utrustning som innehåller uppgifterna finns i beslag. Dessa frågor är inte tydligt reglerade i lag i dag. Mot bakgrund av det anförda överlappar vårt uppdrag i den delen Beslagsutredningens (Ju 2016:08) uppdrag, i vilket bl.a. ingår att utreda förutsättningar för att genomföra husrannsakan på distans. Vid samråd mellan utredningarna har det konstaterats att det visserligen kan tänkas att teknik för verkställighet av olika åtgärder kan vara densamma eller liknande. Syftet med de åtgärder utredningarna ska överväga ser dock olika ut. Hemlig dataavläsning ska utredas som ett potentiellt nytt hemligt tvångsmedel, som kan genomföras löpande och i realtid, medan Beslagsutredningens uppdrag består i att utreda bl.a. förutsättningarna för att genomföra husrannsakan i it-miljö i stället för i fysisk miljö. Den skillnad som finns mellan uppdragens syften utgör en tillräcklig avgränsning. Vårt betänkande behandlar därför inte i det följande frågor om husrannsakan i it-miljö eller andra åtgärder som sker i öppenhet.

Det har under arbetets gång också framkommit vissa terminologiska anmärkningar avseende direktivens definition. Dessa bör redovisas redan här för att sedan särskilt belysas under respektive delfråga där de aktualiseras.

I direktivets definition används uttrycket *realtid* för att beskriva förhållandet mellan den tidpunkt då den avlästa utrustningen används och den tidpunkt då den brottsbekämpande myndigheten kan läsa av informationen. I Nationalencyklopedin anges betydelsen av ordet realtid som "det faktiska tidsförloppet då en process pågår"[1]. Att den brottsbekämpande myndigheten, som anförs i direktiven, ska kunna "få besked om hur utrustningen används i realtid" får anses leda tanken till att informationen överförs helt utan eller med endast måttlig fördröjning. Det har från utredningens tekniska experter framhållits att det vid all verkställighet av hemliga tvångsmedel sker

[1] Nationalencyklopedin, realtid. www.ne.se/uppslagsverk/encyklopedi/lång/realtid (hämtad 2016-12-05).

viss bearbetning av den information som erhålls, t.ex. för att göra den läs- eller hörbar och förståelig. Denna bearbetning leder till viss fördröjning från att den faktiska processen pågår till dess att den kan uppfattas av de brottsbekämpande myndigheterna. Samma sak skulle enligt experterna gälla för hemlig dataavläsning, alldeles oavsett vilken teknik som används för verkställighet. Det bör anmärkas att utredningens tekniska experter har förklarat att bearbetningen typiskt sett bör ta mycket kort tid men att det i vissa situationer kan ta betydligt längre tid än vad som i dagligt tal kan anses rymmas inom realtidsbegreppet. Även om detta begrepp således inte är helt optimalt har vi inte funnit ett bättre uttryckssätt för det som avses. Utredningen har därför utgått från att realtid i sammanhanget inrymmer hela tiden från det faktiska tidsförloppet då processen pågår (dvs. då en misstänkt använder sin kommunikationsutrustning) till dess att de brottsbekämpande myndigheterna kan ta del av användningen (dvs. när bearbetning av informationen skett), oavsett hur stor fördröjningen är.

Vidare ställs i direktivens definition krav på att den utrustning som ska kunna avläsas genom hemlig dataavläsning *används för kommunikation*. Direktivens ordalydelse ”används för” begränsar enligt vår mening utrymmet för analysen som ska göras lite för mycket. Även utrustning som inte direkt används för kommunikation, t.ex. en dator som inte är ansluten till ett nätverk, kan vara av intresse. Analysen bör därför inte bara inrymma utrustning som används för kommunikation utan också sådan som *kan användas* för kommunikation.

I direktivens definition anges också att de brottsbekämpande myndigheterna ska kunna ta del av ”information som finns i utrustningen”. Det finns en hel del uppgifter som med dagens teknik är möjlig att ta del av genom informationsbärande utrustning men som egentligen lagras någon annanstans. Exempelvis kan uppgifter lagras i molntjänster men tillgängliggöras med en app i en mobiltelefon eller ett program i en dator. Sådan lagring blir allt vanligare. Vi har i sammanhanget inte gjort någon åtskillnad beroende på var uppgifter lagras utan har ansett att det nämnda uttryckssättet innefattar både uppgifter som lagras i utrustningen och information som lagras på annan plats.

Sammanfattningsvis kan således sägas att den definition av hemlig dataavläsning som vi lagt till grund för vår analys lyder enligt följande.

> 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.

2.4 Betänkandets disposition

Våra författningsförslag har redan presenterats i kapitel 1. Efter det nu aktuella kapitlet följer kapitel 3, som innehåller en redovisning gällande rätt och som främst tar sikte på andra hemliga tvångsmedel. Därefter ges en introduktion till hemlig dataavläsning i kapitel 4. I det därpå följande kapitel 5 redogörs för hur frågor om hemlig dataavläsning har reglerats i de nordiska länderna samt, översiktligt, något om hur motsvarande åtgärder används i några andra länder. Därefter följer kapitel 6 som innehåller för utredningen relevanta uppgifter om teknikutvecklingen. I kapitel 7 beskrivs brottsutvecklingen under de senaste åren. Kapitel 8 innehåller uppgifter som kommit in till utredningen från de brottsbekämpande myndigheterna, vilkas samlade behovsbeskrivningar också redovisas separat i sin helhet i bilaga 2. I kapitel 9 redovisas vår grundläggande analys av behovet av samt effektiviteten och integritetsriskerna med hemlig dataavläsning. Där redovisas också våra inledande avvägningar om hemlig dataavläsning. I kapitel 10 och 11 finns sedan våra allmänna överväganden bakom våra författningsförslag om hemlig dataavläsning och de ändringar i andra författningar som dessa medför. I kapitel 12 redovisas vår konsekvensutredning, vilken kompletterar den analys som gjorts i kapitel 9. Betänkandets sista kapitel, kapitel 13, innehåller författningskommentaren. Två särskilda yttranden har upprättats av experter. Dessa redovisas i anslutning till det sista kapitlet.

3 Gällande rätt

3.1 De brottsbekämpande myndigheternas uppgifter

Till polisens uppgifter hör bl.a. att förebygga brott och att bedriva spaning och utredning i fråga om brott som hör under allmänt åtal. Polisen (Polismyndigheten och Säkerhetspolisen) har således en brottsbekämpande funktion. Även Åklagarmyndigheten, Ekobrottsmyndigheten, Tullverket, Kustbevakningen, Skatteverket och Försvarsmakten (militärpolisen) är brottsbekämpande myndigheter.

Förfarandet vid den utredning som föregår ett beslut om åtal, förundersökningen, regleras i rättegångsbalken och i förundersökningskungörelsen (1947:948). Förundersökning ska, enligt 23 kap. 1 § rättegångsbalken, inledas så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats. Beslut att inleda förundersökning fattas oftast av polis eller av åklagare. Om förundersökning har inletts av Polismyndigheten eller Säkerhetspolisen och saken inte är av enkel beskaffenhet, ska ledningen av förundersökningen enligt 23 kap. 2 § rättegångsbalken övertas av åklagare så snart någon är skäligen misstänkt för brottet eller om det finns särskilda skäl. Så är fallet bl.a. om det blir aktuellt att använda sig av hemliga tvångsmedel. Förundersökningen har enligt 23 kap. 2 § rättegångsbalken huvudsakligen två syften. Det ena är att utröna om brott föreligger, vem som skäligen kan misstänkas för brottet och att skaffa tillräckligt material för bedömning av frågan om åtal ska väckas. Det andra syftet är att bereda målet så att bevisningen kan läggas fram i ett sammanhang vid en huvudförhandling i domstol.

Polisen bedriver också underrättelseverksamhet. Även vissa andra myndigheter, såsom Ekobrottsmyndigheten och Tullverket, bedriver sådan verksamhet. Denna verksamhet är i huvudsak inriktad på att avslöja om en viss, inte närmare specificerad brottslighet har ägt rum,

pågår eller kan antas komma att begås. Ett övergripande mål med underrättelseverksamheten är att förse de brottsutredande myndigheterna med kunskap som kan omsättas i operativ verksamhet. I underrättelseverksamheten samlar myndigheterna sålunda in, bearbetar och analyserar uppgifter som senare kan ha betydelse för att utreda, förebygga och förhindra brott. Det framtagna underrättelsematerialet kan också läggas till grund för ett beslut om att inleda en förundersökning.

Säkerhetspolisens uppdrag kan i huvudsak delas in i fem områden: kontraspionage, kontraterrorism, författningsskydd, säkerhetsskydd och personskydd. Säkerhetspolisen arbetar också 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.

Eftersom Säkerhetspolisens verksamhet primärt syftar till att förebygga och inte att utreda brott kan Säkerhetspolisen som regel inte bedriva verksamheten 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.

3.2 Grundläggande regler till skydd för den personliga integriteten

3.2.1 Regeringsformen

Grundläggande bestämmelser som har betydelse för det allmännas ansvar att skydda enskildas privatliv och integritet finns i bl.a. regeringsformen. Av målsättningsstadgandet i 1 kap. 2 § regeringsformen framgår att den offentliga makten ska 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.

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. Därtill gäller enligt paragrafens andra stycke ett skydd 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).

3.2.2 Europakonventionen

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

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 omfattar skydd mot en mängd åtgärder. Med korrespondens avses olika former för att överföra meddelanden mellan individer. Överföring av meddelanden med hjälp av telefon, telefax, radio och datorer omfattas av konventionens skydd för korrespondens (se Danelius, *Mänskliga rättigheter i europeisk praxis*, 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 uppfyller rimliga anspråk på rättssäkerhet, såsom att skydda mot godtycke, vara tillgänglig för allmänheten och 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 (Danelius s. 369 f.).

Frågan om förutsebarhet när det gäller dolda spaningsåtgärder eller hemliga tvångsmedel har vid ett flertal tillfällen prövats av Europadomstolen, som förklarat att innebörden av kravet på förutsebarhet inte innebär att en person bör kunna veta på förhand 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).

I sin rättspraxis på området har Europadomstolen utvecklat en minimistandard beträffande vilka krav som bör ställas på lagstiftningen om dolda spaningsåtgärder eller hemliga tvångsmedel till undvikande av missbruk.[1] Enligt denna bör i den nationella lagstiftningen anges följande.

- 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.

[1] Europadomstolens dom den 4 december 2015 i målet Roman Zakharov mot Ryssland punkt 231 och där angivna rättsfall. Det bör noteras att minimistandarden tar sikte främst på mer ingripande tvångsmedelsanvändning, såsom telefonavlyssning.

– De omständigheter under vilka inspelningar kan eller måste raderas ska anges.

I Europadomstolens dom den 2 september 2010 i målet Uzun mot Tyskland, som gällde frågan om brott mot artikel 8 på grund av övervakning via GPS av förflyttningar på offentliga platser, uttalade domstolen att de relativt strikta krav som minimistandarden ställer har utarbetats i mål om telefonavlyssning. Domstolen fann att dessa krav inte var tillämpliga i målet eftersom övervakning av en persons rörelser med hjälp av GPS-utrustning, i jämförelse med telefonavlyssning, utgjorde ett mindre intrång i dennes privatliv. Domstolen uttalade att vid sådana intrång ska i stället mer allmänna principer för ett adekvat skydd mot missbruk av artikel 8 tillämpas. En helhetsbedömning ska därvid göras av bl.a. arten, omfattningen och tiden för de möjliga åtgärderna, vilka grunder som krävs för att åtgärderna ska kunna begäras, vilka myndigheter som är behöriga att tillåta, genomföra och övervaka dem samt vilka metoder för gottgörelse som tillhandahålls genom den nationella lagstiftningen. En rimlig slutsats av Europadomstolens uttalanden är att åtgärder som utgör större intrång i privatlivet borde tillhandahållas med tydligare bemyndiganden och bli föremål för fler restriktioner än verksamhet som, i jämförelse med de förra, utgör mindre sådana intrång.

Europadomstolen har också slagit fast att nationell lagstiftning om dolda spaningsåtgärder eller hemliga tvångsmedel måste innehålla kontrollmekanismer för att skydda mot missbruk av den prövningsrätt som finns. Vad som krävs i det avseendet beror på omständigheter som 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. Beträffande telefonavlyssning har Europadomstolen ansett att beslutet normalt sett ska kontrolleras av domstol, åtminstone i sista instans. Den nationella lagstiftningen måste också, såvitt avser telefonavlyssning, innehålla tillfredsställande mekanismer för att övervaka vad som sker med överskottsinformation (se t.ex. det ovan nämnda målet Uzun mot Tyskland). När det gäller mindre ingripande åtgärder, exempelvis sådana som kan vidtas inom ramen för ett tillstånd till hemlig övervakning av elektronisk kommunikation, ställer konventionen däremot lägre krav. Som ett exempel på detta kan nämnas Europadomstolens dom den 25 september 2001 i målet

P.G. och J.H. mot Storbritannien. I målet uttalade domstolen att vad som krävs i fråga om skyddsåtgärder beror, åtminstone i viss utsträckning, på det aktuella intrångets natur och omfattning. Domstolen fann att de brittiska reglerna om telefonövervakning innehöll tillräckliga garantier mot missbruk, trots att det saknades lagregler (i motsats till interna riktlinjer för polisen) om lagring och förstörande av den information som samlades in.

Enligt artikel 13 i Europakonventionen ska var och en som fått sina fri- och rättigheter enligt konventionen kränkta ha tillgång till ett effektivt rättsmedel inför en nationell myndighet, och detta även om kränkningen förövats av någon under utövning av offentlig myndighet. Artikeln kräver inte ett rättsmedel inför domstol, utan även administrativa rättsmedel kan vara tillräckliga för att uppfylla konventionskraven (se prop. 2011/12:55 s. 55). För att rättsmedlet ska anses vara effektivt får dock den prövning som görs 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 i artikel 13 (Danelius s. 546). Europadomstolen har framhållit att det vid hemlig telefonavlyssning är svårt – eller ibland omöjligt – 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 (Danelius s. 547).

Artikel 6 i Europakonventionen innehåller bestämmelser om rätten till en rättvis rättegång. Att använda information från hemliga tvångsmedel, t.ex. överskottsinformation, som bevis kan därför beröras av artikeln. Av Europadomstolens praxis framgår dock att artikel 6 inte reglerar vilka bevis som ska vara tillåtna under förundersökning och rättegång. Frågan om vilken utredning som får läggas fram inför en nationell domstol är i första hand en angelägenhet för den nationella rättsordningen, och det kan vara legitimt att åberopa även sådan utredning som inhämtats på ett sätt som inte är förenligt med konventionen. Den fråga Europadomstolen i stället har att ta ställning till i mål om artikel 6 är om rättegången som helhet, inbegripet hur bevisningen har erhållits, har varit rättvis. För det

fall det har förekommit en kränkning av t.ex. artikel 8 har kränkningens karaktär varit avgörande. Som exempel på omständigheter som domstolen har beaktat kan nämnas om en tilltalad under rättegången har haft möjlighet att ifrågasätta tillförlitligheten av en åberopad inspelning som gjorts via telefonavlyssning, samt om ett bevis som erhållits på olagligt sätt är det enda bevis som lett till fällande dom eller om domen grundats på en samlad bedömning av olika bevis (se t.ex. P.G. och J.H. mot Storbritannien och NJA 2003 s. 323).

3.2.3 FN:s konvention om medborgerliga och politiska rättigheter

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

3.2.4 EU:s rättighetsstadga

En bestämmelse om rätt till respekt för bl.a. privatlivet 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). Av artikel 52.3 i stadgan 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.

Rättighetsstadgan riktar sig till medlemsstaterna endast när de tillämpar unionsrätten (artikel 51.1). Av EU-domstolens praxis framgår att detta innebär att rättigheterna i stadgan måste iakttas inte bara vid tillämpningen av nationell lagstiftning som genomför EU-rätt, utan så snart nationell lagstiftning omfattas av unionens tillämpningsområde (se t.ex. EU-domstolens dom den 26 februari 2013 i målet Åkerberg Fransson, C-617/10, punkt 21).

3.3 Allmänt om straffprocessuella tvångsmedel

När regleringen av tvångsmedel beskrivs bör inledningsvis framhållas att tre allmänna principer gäller för all tvångsmedelsanvändning, nämligen ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Dessa principer gäller således 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 inte är tillräcklig. Enligt proportionalitetsprincipen ska en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet stå i rimlig proportion till vad som står att vinna med åtgärden.

Rättegångsbalken innehåller inte någon definition av vad ett straffprocessuellt tvångsmedel är. Det rör sig dock om åtgärder som har en funktion inom straffprocessen men som inte är straff eller andra sanktioner. Åtgärderna företas i myndighetsutövning och utgör ett intrång i någons rättssfär. Vanligtvis – men inte för alla tvångsmedel – innefattar användningen tvång mot person eller egendom. (Se t.ex. Lindberg, *Straffprocessuella tvångsmedel*, 3 uppl. 2012, s. 5 f. och Ekelöf, *Rättegång, tredje häftet*, 7 uppl. 2006, s. 38 f.)

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

Bland de straffprocessuella tvångsmedlen intar de hemliga tvångsmedlen en särställning. Den berörde är inte medveten om att hemliga tvångsmedel 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 Ekelöf, a.a. s. 42).

De hemliga tvångsmedlen är hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation[2], hemlig kameraövervakning och hemlig rumsavlyssning.

[2] Hemlig teleavlyssning och hemlig teleövervakning bytte benämningar till hemlig avlyssning av elektronisk kommunikation respektive hemlig övervakning av elektronisk kommunikation den 1 juli 2012 (se prop. 2011/12:55 s. 127 ff.). När de senare begreppen används i

Även kvarhållande (och kontroll) av försändelse får – trots att åtgärden i rättegångsbalken inte upptas under rubriken Hemliga tvångsmedel – 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 anses också inhämtning enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) utgöra ett hemligt tvångsmedel (se prop. 2011/12:55 s. 111).

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 åtgärden vidtas, t.ex. ett gripande. Undantag finns dock, se t.ex. 23 kap. 22 § rättegångsbalken. Under vissa förutsättningar får några av de brottsbekämpande myndigheterna använda en del hemliga tvångsmedel i sin underrättelseverksamhet. Detta sker då i syfte att förhindra särskilt allvarlig brottslighet.

3.3.1 De olika lagarna på området

Det finns flera olika lagar som reglerar tvångsmedelsanvändningen och frågor förbundna med den i Sverige. I rättegångsbalken regleras försutsättningarna för användning av tvångsmedel under förundersökning, dvs. i brottsutredande verksamhet. I det följande benämns denna tvångsmedelsanvändning *förundersökningsfallen*. Tvångsmedel är också ibland tillåtna i lagstiftning om underrättelseverksamhet. I lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen), lagen om särskild utlänningskontroll (LSU) och inhämtningslagen regleras förutsättningarna för användning av tvångsmedel i dessa fall, som i det följande benämns *underrättelsefallen*.

betänkandet avses, i förekommande fall, motsvarande tvångsmedelsanvändning enligt de tidigare benämningarna.

3.4 Materiella förutsättningar för nuvarande hemliga tvångsmedel

3.4.1 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. Åtgärden får under vissa i rättegångsbalken angivna förutsättningar tillåtas under förundersökning men kan också tillåtas i underrättelseverksamhet enligt bestämmelserna i preventivlagen och LSU.

Definitionen av begreppet elektroniskt kommunikationsnät finns i 1 kap. 7 § lagen om elektronisk kommunikation och förklaras där som 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. Såvitt avser uttrycket adress framgår av förarbetena att det i begreppet ingår, liksom i det tidigare använda begreppet teleadress, olika typer av nummer, t.ex. telefonnummer och andra identifikationsnummer och adresser, såsom e-postadresser (prop. 2011/2012:55 s. 62). Tvångsmedlet kan tillämpas på alla former av kommunikation genom elektroniska kommunikationsnät och är tillämpligt på muntlig och skriftlig kommunikation, liksom på datakommunikation.

Enligt 27 kap. 18 § andra stycket rättegångsbalken kan tillstånd till hemlig avlyssning av elektronisk kommunikation lämnas vid förundersökning som rör följande brott.

1. Brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år.
2. Sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken.
3. Mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel.

4. Uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken.
5. Högförräderi, krigsanstiftan, spionerі, grovt spionerі, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6, 7, 8, 10, 10 a eller 10 b § brottsbalken.
6. Företagsspionerі enligt 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning.
7. Terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, brott enligt 3 eller 3 a § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller brott enligt lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.
8. Försök, förberedelse eller stämpling till något av de nu angivna brotten, om en sådan gärning är belagd med straff.
9. Annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Hemlig avlyssning av elektronisk kommunikation får i förundersökningsfallen, enligt 27 kap. 20 § rättegångsbalken, endast ske om någon är skäligen misstänkt för ett brott och tvångsmedlet ger, enligt 27 kap. 18 § tredje stycket rättegångsbalken, också rätt att vidta sådana åtgärder som kan vidtas inom ramen för ett tillstånd till hemlig övervakning av elektronisk kommunikation (se nedan om detta tvångsmedel).

Enligt 1 § preventivlagen får tillstånd till hemlig avlyssning av elektronisk kommunikation meddelas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar något av de brott som anges i punkterna 2–7 i uppräkningen ovan, med vissa undantag. På grund av dessa undantag är det således inte möjligt med hemlig avlyssning av elektronisk kommunikation i underrättelseverksamhet vid risk för följande brott.

– Olovlig underrättelseverksamhet mot Sverige, främmande makt eller person som inte är grovt brott,
– Brott enligt 3 § första stycket eller 3 a § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall.
– Brott enligt lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet som inte är grovt.

Det är särskilt reglerat i preventivlagen att tvångsmedlet också får tillåtas om det med hänsyn till omständigheterna finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar mord, dråp, grov misshandel, synnerligen grov misshandel, människorov eller olaga frihetsberövande enligt 3 kap. 1, 2 eller 6 § eller 4 kap. 1 § eller 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

Tillstånd till hemlig avlyssning av elektronisk kommunikation enligt preventivlagen får också meddelas 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.

Enligt 19–20 §§ LSU kan hemlig avlyssning av elektronisk kommunikation tillåtas 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.

Hemlig avlyssning av elektronisk kommunikation får i såväl förundersökningsfallen som 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, i förundersökningsfallen och i preventivlagsfallen, 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 rättegångsbalken 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 rättegångsbalken och 9 § preventivlagen). Av förarbetena framgår att uttryckssättet i bestämmelsen syftar till att klarlägga att polisen får verkställa beslut om tvångsmedel på avlyssningsområdet inte bara genom att använda traditionell avlyssningsutrustning utan också genom att använda såväl hårdvara som programvara (prop. 1994/95:227 s. 29, se också vidare i avsnitt 4.3.4).

3.4.2 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. Tvångsmedlet ger, till skillnad från hemlig avlyssning av elektronisk kommunikation, inte tillgång till uppgifter om innehållet i meddelanden. Det som kan hämtas in är i stället trafikuppgifter och lokaliseringsuppgifter. Åtgärden får under vissa i rättegångsbalken angivna förutsättningar tillåtas under förundersökning men kan också tillåtas i underrättelseverksamhet enligt bestämmelserna i preventivlagen och LSU (se strax nedan angående inhämtning enligt inhämtningslagen).

Enligt 27 kap. 19 § andra stycket rättegångsbalken kan tillstånd till hemlig övervakning av elektronisk kommunikation lämnas vid förundersökning som rör följande brott.

1. Brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader.
2. Dataintrång enligt 4 kap. 9 c § brottsbalken, barnpornografibrott enligt 16 kap. 10 a § brottsbalken som inte är att anse som ringa, narkotikabrott enligt 1 § narkotikastrafflagen (1968:64) och

narkotikasmuggling enligt 6 § första stycket lagen (2000:1225) om straff för smuggling.

3. De brott som framgår av punkterna 2–7 i listan ovan angående hemlig avlyssning av elektronisk kommunikation (se avsnitt 3.4.1).
4. Försök, förberedelse eller stämpling till brott som avses i 1–3, om en sådan gärning är belagd med straff.

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 rättegångsbalken), och att övervakning som innebär att uppgifter hämtas in om meddelanden endast får avse förfluten tid (27 kap. 20 § andra stycket rättegångsbalken).

När det gäller underrättelsefallen (enligt preventivlagen och LSU) gäller samma förutsättningar för tillstånd till hemlig övervakning av elektronisk kommunikation som för hemlig avlyssning såväl avseende vilken (möjlig) brottslighet som kan aktualisera åtgärden som vilka telefonnummer eller adresser som får övervakas.

Som för hemlig avlyssning av elektronisk kommunikation gäller vid hemlig övervakning av elektronisk kommunikation att de tekniska hjälpmedel som behövs för åtgärden får användas.

Särskilt om inhämtningslagen

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 enligt lagen 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

(2 §). Enligt en särskild bestämmelse, som för närvarande är tidsbegränsad till utgången av 2019, är inhämtning av uppgifter också möjlig vid brottslig verksamhet som innefattar vissa särskilt angivna samhällsfarliga brott inom Säkerhetspolisens ansvarsområde med ett lägre straffminimum än fängelse två år (3 §). Det bör noteras att inhämtningslagen alltså möjliggör inhämtning i tidigare skede i underrättelsefallen än vad som gäller enligt preventivlagen (som ju uppställer ett krav på *påtaglig risk*).

3.4.3 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. Tvångsmedlet omfattar inte ljudupptagning (se prop. 1995/96:85 s. 37). Åtgärden får under vissa i rättegångsbalken angivna förutsättningar tillåtas under förundersökning men kan också tillåtas i underrättelseverksamhet enligt bestämmelserna i preventivlagen.

Enligt 27 kap. 20 a § andra stycket rättegångsbalken kan tillstånd till hemlig kameraövervakning lämnas vid förundersökning som rör de brott som kan aktualisera tillstånd till hemlig avlyssning av elektronisk kommunikation (se avsnitt 3.4.1). Övervakningen får som huvudregel, i likhet med vad som gäller för hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation, användas endast om någon är skäligen misstänkt för brottet. Åtgärden får avse sådan plats där den skäligen misstänkte kan antas komma att uppehålla sig, 27 kap. 20 b § rättegångsbalken. Om det inte finns någon skäligen misstänkt för brottet får hemlig kameraövervakning användas för att övervaka den plats där brottet har begåtts eller en nära omgivning till denna plats, dock endast om syftet är att fastställa vem som skäligen kan misstänkas för brottet (27 kap. 20 c §).

När det gäller hemlig kameraövervakning enligt preventivlagen gäller samma förutsättningar för tillstånd till hemlig kameraövervakning som för hemlig avlyssning av elektronisk kommunikation avseende vilken (möjlig) brottslighet som kan aktualisera åtgärden (1 §). Hemlig kameraövervakning enligt preventivlagen får endast

avse en plats där den för tvångsmedlet aktuella personen 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 §).

3.4.4 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. Tvångsmedlet får inte användas i underrättelseverksamhet utan endast, enligt 27 kap. 20 d § rättegångsbalken, vid en förundersökning om något av följande brott.

1. Brott för vilket det inte är föreskrivet lindrigare straff än fängelse i fyra år.
2. Spioneri enligt 19 kap. 5 § brottsbalken.
3. Brott som avses i 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning och det kan antas att brottet inte leder till endast böter.
4. Annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i fyra år och det är fråga om
   a) människohandel enligt 4 kap. 1 a § brottsbalken,
   b) våldtäkt enligt 6 kap. 1 § första eller andra stycket brottsbalken,
   c) grovt sexuellt tvång enligt 6 kap. 2 § tredje stycket brottsbalken,
   d) våldtäkt mot barn enligt 6 kap. 4 § första eller andra stycket brottsbalken,
   e) grovt sexuellt övergrepp mot barn enligt 6 kap. 6 § andra stycket brottsbalken,

f) grovt utnyttjande av barn för sexuell posering enligt 6 kap. 8 § tredje stycket brottsbalken,

g) grovt koppleri enligt 6 kap. 12 § tredje stycket brottsbalken,

h) grov utpressning enligt 9 kap. 4 § andra stycket brottsbalken,

i) grovt barnpornografibrott enligt 16 kap. 10 a § femte stycket brottsbalken,

j) grovt övergrepp i rättssak enligt 17 kap. 10 § tredje stycket brottsbalken,

k) grovt narkotikabrott enligt 3 § narkotikastrafflagen (1968:64), eller

l) grov narkotikasmuggling enligt 6 § tredje stycket lagen (2000:1225) om straff för smuggling.

5. Försök, förberedelse eller stämpling till brott som avses i 1–3, om en sådan gärning är belagd med straff.

6. Försök, förberedelse eller stämpling till brott som avses i 4, om en sådan gärning är belagd med straff och det med hänsyn till omständigheterna kan antas att gärningens straffvärde överstiger fängelse i fyra år.

Tvångsmedlet får användas endast när någon är skäligen misstänkt för något av de nu angivna brotten. Därtill gäller att åtgärden endast får avse en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Avser åtgärden 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.

3.4.5 Kvarhållande av försändelse m.m.

Kvarhållande av försändelse, ibland benämnt postkontroll, finns, som ovan nämnts, inte upptaget som ett hemligt tvångsmedel under den rubriken i 27 kap. rättegångsbalken. Bestämmelserna i balken om åtgärden är i stället placerade i anslutning till reglerna om beslag. Tvångsmedlet är emellertid, som också anförts tidigare, att jämföra med de övriga hemliga tvångsmedlen. Det finns möjlighet att också i

underrättelsefallen besluta om kvarhållande av försändelse. Regelverken beträffande förundersökningsfallen och underrättelsefallen skiljer sig åt varför framställningen i det följande först inriktas på förundersökningsfallen och därefter på underrättelsefallen.

Kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken innebär att en försändelse som får tas i beslag och som väntas komma in till ett befordringsföretag, när försändelsen kommer in dit, ska hållas kvar till dess frågan om beslag har avgjorts. Förutsättningarna för att använda detta tvångsmedel är sålunda huvudsakligen knutna till reglerna om beslag. Av dessa bestämmelser framgår att ett föremål får tas i beslag om det skäligen kan antas ha betydelse för utredning om brott eller vara avhänt någon genom brott eller förverkat på grund av brott (27 kap. 1 § rättegångsbalken). En försändelse som finns hos ett post- eller telebefordringsföretag får dock tas i beslag endast om det för brottet är föreskrivet fängelse i ett år eller därutöver och försändelsen hade kunnat tas i beslag hos mottagaren (27 kap. 3 § rättegångsbalken). Kvarhållandet är hemligt i den meningen att den misstänkte eller annan som drabbas av åtgärden inte ska underrättas om den. När en försändelse hållits kvar ska befordringsföretaget utan dröjsmål göra anmälan hos den som har begärt förordnandet och denne ska omedelbart pröva om beslag ska ske. Om försändelsen tas i beslag gäller inte huvudregeln att den från vilken beslaget sker, när denne inte varit närvarande vid beslaget, utan dröjsmål ska underrättas om beslaget och om vad som skett med det beslagtagna. I stället ska underrättelse lämnas så snart det kan ske utan men för utredningen (27 kap. 11 § rättegångsbalken). Detta beror på att syftet med åtgärden annars skulle förfelas. Post- eller telegrafförsändelse, handelsbok eller annan enskild handling, som tagits i beslag, får inte närmare undersökas eller öppnas av annan än rätten, undersökningsledaren eller åklagaren. Dock får den som har rätt att närmare undersöka handlingen låta sakkunnig eller annan som hörs under utredningen granska denna (27 kap. 12 § rättegångsbalken).

När det gäller underrättelsefallen (enligt preventivlagen och LSU) är regleringen inte knuten till beslagsinstitutet. I stället gäller att rätten under vissa, i respektive lag, angivna förutsättningar får lämna tillstånd att närmare undersöka, öppna eller granska post- eller telegrafförsändelser, brev, andra slutna handlingar eller paket som finns hos ett befordringsföretag. Rätten får också i ett sådant

tillstånd förordna att en försändelse som avses i tillståndet och som ankommer till ett befordringsföretag ska hållas kvar till dess att den närmare har undersökts, öppnats eller granskats. Förordnandet ska innehålla en underrättelse om att meddelande om åtgärden inte får lämnas till avsändaren, mottagaren eller någon annan, utan tillstånd av den som har begärt åtgärden (4 § preventivlagen och 20 § LSU). Enligt båda lagarna gäller som huvudregel också att en sådan försändelse som avses får undersökas, öppnas eller granskas av rätten, en åklagare, Säkerhetspolisen eller Polismyndigheten (14 § preventivlagen och 22 § tredje stycket LSU). Vid kontroll enligt preventivlagen får, efter anvisning av någon av de som har rätt att närmare undersöka handlingen, granskningen utföras av en sakkunnig eller någon annan som har anlitats i ärendet.

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

I avsnitt 3.4 har innebörden av och några av de materiella förutsättningarna för användning av hemliga tvångsmedel beskrivits. Eftersom de materiella förutsättningarna, t.ex. beträffande vilka brott som kan leda till tvångsmedelsanvändning, utgör begränsningar i möjligheten till tvångsmedelsanvändning kan de i vid mening sägas utgöra skydd för den personliga integriteten. I följande avsnitt kommer emellertid åtgärder som i mer snäv mening utgör skydd för den personliga integriteten, garantier mot godtycklig användning av tvångsmedel och rättssäkerhetsgaranterande åtgärder vid tillämpningen av reglerna om hemliga tvångsmedel beskrivas.

3.5.1 Domstolsprövning

I förundersökningsfallen gäller som utgångspunkt att domstol prövar frågor om hemliga tvångsmedel. Ansökan görs när det gäller hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning av åklagaren (27 kap. 21 § rättegångsbalken) och vid fråga om kvarhållande av försändelse av denne eller förundersökningsledaren (27 kap. 9 § rättegångsbalken). Huvudregeln,

såvitt avser forum, är att prövningen i första instans sker vid tingsrätten i den ort där förundersökningen bedrivs, dvs. normalt den ort där gärningen är begången eller den ort där den misstänkte mera varaktigt uppehåller sig. Om ett beslut i frågan bör fattas utan dröjsmål och det är lämpligt får en sådan fråga tas upp även av rätten i en annan ort. Vid förundersökning om sådana brott som anges i punkterna 2–8 i punktlistan i avsnitt 3.4.1 ovan får Stockholms tingsrätt, som ett alternativt forum, pröva frågor om hemliga tvångsmedel (19 kap. och 27 kap. 34 § rättegångsbalken).

Även i underrättelsefallen enligt preventivlagen och LSU 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 sker ansökan av åklagaren (6 § preventivlagen) medan yrkande enligt LSU framställs av Säkerhetspolisen eller Polismyndigheten (21 § LSU). När det däremot gäller inhämtningslagen är det myndigheten själv som fattar beslut om inhämtning av uppgifter. Det är myndighetschefen, eller den som denne delegerat rätten till, som fattar beslutet. Dock gäller den begränsningen att en tjänsteman till vilken en sådan rätt delegerats inte får fatta beslut om inhämtning i sådan operativ verksamhet som han eller hon deltar i (4 § inhämtningslagen). Säkerhets- och integritetsskyddsnämnden (se nedan avsnitt 3.5.9) ska inom en månad efter att ett ärende om inhämtning avslutats underrättas om ett beslut om inhämtning av uppgifter enligt lagen (6 § inhämtningslagen).

I förundersökningsfallen finns möjlighet för åklagare att i vissa fall besluta om tillstånd till hemliga tvångsmedel interimistiskt, i avvaktan på rättens beslut. Åklagaren ska, om denne har gett ett sådant tillstånd, utan dröjsmål skriftligt anmäla beslutet till rätten. I anmälan ska skälen för åtgärden anges. Rätten ska skyndsamt pröva ärendet och om den finner att det inte finns skäl för åtgärden, upphäva beslutet. Om åklagarens beslut har verkställts innan rätten hunnit göra en prövning ska rätten pröva om det funnits skäl för åtgärden. Finner rätten att det saknats sådana skäl, får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av avlyssningen eller övervakningen, eller för någon annan som uppgifterna avser (27 kap. 21 a rättegångsbalken). Motsvarande förfarande om interimistiskt åklagarbeslut gäller enligt 27 kap. 9 a § rättegångsbalken för kvarhållande av postförsändelse

med den skillnaden att om förordnandet om sådan åtgärd upphört att gälla innan rätten har prövat ärendet ska åklagaren i stället anmäla åtgärden till Säkerhets- och integritetsskyddsnämnden. Skälet till denna skillnad är att tvångsmedlet ju inte ger tillgång till några uppgifter utan endast är ägnat att ge möjlighet till ställningstagande om försändelsen ska tas i beslag. Det bedömdes därför inte vid bestämmelsens införande ändamålsenligt med domstolsprövning av ett upphört förordnande (se prop. 2013/14:237 s. 144 f.).

Enligt 6 a § preventivlagen finns en i huvudsak motsvarande möjlighet som i förundersökningsfallen till interimistiskt åklagarbeslut beträffande hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och kvarhållande av postförsändelse (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. Därtill är en skillnad mellan bestämmelserna, eftersom tillstånd att hålla kvar en försändelse enligt preventivlagen alltid meddelas tillsammans med ett tillstånd även att undersöka, öppna och granska den försändelse som tillståndet gäller (4 §), att domstolsprövning ska ske även av sådana beslut om kvarhållande av försändelse som har verkställts (se prop. 2013/14:237 s. 145).

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 § rättegångsbalken, 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. Proportionalitetsprincipen finns kodifierad i bl.a. 27 kap. rättegångsbalken, 5 § preventivlagen och 2 § 2 inhämtningslagen men gäller, som redan nämnts, vid tillämpningen av all tvångsmedelslagstiftning.

För att hemliga tvångsmedel ska få tillåtas ställs också upp vissa kvalificerande krav som tar sikte på behovet av åtgärden i det enskilda fallet. Således krävs att åtgärden är av synnerlig vikt för utredningen (rättegångsbalken), av synnerlig vikt för att förhindra brottslighet (preventivlagen) alternativt att det ska föreligga synnerliga skäl för åtgärden (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 lagen. Något dylikt kvalificerande krav för tillstånd till kvarhållande av försändelse i förundersökningsfallen finns emellertid inte uttryckt i lagtext.

3.5.2 Beslutets innehåll

I samtliga beslut om hemliga tvångsmedel ska rätten, eller i förekommande fall annan beslutsfattande myndighet, ange vilken tid beslutet gäller. Tiden får inte bestämmas längre än nödvändigt och får, när det gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet. Nytt beslut krävs för fortsatt användning av hemliga tvångsmedel efter att den i beslutet angivna tiden löpt ut.

I ett tillstånd till hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation ska i beslutet anges vilket telefonnummer eller annan adress alternativt vilken elektronisk kommunikationsutrustning tillståndet avser. Det ska vidare särskilt anges om åtgärden får verkställas utanför allmänt tillgängliga elektroniska kommunikationsnät. I förundersökningsfallen ska det, vid tillstånd till inhämtning av uppgifter om vilka mobila kommunikationsutrustningar som har funnits inom ett visst geografiskt område (dvs. uppgifter som får hämtas in efter tillstånd till hemlig övervakning av elektronisk kommunikation), anges vilket geografiskt område tillståndet avser.

När det gäller tillstånd till hemlig kameraövervakning ska, såväl enligt rättegångsbalken som enligt preventivlagen, 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 till 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.

3.5.3 Skydd för samtal med och meddelanden till och från vissa personer

I 36 kap. 5 § andra–sjätte styckena rättegångsbalken finns regler beträffande personkategorier som till följd av sitt yrke, under i lagrummet angivna förutsättningar, är undantagna från vittnesplikten, bl.a. advokater, präster och läkare. Med anledning av dessa regler finns särskilda bestämmelser såvitt avser användningen av vissa hemliga tvångsmedel när den som tvångsmedlet riktas mot samtalar med eller skickar alternativt tar emot meddelanden till eller från personer som omfattas av reglerna i nämnda bestämmelse i rättegångsbalken. Hemlig avlyssning av elektronisk kommunikation får således inte avse 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. 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 omedelbart förstöras i de delar som de omfattas av förbud (27 kap. 22 § rättegångsbalken). Motsvarande bestämmelse (beträffande hemlig avlyssning av elektronisk kommunikation) finns i preventivlagen (11 §).

3.5.4 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 såvitt avser inhämtningslagen, där i stället den brottsbekämpande myndigheten själv ska häva beslutet. Det anförda följer

av bestämmelser i 27 kap. 23 § rättegångsbalken, 10 § preventivlagen och 5 § inhämtningslagen. Vid tvångsmedelsanvändning enligt preventivlagen gäller dessutom att Polismyndigheten eller Säkerhetspolisen omedelbart ska underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas.

3.5.5 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 leder endast 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 för att berika materialet i en redan pågående förundersökning (27 kap. 23 a § rättegångsbalken).

I underrättelsefallen gäller delvis olika förutsättningar för användande av överskottsinformation. I samtliga fall gäller dock, vilket även gäller i förundersökningsfallen, att uppgifter om förestående brott alltid får användas för att förhindra brott. När det gäller överskottsinformation som framkommit vid tvångsmedelsanvändning enligt preventivlagen får sådan information användas för att utreda brottet endast om det är fråga om brott som omfattas av lagen, försök, förberedelse eller stämpling till sådant brott om en sådan gärning är belagd med straff samt brott för vilket det är föreskrivet fängelse i tre år eller däröver (12 §). Enligt 21 a § LSU får överskottsinformation som framkommit vid hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation användas för att utreda brottet. Förundersökning eller mot-

svarande 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 det finns särskilda skäl. Uppgifter som har kommit fram vid inhämtning enligt inhämtningslagen får enligt dess 8 § 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.

3.5.6 Granskning, bevarande och förstörande av insamlat material

I samtliga fall då hemliga tvångsmedel använts gäller att upptagningen eller uppteckningen som gjorts ska 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. Upptagningar och uppteckningar ska i dessa fall, i de delar de är av betydelse från brottsutredningssynpunkt, bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet har avgjorts slutligt. I de delar 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 § rättegångsbalken). Eftersom det ofta är svårt att vid varje tidpunkt under en brottsutredning bedöma vilken information som är av betydelse från utredningssynpunkt och vilken som inte är det torde i praktiken allt material som inte omedelbart ska förstöras, på grund av t.ex. förbud mot avlyssning, bevaras så länge förundersökning och lagföring pågår.

Både preventivlagen och LSU stadgar att granskning av uppteckningar eller upptagningar ska ske snarast möjligt och att sådan får utföras av rätten, Säkerhetspolisen, Polismyndigheten eller åklagare. Enligt preventivlagen får granskning ske även av sakkunnig eller någon annan som har anlitats i ärendet.

Preventivlagen 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 LSU ska upptagningen eller upptecknin gen om den innehåller något som inte är av betydelse för ändamålet med avlyssningen i denna del omedelbart förstöras efter granskningen. I fråga om brott eller förestående brott som inte är av betydelse för ändamålet med avlyssningen gäller dock motsvarande bestämmelser som i förundersökningsfallen (22 § LSU).

I inhämtningslagen regleras frågan om granskning av upptecknin gar av uppgifter i 9 §. Upptecknin gar ska, i de delar de är av betydelse för att förebygga, förhindra eller upptäcka brottslig verksamhet som omfattas av beslutet om inhämtning eller för att förhindra annat brott, bevaras så länge det behövs för något av dessa syften. De ska därefter förstöras.

I både förundersöknings- och underrättelsefallen gäller, trots vad som nu angetts, att brottsutredande myndigheter under vissa förutsättningar får behandla uppgifter från upptagningar och upptecknin gar i enlighet med vad som är särskilt föreskrivet i lag. Det kan t.ex. finnas regler om att uppgifter från upptagningarna och upptecknin garna ska bevaras. I sådana fall får brottsutredande myndigheter i enlighet med de särskilda villkor som ställs upp i rättegångsbalken, preventivlagen, LSU och inhämtningslagen behandla uppgifterna i enlighet med annan lagstiftning.

3.5.7 Offentliga ombud

Offentliga ombud ska bevaka 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, i de senare genom hänvisning till rättegångsbalkens regler (6 § preventivlagen och 21 § LSU). Däremot finns inte regler om offentligt ombud beträffande hemlig övervakning av elektronisk kommunikation eller kvarhållande av försändelse. Inte heller finns krav på offentligt ombud vid tillämpning av inhämtningslagen.

Regeringen förordnar för tre år i sänder personer som kan tjänstgöra som offentliga ombud. Ett offentligt ombud ska vara svensk

medborgare och vara eller ha varit advokat alternativt ha varit ordinarie domare. Regeringen ska inhämta förslag på lämpliga kandidater från Sveriges advokatsamfund och Domarnämnden (27 kap. 27 § rättegångsbalken).

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 § rättegångsbalken). 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 ett sammanträde. Vid sammanträdet ska åklagaren och det offentliga ombudet närvara (27 kap. 28 § rättegångsbalken).

3.5.8 Underrättelse till enskild

Det finns en skyldighet att i efterhand underrätta vissa personer om att hemliga tvångsmedel har använts. I förundersökningsfallen gäller som huvudregel enligt 27 kap. 31 § rättegångsbalken 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. Om 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 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 § rättegångsbalken). Det finns dock ett flertal undantag från underrättelseskyldigheten. Exempelvis kan den omständigheten att viss sekretess råder leda till att underrättelse ska skjutas upp till dess att sekretess inte längre gäller. Detta kan leda till att underrättelseskyldigheten helt faller bort. I sådana fall ska Säkerhets- och integritetsskyddsnämnden underrättas enligt 14 b § förundersökningskungörelsen. Ytterligare ett undantag från underrättelseskyldigheten är att om

förundersökningen angår vissa särskilt angivna brott, huvudsakligen brott mot Sveriges säkerhet, ska underrättelse inte lämnas.

På motsvarande sätt som för förundersökningsfallen gäller underrättelseskyldighet enligt preventivlagen. Underrättelse till enskild ska i dessa fall lämnas så snart det kan ske efter att det ärende som åtgärden vidtogs i avslutades. Eftersom flertalet brott enligt lagen som kan föranleda tvångsmedelsanvändning emellertid är brott mot Sveriges säkerhet kan huvudregeln i dessa fall snarare sägas vara att underrättelse inte ska lämnas. För åtgärder som vidtas enligt LSU gäller ingen underrättelseskyldighet, vilket har motiverats med att det brott som lagen avser är terroristbrott. I fråga om inhämtning av uppgifter om elektronisk kommunikation enligt inhämtningslagen finns ingen bestämmelse om underrättelse till enskild. Däremot ska enligt 6 § inhämtningslagen Säkerhets- och integritetsskyddsnämnden underrättas om varje beslut om inhämtning senast en månad efter att inhämtningen avslutats.

3.5.9 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 samt 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 (1 och 2 §§). 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 (3 §).

I vissa fall ska Säkerhets- och integritetsskyddsnämnden få underrättelse från åklagaren om vidtagna tvångsmedelsåtgärder. När underrättelse i efterhand till enskild om tvångsmedelsanvändningen har underlåtits på grund av sekretess, ska nämnden underrättas om detta. Säkerhets- och integritetsskyddsnämnden ska också underrättas om beslut om inhämtning enligt inhämtningslagen (6 §).

3.6 Något om vissa andra tvångsmedel

3.6.1 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. rättegångsbalken.

Beslag får enligt 27 kap. 1 § första stycket rättegångsbalken göras för olika ändamål. För det första får föremål som skäligen kan antas ha betydelse för utredning om brott tas i beslag (bevisbeslag). Beslaget 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 eller att försöka knyta en gärningsman till brottet. Beslaget kan också syfta till att belysa gärningsmannens uppsåt eller brottets svårhet. En annan typ av beslag avser föremål som skäligen kan antas vara någon avhänt 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 förverkande av utbyte av brottslig verksamhet enligt 36 kap. 1 b § brottsbalken. Eftersom beslaget avser att säkra föremål och handlingar som behövs för att utreda en sådan förverkandefråga är detta en form av bevisbeslag.

Endast lösa föremål och skriftliga handlingar får tas i beslag. Beslag får i allmänhet ske 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. 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. Beslag kan därför 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. Eftersom beslagsbeslutet ska kunna verkställas omedelbart förutsätter ett beslag också att godset är fysiskt tillgängligt.

I 27 kap. 2 § rättegångsbalken regleras det s.k. beslagsförbudet. Av bestämmelsen framgår 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 § rättegångsbalken inte får höras som vittne om och handlingen innehas av honom eller henne eller av den som tystnadsplikten gäller till förmån för. Vidare gäller enligt bestämmelsen att ett skriftligt meddelande mellan den misstänkte och en närstående som avses i 36 kap. 3 § rättegångsbalken, eller mellan sådana närstående inbördes, får tas i beslag hos den misstänkte eller en närstående endast vid en förundersökning om sådana brott som anges i punktlistan i avsnitt 3.4.1, med undantag för brott enligt punkten 9 där. Högsta domstolen har i rättsfallet NJA 2015 s. 631 fastslagit att beslagsförbudet i 27 kap. 2 § rättegångsbalken omfattar även annan information än skrift och andra bärare av information än papper.

3.6.2 Husrannsakan

Om det finns anledning att anta att ett brott på vilket fängelse kan följa har begåtts får, enligt 28 kap. 1 § första stycket rättegångsbalken, 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 dock 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 vid rannsakningen ska 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 (samma §, andra stycket). Husrannsakan får också ske för andra syften, t.ex. delgivning och eftersökande av person, se 28 kap. 2–3 § rättegångsbalken.

Det är i normalfallet undersökningsledaren eller åklagaren som förordnar om husrannsakan som avses i 28 kap. 1 § rättegångsbalken men enligt 28 kap. 4 § första stycket rättegångsbalken får också rätten besluta i frågan. Om det är fara i dröjsmål får en polisman, enligt 28 kap. 5 § rättegångsbalken, företa husrannsakan utan sådant förordnande. Motsvarande befogenhet finns enligt 26 § smugglingslagen för tjänsteman vid Tullverket eller Kustbevakningen i vissa situationer.

Vid en husrannsakan ska, om det är möjligt, ett av den som utför åtgärden anmodat trovärdigt vittne närvara. Den, hos vilken husrannsakan sker, ska få tillfälle att övervaka förrättningen och att även tillkalla vittne om detta inte orsakar dröjsmål. Är vederbörande inte hemma gäller detsamma för ”hans hemmavarande husfolk”. Om varken den som husrannsakan genomförs hos eller hans husfolk eller av dem tillkallat vittne närvarat vid husrannsakan ska han eller hon, så snart det kan ske utan men för utredningen, underrättas om den vidtagna åtgärden (28 kap. 7 § rättegångsbalken). En husrannsakan kan således ske i hemlighet, och kan därför i vissa fall anses utgöra ett hemligt tvångsmedel.

Liksom för alla tvångsmedel gäller att den som beslutar om husrannsakan ska göra en proportionalitetsavvägning (28 kap. 3 a § rättegångsbalken). Reglerna om husrannsakan och beslag har vidare ett funktionellt samband på så sätt att en husrannsakan ofta är nödvändig för att möjliggöra ett beslag. Rättsligt sett föreligger det sambandet att husrannsakan i beslagssyfte förutsätter att det sökta föremålet kan tas i beslag. Som nämnts ovan under redogörelsen för beslagsinstitutet har Högsta domstolen genom lagtolkning fastslagit att beslagsförbudet i 27 kap. 2 § rättegångsbalken omfattar även annan information än skrift och andra bärare av information än papper. Det råder dock alltjämt viss osäkerhet om reglerna om husrannsakan och beslag är direkt tillämpliga på den information som är lagrad i elektronisk utrustning eller kan göras tillgänglig med sådan utrustning. Högsta domstolen anförde med anledning därav i det angivna rättsfallet att ”lagregleringen när det gäller tvångsmedelsanvändning i vad som skulle kunna kallas det virtuella rummet är

otidsenlig". Regeringen har tillsatt en utredning som ska se över reglerna om beslag och husrannsakan i syfte att skapa ändamålsenliga regler som möjliggör effektiva och rättssäkra brottsutredningar (dir 2016:20).[3]

3.7 Något om annan relevant lagstiftning

3.7.1 Lagen om internationell rättslig hjälp i brottmål

Genom lagen (2000:562) om internationell rättslig hjälp i brottmål och förordningen (2000:704) med samma namn har innehållet i flera internationella överenskommelser som Sverige är bundet av implementerats. Lagen är tillämplig på samarbete som tar sikte på rättsliga förfaranden som gäller utredning om och lagföring för brott. Enligt 1 kap. 2 § den lagen kan rättslig hjälp omfatta bl.a.

- hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,
- tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,
- tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation,
- hemlig kameraövervakning samt
- hemlig rumsavlyssning.

Tillstånd till hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning i Sverige – utförd av svenska myndigheter – lämnas under samma förutsättningar som gäller för motsvarande åtgärder under en svensk förundersökning, enligt rättegångsbalken eller annan lag eller författning, med beaktande av de särskilda bestämmelser som finns i lagen om internationell rättslig hjälp i brottmål (2 kap. 1 §). En ansökan om rättslig hjälp i form av

[3] Se vidare beträffande den osäkerhet som råder på området Lindberg, *Straffprocessuella tvångsmedel*, 3 uppl. s. 403 f., Hjertstedt, *Tillgången till handlingar för brottsutredare*, s. 213 f. och Ds 2005:6 s. 283 f.

dessa tvångsmedel handläggs av åklagare. Åklagaren ska genast pröva om det finns förutsättningar för den begärda åtgärden och ansöka om rättens tillstånd eller, när det får ske enligt 27 kap. 21 a § rättegångsbalken, själv besluta om åtgärden (4 kap. 25, 27 och 28 a §§). Vid prövningen om åtgärden kan vidtas i Sverige ska gärningen bedömas enligt svensk rätt och de svenska strafftrösklarna gäller. Det föreligger ett krav på dubbel straffbarhet (2 kap. 2 §).

Enligt 4 kap. 25 a § får rättens beslut att tillåta hemlig avlyssning eller övervakning av elektronisk kommunikation verkställas genom omedelbar överföring av meddelanden eller uppgifter om meddelanden till den ansökande staten, om det kan ske under betryggande former och den andra staten antingen är en stat som är medlem i Europeiska unionen eller Island eller Norge. Tekniskt bistånd i Sverige med hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation i form av omedelbar överföring av meddelanden eller uppgifter om meddelanden får lämnas i Sverige enligt 4 kap. 25 b §. Sådant bistånd kan enligt bestämmelsen lämnas på ansökan av EU-länder, Island eller Norge, varvid förutsätts bl.a. att avlyssningen eller övervakningen avser någon som befinner sig i en av de nämnda staterna – dvs. inte i Sverige – och att ansökan innehåller en bekräftelse på att ett beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation i en brottsutredning har meddelats i den ansökande staten. Ansökan prövas av åklagare och genom hänvisning till vissa bestämmelser i rättegångsbalken gäller, bl.a. samma definitioner som där för tvångsmedlen, reglerna om begränsning i tid för tillstånd och skyldigheten att i omedelbart upphäva beslutet om det inte längre finns skäl för det. Enligt 2 kap. 2 § får tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation lämnas även om den gärning som ansökan avser inte motsvarar ett brott enligt svensk lag.

De länder som nämnts i föregående stycke kan även ansöka om tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation – utan svenskt bistånd – av någon som befinner sig i Sverige. En ansökan om sådan rättslig hjälp handläggs av åklagare som genast ska pröva om förutsättningar för åtgärden finns och i så fall ansöka om rättens tillstånd. Rätten har vid tillståndsprövningen att pröva

ansökan utifrån de förutsättningar som föreskrivs i 27 kap. 18–20, 21 och 22 §§ rättegångsbalken om brottets svårhetsgrad, misstankegrad m.m. gäller i dessa fall och det finns särskilda regler om att beslut ska meddelas inom viss tid från det att ansökan inkom (4 kap. 26 a och b §§). För bifall krävs dessutom dubbel straffbarhet (2 kap. 2 §).

Det finns också möjlighet för Sverige att tillåta hemlig kameraövervakning och hemlig rumsavlyssning på ansökan av annan stat. I båda fallen gäller att åklagare genast ska pröva om det finns förutsättningar för åtgärden enligt ansökan och, om så är fallet, ansöka om rättens tillstånd. I de fall som avser hemlig kameraövervakning får åklagaren, när förutsättningar finns enligt 27 kap. 21 a § rättegångsbalken, själv besluta om åtgärden. Prövningen ska i båda fallen göras utifrån de för respektive tvångsmedel i rättegångsbalken angivna reglerna. Dock behöver inte granskning av upptagningar ske enligt 27 kap. 24 § rättegångsbalken. Därtill gäller vissa särskilda bestämmelser om underrättelse till enskild och bevarande av upptagningar (4 kap. 27 och 28 §§).

Det finns också vissa allmänna regler som gäller för samtliga prövningar av ansökningar från andra länder. En ansökan ska enligt dessa bestämmelser avslås om ett bifall till ansökan skulle kränka Sveriges suveränitet, medföra fara för rikets säkerhet eller strida mot svenska allmänna rättsprinciper eller andra väsentliga intressen. Ansökan får vidare avslås om gärningen har karaktär av ett politiskt brott, gärningen utgör ett militärt brott, om inte gärningen motsvarar även annat brott enligt svensk lag vilket inte är ett militärt brott, det i Sverige har meddelats dom eller beslut om åtalsunderlåtelse eller straffvarning beträffande gärningen, eller omständigheterna annars är sådana att ansökan inte bör bifallas. Om åklagaren eller domstolen finner att ansökan bör avslås på någon av de nu angivna grunderna ska ansökan överlämnas till regeringen som beslutar i frågan (2 kap. 14 och 15 §§).

Om en begäran om rättslig hjälp bifalls, kan beslutet förenas med villkor som är påkallade med hänsyn till enskilds rätt eller som är nödvändiga från allmän synpunkt. Villkor får dock inte ställas upp om de strider mot en internationell överenskommelse som är bindande för Sverige (5 kap. 2 §).

Det finns också möjlighet för Sverige att med stöd av lagens bestämmelser, och i vissa fall utan stöd i aktuell lag under förutsättning att den andra staten tillåter det, begära rättslig hjälp i brott-

mål utomlands. Det är i lagen föreskrivet bl.a. vad åklagaren har att iaktta vid ansökan om rättslig hjälp till annan stat och vart ansökan ska skickas.

3.7.2 Lagen om elektronisk kommunikation

I lagen om elektronisk kommunikation, som syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster, finns bestämmelse av stor betydelse för användningen av hemliga tvångsmedel. Flera centrala begrepp definieras (se t.ex. 1 kap. 7 § och 6 kap. 1 §) och viktiga gränsdragningar görs i lagen som är av betydelse för bl.a. verkställighet av hemlig avlyssning och övervakning av elektronisk kommunikation. I 2 kap. 1 § slås fast att allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster endast får tillhandahållas efter anmälan till tillsynsmyndigheten (Post- och telestyrelsen). Som utgångspunkt gäller att den som bedriver 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 §). 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 emellertid 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, inhämtning av uppgifter enligt inhämtningslagen (6 kap. 8 §).

Vidare finns i lagen bestämmelser om lokaliseringsuppgifter som inte är trafikuppgifter. Sådana 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 undantag som innebär att de får behandlas utan nyss nämnda begränsning om de omfattas av beslut om inhämtning

av uppgifter enligt 27 kap. rättegångsbalken eller inhämtningslagen (6 kap. 10 a§).

Vid verkställighet av hemlig avlyssning eller övervakning av elektronisk kommunikation finns i vissa situationer möjlighet för de brottsbekämpande myndigheterna att få information från operatörer och andra som tillhandahåller tjänster på området. Enligt 6 kap. 19 § 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 i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket 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. lagen om elektronisk kommunikation kan härledas från ett EU-direktiv från 2002.[4] Det direktivet antogs bl.a. för att säkerställa full respekt för rättigheter enligt artikel 7 och 8 i EU:s rättighetsstadga. En sammanfattning av direktivets innehåll i här relevanta delar och kopplingen till bestämmelserna i 6 kap. lagen om elektronisk kommunikation finns i SOU 2017:75, kapitel 4.

3.7.3 Sekretessfrågor

I 2 kap. 1 tryckfrihetsförordningen finns den svenska utgångspunkten om allmänna handlingars offentlighet. Av bestämmelsen framgår att till främjande av ett fritt meningsutbyte och en allsidig upplysning ska varje svensk medborgare ha rätt att ta del av allmänna

[4] Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation) (EGT L 201, 2002, s. 37), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 (EUT L 337, 2009, s. 11).

handlingar. Enligt 2 kap. 2 § första stycket tryckfrihetsförordningen får rätten att ta del av allmänna handlingar dock begränsas bl.a. om det är påkallat med hänsyn till intresset att förebygga eller beivra brott och skyddet för enskildas personliga eller ekonomiska förhållanden. Regler om sådana begränsningar finns bl.a. i offentlighets- och sekretesslagen (OSL). I den lagen finns vissa bestämmelser som är av särskild betydelse när reglerna om hemliga tvångsmedel ska beskrivas.

Sekretess gäller enligt 18 kap. 1 § OSL 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. I 18 kap. 2 § OSL regleras om sekretess 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. Enligt 18 kap. 3 § OSL gäller sekretessen enligt nu nämnda bestämmelser i annan verksamhet än som där avses hos en myndighet för att biträda en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott. 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 18 kap. 19 § regleras i vilka fall den tystnadsplikt som följer av sekretessbestämmelserna inskränker den grundlagsstadgade rätten att meddela och offentliggöra uppgifter (se 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen). Såvitt avser uppgifter om hemliga tvångsmedel är huvudregeln att tystnadsplikten som följer av 18 kap. 1–3 och 17 §§ OSL att tystnadsplikten har företräde framför rätten att meddela och offentliggöra uppgifter.

I 35 kap. OSL regleras sekretess till skydd för skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott, m.m. Av dess 1 § bl.a. att sekretess gäller för uppgift om en enskilds person-

liga 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. Tystnadsplikten enligt bestämmelsen har inte företräde framför rätten att meddela och offentliggöra uppgifter.

Det finns också bestämmelser i enskilda lagar som reglerar sekretess. Av visst intresse i detta sammanhang är att det i 6 kap. 21 § lagen om elektronisk kommunikation regleras om tystnadsplikt för den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av uppgift som hänför sig till bl.a. angelägenhet som avser användning av hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 27 kap. 18 eller 19 § rättegångsbalken eller tekniskt bistånd med hemlig avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § lagen (2000:562) om internationell rättslig hjälp i brottmål. Enligt 44 kap. 4 § OSL gäller att tystnadsplikt som följer av 6 kap. 21 § lagen om elektronisk kommunikation såvitt avser hemliga tvångsmedel har företräde framför rätten att meddela och offentliggöra uppgifter.

4 Introduktion till hemlig dataavläsning

4.1 Inledning

Frågan om hemlig dataavläsning i Sverige kom officiellt upp på regeringens agenda när Beredningen för rättsväsendets utveckling (BRU) lämnade delbetänkandet *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 det på betänkandet följande remissförfarandet riktades viss kritik mot förslaget om hemlig dataavläsning och det ledde inte till lagstiftning. Frågan om hemlig dataavläsning har också varit uppe i samband med annat utredningsarbete (bland annat SOU 2012:44).

I detta kapitel presenteras först det tidigare svenska förslaget till lagstiftning avseende hemlig dataavläsning, jämte vissa synpunkter från remissinstanserna. Något sägs också om vad Utredningen om vissa hemliga tvångsmedel anförde om hemlig dataavläsning. Därefter introduceras hemlig dataavläsning, främst avseende vilka typer av uppgifter åtgärden potentiellt skulle kunna förse de brottsbekämpande myndigheterna med och varför metoden inte redan används.

4.2 Tidigare förslag om hemlig dataavläsning i Sverige

4.2.1 SOU 2005:38

BRU:s uppdrag bestod i att verka för rättsväsendets utveckling. Enligt dess huvuddirektiv hade beredningen i uppdrag att undersöka möjligheterna att än mer öka effektiviteten och kvaliteten i rätts-

väsendets arbete. Inom ramen för uppdraget fanns bland annat uppgiften att särskilt överväga på vilket sätt brottsutredningsverksamheten ytterligare kunde förbättras.

Det fanns inget riktat uppdrag i beredningens direktiv att utreda frågan om hemlig dataavläsning. Anledningen till att frågan togs upp var i stället att det under beredningens arbete från flera håll framfördes att möjligheten till användning av hemlig dataavläsning för de svenska brottsutredande myndigheterna borde utredas (SOU 2005:38 s. 50).

Som bakgrund till angelägenheten att se på frågan om att införa bestämmelser om dataavläsning i svensk rätt, efter den modell som redan då fanns i Danmark, anfördes bland annat att teknikutvecklingen som skett under tiden som bestämmelserna om hemlig avlyssning och övervakning av elektronisk kommunikation funnits hade varit oerhört kraftig och mycket snabb. Det var därför självklart att de allra senaste nyheterna på teknikområdet utnyttjades som verktyg, särskilt i grov brottslig verksamhet. Således ansåg BRU att det var helt nödvändigt för samhället att myndigheterna inte hamnade hjälplöst efter utan, inom ramen för ett godtagbart integritetsintrång, fick rätt att använda brottsutredande metoder som var effektiva och anpassade till den tekniska situation som rådde vid varje givet tillfälle. Det kunde, enligt beredningen, vidare ifrågasättas om de då befintliga hemliga tvångsmedlen var tillräckliga i alla fall. Även de konsekvenser för brott och brottsbekämpning som följde av en ökad internationalisering och det genomdatoriserade samhället framfördes som argument, liksom medborgarnas och då även de kriminellas ökade kompetens i it-frågor. Vidare framhölls den omständigheten att möjligheten att kommunicera över internet på ett relativt anonymt och säkert sätt (främst frågan om kryptering), vid sidan av globalisering och mobilitet, utgjorde stora utmaningar som den it-relaterade brottsligheten ställde upp för rättsväsendet. (Se a. SOU s. 50 f.)

När det gällde behovet och effektiviteten av hemlig dataavläsning som ett nytt tvångsmedel konstaterade BRU att det största behovet av hemlig dataavläsning fanns vid brottslighet som innehåller organisation och planering. Detta då det särskilt vid organiserad eller annan allvarlig brottslighet ofta fanns vissa deltagande personer som var utomordentligt skickliga i användningen av datorer och utnyttjade sina kunskaper fullt ut. Genom olika åtgärder via datorerna kunde de därigenom genomföra brott, gömma information, hålla sig anonyma och undgå upptäckt. Den snabba tekniska utvecklingen

medförde enligt beredningen vidare att det fanns stora problem i brottsutredningar med att få fram uppgifter ur datorer eller avlyssna meddelanden mellan datorer. Det gällde särskilt när den informationen var skyddad av kryptering, eller när program användes som på annat sätt dolde information. I ett ständigt ökande antal brottsutredningar påträffades, enligt BRU, krypterad information i form av enskilda filer eller i en viss yta av lagringsutrymmet (exempelvis en dators hårddisk). Också den omständigheten att det bland kriminella är välkänt vilka arbetsmetoder polisen har och inte har och att dessa kunskaper utnyttjas för att göra brottslig verksamhet så effektiv som möjligt framhölls av BRU i behovsanalysen. Därtill anförde beredningen den ökade användningen av kryptering i samband med elektronisk kommunikation och de svårigheter detta medförde för de brottsbekämpande myndigheterna att genom de tillgängliga tvångsmedlen ta del av innehåll i meddelanden som skäl för behovet av den nya åtgärden. Ytterligare en omständighet som beredningen pekade på var möjligheten för dem som agerar i brottsliga syften att vara anonyma vid användning av informationsteknik eftersom uppgifter om abonnemang och IP-adress, vilka är möjliga att få fram genom andra tvångsmedel, inte säger någonting säkert om vem som suttit vid datorn och agerat vid den aktuella tidpunkten. (Se a. SOU s. 52 f. och 356 ff.)

Mot bakgrund av bland annat det anförda fann BRU att det knappast fanns några alternativ till hemlig dataavläsning att få fram den gömda informationen på. Beredningen konstaterade att det är en svår uppgift att avväga integritetsintresset mot nödvändigheten av att myndigheterna har effektiva metoder för bland annat brottsutredning men fann att i allmänhet bör kunna sägas att integritetsintrånget med hemlig dataavläsning i vart fall inte skulle bli större än vid tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. (Se a. SOU s. 54 och 367 f.)

BRU:s förslag blev att införa bestämmelser om hemlig dataavläsning i en särskild, tidsbegränsad, lag eftersom närmare detaljer i frågor om behovet och effektiviteten inte var helt enkla att bedöma innan tvångsmedlet tillämpats under en tid. Enligt beredningen skulle, för att det senare skulle finnas ett fullgott underlag för en utvärdering av bestämmelserna och för en bedömning av frågan om lagen borde ges förlängd giltighetstid eller t.ex. permanentas, lagens

giltighetstid bestämmas till i vart fall fem år. (Se a. SOU s. 55 och 370 f.)

Enligt den föreslagna lagens 1 § avsågs med hemlig dataavläsning att ”information i informationssystem i hemlighet avläses med hjälp av program eller annat tekniskt hjälpmedel vid förundersökning i brottmål”. Det innebar enligt BRU att såväl information som fanns i informationssystemet när verkställigheten påbörjades som information som därefter genererades kunde avläsas. Med begreppet informationssystem avsåg BRU att få ett teknikneutralt uttryck som täckte in både de dåvarande och framtida informationsmöjligheterna och informationsvägarna men som ändå var avgränsat (främst på grund av att det användes i andra författningar och sammanhang utan att definieras). (Se a. SOU s. 419)

Beträffande proceduren vid tillståndsprövningen föreslog BRU att domstol skulle besluta efter ansökan av åklagare och att offentliga ombud skulle bevaka enskildas intressen vid prövningen hos domstol (a. SOU s. 371 ff.).

Brottskatalogen, dvs. vilka brott som vid misstanke om dem skulle kunna leda till hemlig dataavläsning, föreslogs motsvara den som gällde för hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning med vissa anpassningar beträffande dataintrång, hets mot folkgrupp och barnpornografibrott (a. SOU s. 373 f.). När det gällde brottsmisstankens styrka och behovet av åtgärden föreslog BRU även i denna del motsvarande bestämmelse som gällde för övriga hemliga tvångsmedel, dvs. att huvudregeln skulle vara att metoden skulle få användas när utredningen kommit så långt att någon var skäligen misstänkt för brottet, att åtgärden skulle vara av synnerlig vikt för utredningen samt att skälen för åtgärden uppvägde det intrång eller men i övrigt som åtgärden innebar för den misstänkte eller något annat motstående intresse (a. SOU s. 378 ff.). Emellertid föreslog beredningen också, mot bakgrund av att de två huvudsakliga skälen för att införa hemlig dataavläsning var problemen med krypterad information och möjligheten att vara anonym, att hemlig dataavläsning i vissa fall skulle få äga rum även om det saknades en skäligen misstänkt person. Så skulle endast få ske om åtgärden syftade till att fastställa vem som skäligen kan misstänkas för brottet. I de fallen fick åtgärden endast avse informationssystem som använts eller användes vid brottet (a. SOU s. 382 ff.).

Beträffande sambandet mellan den misstänkte och informationssystemet som tillståndet skulle avse föreslog BRU, i de fall det fanns en skäligen misstänkt person, att hemlig dataavläsning endast skulle få avse ett informationssystem som det fanns särskild anledning att anta att den misstänkte använt sig av eller skulle komma att använda sig av. Om åtgärden avsåg ett informationssystem i någon annans stadigvarande bostad skulle enligt förslaget hemlig dataavläsning få äga rum bara om det fanns synnerlig anledning att anta att den misstänkte använt sig av eller skulle komma att använda sig av det (a. SOU s. 384 ff.). Bestämmelsen om den tid för vilken tillstånd till hemlig dataavläsning enligt BRU:s förslag skulle kunna meddelas motsvarade de som gällde för övriga hemliga tvångsmedel, dvs. tillstånd skulle kunna meddelas för högst en månad åt gången (a. SOU s. 387 ff.).

Beredningen föreslog också att hemlig dataavläsning inte skulle få ske av meddelanden mellan den misstänkte och dennes försvarare. Om det framkom under avläsningen att det var fråga om ett sådant meddelande skulle avläsningen omdedelbart avbrytas och upptagningen omedelbart förstöras (a. SOU s. 391 f.). Användande av överskottsinformation skulle enligt förslaget få ske för att inleda förundersökning eller motsvarande utredning endast om det för brottet var föreskrivet fängelse i ett år eller däröver och det kunde antas att brottet inte skulle föranleda endast böter eller om det fanns särskilda skäl. Liksom vad som gällde för övriga tvångsmedel skulle det enligt förslaget vara tillåtet att använda överskottsinformationsuppgifter för att förhindra förestående brott (a. SOU s. 392 f). Granskning av upptagningar från hemlig dataavläsning skulle enligt förslaget ske snarast möjligt. De delar av upptagningarna som var av betydelse från brottsutredningssynpunkt skulle bevaras till dess att förundersökningen lagts ned eller avslutats eller, om åtal väckts, målet avgjorts slutligt. Om upptagningar var av betydelse för förhindrande av förestående brott skulle de bevaras så länge det behövdes för att förhindra brott och därefter förstöras (a. SOU s. 394 ff.). I enlighet med vad som gällde för övriga hemliga tvångsmedel föreslogs att regeringen årligen i en skrivelse till riksdagen skulle redovisa tillämpningen av bestämmelserna om hemlig dataavläsning. (Se a. SOU s. 399 f.)

I beredningens utredning fanns också förslag om att hemlig dataavläsning skulle få användas som ett hemligt tvångsmedel i preventivt syfte i vissa situationer (a. SOU s. 396 ff.).

Kritik mot förslaget

Som redan nämnts framfördes kritik mot BRU:s förslag att införa hemlig dataavläsning som ett nytt tvångsmedel. Såväl beträffande behovet av tvångsmedlet och dess förväntade effektivitet som beträffande det integritetsintrång åtgärden skulle innebära restes invändningar. Därtill efterlyste ett flertal remissinstanser en samlad översyn över frågan om hemliga tvångsmedel med anledning av de många förslag som vid tiden hade förts fram. Det bör anmärkas att kritiken riktades från flera håll; såväl olika myndigheter som privata aktörer fann skäl att kritisera förslaget.

När det gällde frågan om behov och effektivitet av hemlig dataavläsning anmärktes bland annat att det saknades uppgifter om i hur många fall behov kunde tänkas uppkomma, att utredningen inte förmått visa att hemlig dataavläsning var ett oundgängligen nödvändigt medel för en effektiv brottsbekämpning och att det inte redovisades någon information om det konstaterade, faktiska behovet. Det framhölls också från flera håll att underlaget för att bedöma behovet och effektiviteten av åtgärden inte var tillräckligt. Ett antal remissinstanser anmärkte mot att delar av utredningen, såvitt avsåg effektiviteten, hade sekretessbelagts, vilket enligt dessa försvårade analysen av om tvångsmedlet som föreslogs kunde förväntas vara effektivt.

Invändningarna beträffande integritetsaspekter var av varierande karaktär. Det framhölls bland annat att integritetsintrånget skulle eller kunde bli större än vid annan tvångsmedelsanvändning. Detta t.ex. eftersom hemlig dataavläsning kunde ge de brottsbekämpande myndigheterna möjlighet att i hemlighet installera tekniska hjälpmedel i någons hem, vilket innebar dubbla intrång. Också den omständigheten att den som skyddar sin information genom kryptering signalerar att denne, av en eller annan anledning, personliga liksom kriminella, inte önskar att informationen sprids framhölls som argument för att hemlig dataavläsning innebar ett större integritetsintrång än andra hemliga tvångsmedel. Även risker för att information från tredje man, som över huvud taget inte hade med utredningen att göra, skulle läsas av anfördes; både på grund av delade nätverk och på grund av svårigheten att identifiera rätt enhet.

Det riktades vidare kritik mot den brottskatalog som föreslogs kunna föranleda åtgärden. I det sammanhanget framhölls särskilt att den danska lagstiftningen, som varit en utgångspunkt för förslaget,

var betydligt mer begränsad till misstanke om allvarliga brott än det svenska förslaget och att förslaget var allt för långtgående beträffande viss brottslighet. Även mot förslaget att åtgärden skulle kunna vidtas i syfte att fastställa vem som skäligen kunde misstänkas för brottet riktades från flera håll kritik. Detta särskilt med hänsyn till hur ingripande hemlig dataavläsning var ur ett integritetsperspektiv.

Det ifrågasattes också hur effektiv proportionalitetsprövningen skulle bli, mot bakgrund av svårigheterna för rätten och ett offentligt ombud – innan dataavläsningen inletts – att bilda sig en närmare uppfattning om förutsättningarna för verkställigheten.

4.2.2 SOU 2012:44

Utredningen om vissa hemliga tvångsmedel lämnade i juni 2012 betänkandet *Hemliga tvångsmedel mot allvarliga brott* (2012:44). I betänkandet gjordes bland annat utvärderingar av vissa tidsbegränsade lagar på området för hemliga tvångsmedel. Utredningens uppdrag innefattade inte att utreda frågan om hemlig dataavläsning. Mot bakgrund av att de brottsbekämpande myndigheterna ”med viss emfas” framhållit att det fanns ett behov av tvångsmedlet, att det borde införas och att åtgärden av den öppna polisen bedömdes som den i princip viktigaste lagstiftningsfrågan i bekämpningen av den grova organiserade brottsligheten fann utredaren skäl att ändå göra bland annat följande anmärkningar om hemlig dataavläsning (se SOU 2012:44 s. 767).

> Vid vår kartläggning har det kommit fram uppgifter om utvecklingen över tid av kommunikationsteknik och av de misstänktas strategier för att hemlighålla kommunikation. Det har framgått t.ex. att personer inom den organiserade brottsligheten numera ofta räknar […] med att hemlig teleavlyssning förekommer och ägnar stor möda åt att kommunicera utan att myndigheterna ska kunna avlyssna samtal. Krypterade telefonitjänster används. E-post används också, och det finns exempel på hur gemensamma mailkonton utnyttjas för att undgå att meddelanden sänds mellan konton. Inom Säkerhetspolisens område har den tekniska utvecklingen delvis gjort det svårare att upptäcka spioneri. Bland annat digitala krypteringsmetoder har gjort det enklare att spionera. Mångfalden av kommunikationsmedel har även gjort det möjligt för terrorister att ständigt förändra sitt sätt att kommunicera […]. Det som kommit fram vid kartläggningen ger stöd för att tvångsmedlet hemlig dataavläsning skulle kunna medföra beaktansvärd nytta för de brottsbekämpande myndigheterna. Med den utformning som BRU föreslagit

> – där avgränsningen av vilken informationsinhämtning som får ske inte är helt klar – skulle tvångsmedlet kunna medföra avsevärda integritetsintrång. Dessa intrång skulle emellertid, på samma sätt som beträffande hemlig rumsavlyssning i vissa fall kunna vara berättigade.

Utredningen konstaterade emellertid att frågan inte rymdes i dess uppdrag men påpekade vikten av att den utreds.

4.3 Vad är då hemlig dataavläsning?

4.3.1 Introduktion

Det finns, av förklarliga skäl, ingen legaldefinition av hemlig dataavläsning. Av den definition för analys som finns i våra direktiv och som vi diskuterat (och i någon mån modifierat) i avsnitt 2.3 framgår följande.

> 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 således sägas innebära två delar, nämligen dels att den brottsbekämpande myndigheten bereder sig tillgång till teknisk utrustning som kan användas för kommunikation, dels att myndighetenen tar del av uppgifter som finns i utrustningen. Vi kommer senare i betänkandet att återkomma till verkställighet av hemlig dataavläsning och då också redovisa bl.a. några olika tekniker för att bereda sig tillgång till teknisk utrustning. Det centrala här är i stället att uppgifterna som är tänkta att kommas åt med hemlig dataavläsning alltså finns i den tekniska utrustningen. Det skiljer sig från vad som är fallet vid t.ex. hemlig avlyssning eller övervakning av elektronisk kommunikation, där uppgifterna hämtas in på väg till eller från någons tekniska utrustning.

4.3.2 Begreppet hemlig dataavläsning

Utredningen har noterat ett problem med benämningen hemlig dataavläsning, nämligen att det är ett tämligen oprecist uttryck. I stort sett all hemlig tvångsmedelsanvändning sker numera i

faktisk mening genom att digitala data läses av och struktureras till information som kan bearbetas och analyseras. Detta kan illustreras med ett exempel. Det som sker vid ett vanligt mobiltelefonsamtal mellan två personer när den ene pratar och den andre uppfattar vad som sägs är (mycket förenklat) följande. Den som pratar talar in i mobiltelefonens mikrofon. Det sagda omvandlas (kodas) till digitala data som skickas till den andre. När dessa data ankommer dennes mobiltelefon kodas de till ljud som går ut i mobiltelefonens högtalare varvid den andre kan uppfatta de ord som den förste uttalat. När ett sådant samtal avlyssnas av brottsbekämpande myndigheter är det således inte det sagda utan i stället de digitala data som talet kodats till som (oftast med teleoperatörens hjälp) hämtas in. Det sker således en avläsning av data på väg till (eller från) den avlyssnade.

På motsvarande sätt förhåller det sig alltså även med övrig tvångsmedelsanvändning; metadata (exempelvis uppgifter om meddelanden eller positionering) som kan hämtas in genom hemlig övervakning av elektronisk kommunikation är således digitala data. Likaså är det inspelade från övervakningsfilmer vid hemlig kameraövervakning och ljudupptagningar från hemlig rumsavlyssning typiskt sett digitala data som tas om hand och läses av (och därefter kan spelas upp). I avsaknad av andra lämpliga begrepp använder vi trots det som nu anförts hemlig dataavläsning som arbetsnamn för det som avses betänkandet igenom.

4.3.3 Uppgifter som hemlig dataavläsning kan ge tillgång till

Oavsett vilken teknik som används skulle hemlig dataavläsning kunna ge de brottsbekämpande myndigheterna tillgång till olika typer av uppgifter, däribland sådana som redan i dag kan hämtas in genom tvångsmedelsanvändning. Med tanke på bl.a. den snabba tekniska utvecklingen, se t.ex. kapitel 6, är det vanskligt att uttala sig om vilka uppgifter som skulle kunna hämtas in med hjälp av en viss metod i framtiden. Få tänkte nog t.ex. när bestämmelsen om hemlig teleavlyssning år 1989 kom att omfatta datakommunikation att det knappt 30 år senare skulle vara möjligt att med stöd av bestämmelsen ta del av innehållet i videosamtal eller resebokningar via internet.

För att försöka illustrera vad hemlig dataavläsning skulle kunna åstadkomma har vi tagit fram en lista om tio punkter med olika typer

av uppgifter som metoden redan i dag skulle kunna ge de brottsbekämpande myndigheterna tillgång till. Listan är inte uttömmande, vissa av punkterna i den överlappar varandra och det kan dessutom alltså förväntas att ytterligare uppgifter kan bli möjliga att föra till förteckningen i takt med att den tekniska utvecklingen går fortsatt framåt. Icke desto mindre ger listan en bild av hur många olika typer av uppgifter som skulle kunna hämtas in genom hemlig dataavläsning. Följande tio punkter får således tjäna som exempel.

1. Innehållet i alla telefonsamtal (inklusive videosamtal) som den person åtgärden riktas mot deltar i, såväl vanliga mobilsamtal som via särskilda program eller appar.
2. Innehållet i samtliga e-postmeddelanden och andra direktmeddelanden som den person åtgärden riktas mot skickar och tar emot via internet.
3. Innehållet på de webbsidor som den person åtgärden riktas mot besöker samt uppgifter om hens 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 hen 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 alla samtal som den person åtgärden riktas mot deltar i, t.ex. efter aktivering av den tekniska utrustningens mikrofon.
7. Kontaktuppgifter till samtliga kontakter som finns lagrade på teknisk utrustning som åtgärden riktas mot.
8. Allt innehåll, t.ex. fotografier, dokument och andra filer, inloggningsuppgifter och program, som finns lagrat i teknisk utrustning som åtgärden riktas mot.
9. Uppgifter om lösenord, både till den tekniska utrustningen och till olika sociala nätverk, e-posttjänster samt andra forum där den person åtgärden riktas mot är aktiv.
10. Uppgifter om var, när och hur den tekniska utrustning som åtgärden riktas mot används och har använts.

Det kan noteras att de brottsbekämpande myndigheterna redan i dag kan få rättslig tillgång till många av de uppgifter som skulle kunna hämtas in genom hemlig dataavläsning. Med rättslig tillgång avses att tillstånd får lämnas som tillåter inhämtning av uppgifterna. I många fall, vilket kommer visa sig senare i betänkandet, motsvaras emellertid inte rätten att hämta in uppgifterna av en faktisk möjlighet att göra så. Exempelvis kan en allt högre grad av krypterat innehåll i internetbaserad kommunikation (t.ex. samtal och meddelanden via vanligt förekommande appar som WhatsApp, iMessage eller FaceTime på en telefon) leda till att meddelanden som de brottsbekämpande myndigheterna i och för sig har rätt att lyssna av enligt ett tillstånd till hemlig avlyssning av elektronisk kommunikation inte kan fångas upp i läsbart (eller avlyssningsbart) skick. Man kan därför tala om att myndigheterna har rättslig men inte faktisk tillgång till dessa uppgifter.[1]

Om hemlig dataavläsning alltid tilläts ge brottsbekämpande myndigheter tillgång till all den i punktlistan ovan angivna informationen samtidigt skulle åtgärden vara mycket kraftfull. I så fall skulle metoden ju innefatta åtgärder som i stora delar motsvarar hemlig avlyssning och övervakning av elektronisk kommunikation (punkterna 1–4 och 10), hemlig kameraövervakning (punkt 5), hemlig rumsavlyssning (punkt 6) och undersökningar motsvarande de som i dag kan göras vid beslag (punkterna 7–9). I många av fallen skulle metoden dessutom kunna ge mer eller precisare uppgifter än vad som är möjligt med dagens tvångsmedel. Exempelvis skulle GPS-positionering av en mobiltelefon (punkt 4) kunna ge mer exakta uppgifter om var en viss telefon befinner sig än vad sådan mastpositionering som i dag används med stöd av reglerna om hemlig övervakning av elektronisk kommunikation kan ge.

När det gäller vilka uppgifter som de brottsbekämpande myndigheterna genom hemlig dataavläsning skulle kunna få del av är det tekniken i sig som sätter begränsningarna. I teorin finns emellertid inte några begränsningar avseende vilka uppgifter i teknisk utrustning som skulle kunna hämtas in, förutsatt att rätt teknik finns. Avgörande blir i stället – om hemlig dataavläsning införs – vilka avgränsningar som införs i lagstiftningen och i tillståndsgivningen.

[1] Fenomenet har internationellt benämnts ”going dark”.

4.3.4 Varför används inte hemlig dataavläsning redan?

Frågan i rubriken kan tyckas märklig. Om hemlig dataavläsning vore tillåten hade ju denna utredning inte behövts. Samtidigt kan ju metoden för hemlig dataavläsning användas för att komma åt sådana uppgifter som får hämtas in med andra hemliga tvångsmedel. Det bör därför redan nu klargöras vilka hinder som finns i nuvarande lagstiftning för att använda metoden för hemlig dataavläsning som verkställighetsmetod för andra tvångsmedel.

Till att börja med skulle användning av metoden för hemlig dataavläsning kunna innebära ett dataintrång. Av 4 kap. 9 c § första stycket brottsbalken framgår 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 dataintrång. För dataintrång kan också den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift dömas. Straffansvar för dataintrång förutsätter således att åtgärden sker *olovligen*. Det innebär att en åtgärd som sker med samtycke eller i enlighet med gällande rätt inte är straffbar. Om tvångsmedelsreglerna ger stöd för en viss åtgärd handlar det alltså inte om dataintrång. Det finns därför skäl att närmare granska de bestämmelser och förarbeten som sätter gränserna för befintliga hemliga tvångsmedel. Vi har här valt att begränsa framställningen till vad som gäller för verkställighet av ett tillstånd till hemlig avlyssning av elektronisk kommunikation.

Enligt 27 kap. 18 § rättegångsbalken 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. Det gör emellertid 27 kap. 25 § rättegångsbalken. I det lagrummets första stycke framgår 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.

27 kap. 25 § rättegångsbalken infördes i samband med avregleringen av telemarknaden 1993 för att möjliggöra att beslut om hemlig teleavlyssning och hemlig teleövervakning skulle kunna utföras hos

enskilda företag som bedriver televerksamhet inom allmänt tillgängliga telenät. Skälet till att det krävdes en sådan bestämmelse (vilken alltså inte fanns i balken när Televerket var den enda egentliga teleoperatören på ”marknaden”) var att det enligt regeringsformen krävs lagstöd för att ålägga enskilda (dvs. teleföretagen) att medverka till verkställighet. Teleutredningen – till vilken regeringen hänvisade i propositionen (prop. 1992/93:200 s. 258 ff.) – ansåg att en bestämmelse om att ”erforderlig utrustning får anslutas, underhållas och återtas” innebar en skyldighet för enskilda att biträda och lämna tillträde för polisen. I Teleutredningens specialmotivering angavs inget ytterligare av betydelse, förutom att bestämmelsen gav den som fått tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation ”de befogenheter som behövs för att kunna verkställa åtgärderna” (SOU 1992:70 s. 345 f. och 395 f.).

Regleringen i 27 kap. 25 § rättegångsbalken kom således till som en verkställighetsregel – men inte i första hand för att klargöra för de brottsbekämpande myndigheterna hur de fick/inte fick göra utan i stället för att (direkt eller indirekt) ålägga de privata aktörer som skulle till att äntra telemarknaden att bistå de brottsbekämpande myndigheterna med sådan verkställighet.

I en lagändring några år senare gjordes bestämmelsen i 27 kap. 25 § rättegångsbalken om något. Regeringen uttalade i propositionen som föregick lagändringen (prop. 1994/95:227 s. 28 ff.) att det inte råder något tvivel om att verkställighet med hjälp av datorprogram omfattas av uttrycket ”tekniskt hjälpmedel”. För att förtydliga detta ändrades uttrycket ”anslutas, underhållas och återtas” till ”användas” (dvs. samma uttryck som fortfarande finns i bestämmelsen) eftersom ”det språkligt inte är helt lyckat att med uttrycken ’anslutas’ och ’återtas’ beskriva en verkställighet som sker genom att ett datorprogram tillförs eller modifieras respektive att avsluta en sådan verkställighet”.

Av det anförda är det således inte uteslutet, utan kanske snarare rimligt, att dra slutsatsen att teknik för hemlig dataavläsning (t.ex. installation av programvara i en telefon eller modifiering av ett datorprogram i en dator) kan vara tillåtet vid verkställighet av hemlig avlyssning eller övervakning av elektronisk kommunikation.

En sådan tolkning kan emellertid ifrågasättas eftersom förändringen snarare syftade till någonting annat än att tillåta tekniken för hemlig dataavläsning. Enligt regeringen hade den vid tiden ökade

användningen av it fört med sig att verkställigheten, i stället för att avse en inkoppling av särskilda hårdvaror, i allt högre grad behövde ske genom användning av datorprogram som styr telekommunikationerna. Det hade i det sammanhanget ifrågasatts om datorprogram innefattades i uttrycket tekniskt hjälpmedel (a. prop. s. 28). Uttalandena måste också ses i ljuset av den tid då de gjordes. I mitten av 1990-talet var de tekniska möjligheterna för teleavlyssning och teleövervakning inte så sofistikerade som de är i dag. Det innebär att uttalandena gjordes för att tydliggöra att de metoder som tidigare använts, där polisen fysiskt kopplade in sig på koppartråden som befordrade samtal och meddelanden, när det var nödvändigt kunde kompletteras med nya metoder. Ingenstans i detta sammanhang nämns dessutom t.ex. installation av programvara i den avlyssnades tekniska utrustning.

Frågan om ingrepp i enskildas datorer var emellertid i samma förarbeten uppe till diskussion, fast i ett annat sammanhang (a. prop. s. 22 ff.). Då handlade det om ifall reglerna om hemlig avlyssning och övervakning av elektronisk kommunikation även fortsättningsvis skulle begränsas till det allmänna telenätet eller om även andra nät skulle omfattas, en diskussion som uppstått på grund av att vissa, främst större, företag byggt upp egna nätverk som då undantogs från avlyssnings- och övervakningsområdet. Regeringen gjorde i det sammanhanget följande uttalande. ”Av hänsyn till informationssäkerheten och skyddet för den enskilde bör den som vidtar åtgärden t.ex. inte få göra ingrepp via telenät i de datorer m.m. som används för att befordra telemeddelanden” (a. prop. s. 25).[2]

Några andra normativa yttranden från lagstiftaren än de nu anförda har inte gjorts i detta sammanhang. Sammanfattningsvis kan således sägas att lagtexten, sådan som den är utformad i dag, i och för sig inte utesluter verkställighet av hemlig avlyssning av elektronisk kommunikation genom sådan teknik som kan användas för hemlig dataavläsning. En lagtolkning i ljuset av de förarbetsuttalanden som gjorts ger emellertid vid handen att en sådan verkställighetsåtgärd framstår som tveksam. Experterna från de brottsbekämpande myndigheterna har också förklarat att myndigheterna, vid verkställighet

[2] Trots att det citerade uttalandet gjordes i anslutning till frågor om vilka nät som skulle omfattas, en fråga som regleras i 27 kap. 20 § tredje stycket rättegångsbalken, har det i doktrin lyfts fram som motiv bakom 27 kap. 25 §. Se Fitger m.fl., Rättegångsbalken (mars 2017, Zeteo) kommentaren till 27 kap. 25 §.

av hemlig avlyssning av elektronisk kommunikation, låtit en försiktighetsprincip råda för att inte riskera att förfarandet (dvs. användning av teknik för hemlig dataavläsning) anses som dataintrång.

5 Internationell utblick

5.1 Inledning

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 när landet år 2002 införde en regel om dataaflæsning i retsplejeloven. Även Finland har lagstiftning, bland annat i tvångsmedelslagen och polislagen, som i delar motsvarar hemlig dataavläsning (såsom åtgärden definieras i utredningsdirektiven). Sedan hösten 2016 används åtgärden också i Norge, där regler om dataavlesing införts i straffeprosessloven.

I detta kapitel kommer lagstiftningen i dessa länder att beskrivas. Vi redovisar också mycket kortfattat något om hur andra länder använder motsvarande åtgärder och vad som beskrivits om åtgärdens effektivitet och nytta i internationella sammanhang.

5.2 Danmark

5.2.1 Bakgrund

Danmark är alltså det nordiska land som haft regler om hemlig dataavläsning längst. År 2002 infördes, som ett led i genomförandet av bland annat FN:s internationella konvention om bekämpande av finansiering av terrorism och FN:s säkerhetsråds resolution 1373 (2001), dataaflæsning som ett självständigt tvångsmedel i 71 kap. retsplejeloven[1].

I förarbetena till de danska reglerna om dataavläsning framgår att polisen vid tiden redan hade möjlighet att få tillstånd till telefonavlyssning enligt § 780 och hemlig rannsakan enligt § 799 och således

[1] De lagrumshänvisningar som anges i detta avsnitt är, om inte annat anges, till retsplejeloven.

redan, åtminstone rättsligt sett, kunde skaffa sig tillgång till innehållet i elektronisk kommunikation och elektroniskt lagrade uppgifter. Det konstaterades dock att det vid vissa tillfällen hade visat sig omöjligt att i praktiken skaffa sig tillgång till uppgifterna som polisen hade tillstånd att hämta in genom sådan tvångsmedelsanvändning.

I förarbetena pekades särskilt på rättsfallet Ufr 2001 s. 1276 från Højesteret. I målet, som gällde utredning beträffande misstänkt narkotikahandel, var villkoren uppfyllda både för att avlyssna e-postkommunikation från en dator i en lägenhet i ett flerbostadshus och för att ålägga danska teleföretag att upplysa om vilken kommunikationsanläggning som var i förbindelse med den datorn. Polisen hade emellertid inte teknisk möjlighet att genomföra avlyssningen eftersom installation av avlyssningsutrustningen skulle medföra stor risk för avslöjande. Dessutom var det inte möjligt för polisen att skilja den e-post som skickades från den misstänktes dator från e-post skickad av andra datoranvändare i huset. Polisen bad därför rätten om tillstånd till att installera ett s.k. ”snifferprogram” i den misstänktes dator. Med ett sådant program skulle polisen – utan att den misstänkte fick reda på det – få kopior skickade till sig av alla elektroniska meddelanden som sändes från datorn. Programmet skulle också ge möjlighet att registrera samtliga inmatningar som gjordes i datorn av användaren och det skulle registreras och vidaresändas upplysningar till polisen när datorn slogs på, vilka webbplatser som besöktes samt om dokument skapades eller redigerades m.m.

Højesteret kom fram till att det låg nära till hands att jämföra användandet av ett sådant program det var fråga om med upprepade hemliga rannsakningar, som § 799 vid den tiden inte gav möjlighet till.[2] I förarbetena till förslaget om dataavläsning slogs sedan, med hänvisning till avgörandet, fast att bestämmelsen om hemlig rannsakan inte tillåter undersökning av material i en dator genom ”løbende aflæsning, der foretages af politiet fra et andet sted”.

Det danska justitiedepartementet (Justitsministeriet) pekade på att tekniska förhållanden och risken för avslöjande innebar att polisen inte i alla situationer hade möjlighet att utnyttja den existerande möjligheten att ta del av elektroniska meddelanden och elek-

[2] I dag finns en sådan möjlighet, se avsnitt 5.2.3.

troniskt lagrat material. Justitsministeriet framhöll vidare att polisen, bland annat i ljuset av terrorangreppen i USA den 11 september 2001, kunde ha behov av att löpande kunna registrera innehållet och användandet av ”bestemte computere mv.” i samband med utredandet av allvarlig kriminalitet, till exempel genom installation av speciella programvaror, som ”sniffer-programmer”. Detta gällde enligt ministeriet särskilt vid utredningar i ärenden om vissa brott enligt danska straffeloven som till sin karaktär var sådana att de kunde ”tænkes at finde sted som led i eller i forbindelse med egentlige terrorhandlinger”. Bland de brott som angavs som exempel fanns brott enligt straffelovens kapitel om ”Forbrydelser mod statsforfatningen og de øverste statsmyndigheder, terrorisme m.v.” och ”Landsforræderi og andre forbrydelser mod statens selvstændighed og sikkerhed”.

Mot bakgrund av bland annat det anförda föreslog således Justitsministeriet genom lagförslaget om dataaflæsning att polisen i vissa situationer skulle ges möjlighet att använda ”sniffer-programmer” eller annan utrustning för att löpande kunna motta kopior av icke offentligt tillgängliga upplysningar i ett datasystem, inkluderande e-post som mottas eller skickas och uppgifter som lagras i systemets minne. Det uppmärksammades också att polisen vid användning av det föreslagna tvångsmedlet, i vissa fall, skulle få möjlighet att läsa krypterade elektroniska meddelanden (och som därför inte var möjliga att läsa i klartext vid användande av telefonavlyssning).

5.2.2 Reglerna om dataaflæsning

Sedan införandet har bestämmelsen om dataaflæsning ändrats såvitt avser vilka brott som kan föranleda åtgärden. Nuvarande lydelse i § 791 b är följande.

> Aflæsning af ikke offentligt tilgængelige oplysninger i et informationssystem ved hjælp af programmer eller andet udstyr (dataaflæsning) kan foretages, såfremt
>
> 1) der er bestemte grunde til at antage, at informationssystemet anvendes af en mistænkt i forbindelse med planlagt eller begået kriminalitet som nævnt i nr. 3,
>
> 2) indgrebet må antages at være af afgørende betydning for efterforskningen, og

> 3) efterforskningen angår en lovovertrædelse, som efter loven kan straffes med fængsel i 6 år eller derover eller en forsætlig overtrædelse af straffelovens kapitel 12 eller 13.
>
> Stk. 2. Indgreb som nævnt i stk. 1 må ikke foretages, såfremt det efter indgrebets formål, sagens betydning og den krænkelse og ulempe, som indgrebet må antages at forvolde den eller de personer, som det rammer, ville være et uforholdsmæssigt indgreb.
>
> Stk. 3. Afgørelse om dataaflæsning træffes af retten ved kendelse. I kendelsen angives det informationssystem, som indgrebet angår. I øvrigt finder reglerne i § 783, stk. 1, 3. og 4. pkt., samt stk. 3 og 4, tilsvarende anvendelse.
>
> Stk. 4. Efterfølgende underretning om et foretaget indgreb sker efter reglerne i § 788, stk. 1, 3 og 4. Underretningen gives til den, der har rådigheden over det informationssystem, der har været aflæst efter stk. 1. I øvrigt finder reglerne i § 782, stk. 2, §§ 784, 785, 789 samt 791 tilsvarende anvendelse.

Enligt bestämmelsens första stycke är det alltså ”oplysninger i et informationssystem” som kan avläsas. Med informationssystem förstås datorer eller andra databehandlingsanläggningar, t.ex. vissa mobiltelefoner och elektroniska kalendrar. Både program- och hårdvara kan användas för att genomföra avläsningen.

Kravet på vilken misstankegrad som ska föreligga framgår i första stycket första punkten i § 791 b. Bestämd grund att anta att informationssystemet används av en misstänkt i samband med en planlagd eller begången sådan handling som framgår i tredje punkten samma stycke ska således föreligga. När det gäller brottskatalogen i tredje stycket omfattar den dels brott som kan bestraffas med fängelse i sex år eller mer[3], dels uppsåtliga brott enligt kapitel 12 och 13 i straffeloven. I dessa kapitel finns bestämmelser om landsförräderi och andra brott mot Danmarks självständighet och säkerhet (kapitel 12) samt brott mot konstitutionen och de högsta myndigheterna och terroristbrott m.m.

Första styckets andra punkt innebär att dataavläsningen måste antas vara av avgörande betydelse för utredningen för att kunna tillåtas. I bestämmelsens andra stycke har proportionalitetsprincipen lagfästs.

Det är rätten som prövar och avgör om tillstånd till åtgärden ska lämnas. Detta följer av bestämmelsens tredje stycke, av vilket också

[3] Den danska lagstiftningen utgår således inte från den nedre gränsen i straffskalan, vilket varit vanligt i brottskatalogerna för hemliga tvångsmedel i Sverige, se t.ex. avsnitt 3.4.1.

framgår att rätten i sitt beslut ska ange vilket informationssystem som får avläsas. Identifieringen av informationssystemet kan ske genom att utrustningens fabrikat, identifikationsnummer eller liknande anges eller genom angivande av det geografiska ställe där utrustningen befinner sig alternativt vem som har rådigheten över den. Av hänvisningen i tredje stycket till första stycket i § 783 följer att det av beslutet ska framgå vilka konkreta omständigheter det grundas på samt att beslutet när som helst kan omprövas.

Den tid som tillstånd får meddelas för ska vara så kort som möjligt och får inte bestämmas till längre än fyra veckor. Tillståndet kan dock förlängas genom beslut av rätten med upp till fyra veckor per tillfälle. Detta följer av hänvisningen i tredje stycket i § 791 b till tredje stycket i § 783. Hänvisningen till fjärde stycket i § 783 innebär att polisen har rätt att interimistiskt besluta om dataaflæsning på samma villkor som vid hemlig rannsakan och teleavlyssning. Polisen ska, när man interimistiskt meddelat tillstånd, senast inom 24 timmar från att åtgärden (dataaflæsning) vidtas lägga fram saken för rätten som därefter har att fatta beslut om åtgärden kan godkännas och få fortsätta. Om åtgärden enligt rättens uppfattning inte borde ha företagits ska rätten informera Justitsministeriet.

Efter att avläsningen avslutats ska som utgångspunkt den domstol som fattat beslut om tillstånd underrätta den som har rådighet över det avlästa informationssystemet. En advokat som utsetts för den enskilde ska få en kopia av underrättelsen skickad till sig. Underrättelsen ska lämnas snarast möjligt, om polisen inte inom 14 dagar från att tiden för tillståndet löpte ut begärt att underrättelse ska skjutas upp eller underlåtas. En sådan begäran kan polisen framställa om en underrättelse skulle vara till skada för den aktuella utredningen eller annan utredning om en lagöverträdelse som kan medföra ”indgreb i meddelelseshemmeligheden” (t.ex. dataavläsning eller teleavlyssning), eller om hänsyn till skyddande av konfidentiella upplysningar om polisens utredningsmetoder alternativt omständigheterna i övrigt talar emot att underrättelse sker. Rätten kan besluta att underrättelse ska skjutas upp till ett senare fastställt datum (som därefter kan skjutas upp på nytt) eller helt underlåtas. Den advokat som utsetts för den enskilde ska ges möjlighet att yttra sig innan rätten beslutar i frågan. Det anförda följer av hänvisningen i bestämmelsens fjärde stycke till § 788.

Dataaflæsning får, enligt hänvisningen i fjärde stycket till andra stycket i § 782, inte ske av förbindelser mellan den misstänkte och personer som enligt § 170 inte kan avkrävas vittnesmål. De personkategorier som avses i § 170 motsvarar i allt väsentligt de som framgår av 36 kap. 5 § rättegångsbalken.

En advokat ska, enligt hänvisningen i fjärde stycket i § 791 b till §§ 784 och 785, utses för den som åtgärden vidtas mot. Reglerna om att advokat ska utses liknar de svenska bestämmelserna om offentligt ombud (27 kap. 26–30 §§ rättegångsbalken).

Överskottsinformation som framkommer vid dataavläsning får användas av polisen vid utredningen av brott. Som utgångpunkt får dock sådan information inte användas som bevis i rätten om informationen rör brott som tillståndet inte avsåg och som inte hade kunnat leda till tillstånd till något av de tvångsmedel som avses i 71 kap. retsplejeloven (som innehåller bestämmelser om bland annat dataavläsning och avlyssning). Domstolen kan emellertid medge undantag från denna huvudregel. Så får dock ske endast om andra utredningsmetoder inte skulle vara ägnade att säkra bevis om saken, det gäller brott som kan bestraffas med fängelse ett och ett halvt år eller mer samt rätten i övrigt inte finner det olämpligt. Detta följer av hänvisningen i fjärde stycket till § 789.

Av hänvisningen i bestämmelsens fjärde stycke till § 791 följer att upptagningar som gjorts vid dataaflæsning som huvudregel ska förstöras om åtal inte väcks mot någon angående det brott som låg till grund för tillståndet eller om åtal väckts men ogillats. Polisen ska underrätta den advokat som utsetts när materialet har förstörts. Avsteg från huvudregeln om förstörande av upptagningar kan meddelas av rätten, på ansökan av polisen, om materialet är av fortsatt utredningsmässig betydelse. I sådana fall kan rätten, efter hörande av advokaten, bestämma att förstörande ska underlåtas eller skjutas på framtiden till ett bestämt datum.

5.2.3 Andra relevanta danska regler

Enligt första stycket första punkten i § 780 kan polisen, på de villkor som framgår av lagens 71 kapitel avlyssna ”telefonsamtaler eller anden tilsvarende telekommunikation (telefonaflytning)”. För tillgång till avlyssning krävs att det ”er bestemte grunde til at antage, at

der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt" och att åtgärden "må antages at være af afgørende betydning for efterforskningen", se första stycket punkterna 1 och 2 i § 781. De brott som kan föranleda åtgärden är enligt tredje punkten i nyss nämnda lagrum sådana som kan bestraffas med fängelse i sex år eller mer och vissa andra, i lagen angivna, brott. Ett tillstånd till telefonaflytning avser inte bara telefonsamtal, utan också "anden tilsvarende telekommunikation", som e-post och sms. Åtgärden kan dock endast riktas mot meddelanden som är under transport mellan avsändare och mottagare. Mottagen e-post som inte öppnats hos mottagaren får polisen således tillgodogöra sig enligt reglerna om rannsakan och beslag.

Hemlig rannsakan, dvs. rannsakan med fördröjd eller underlåten underrättelse till den mot vilken åtgärden vidtas, är reglerad i § 799. Hemlig rannsakan kan beslutas av rätten om utredningen avser en "forsætlig overtredelse" av den danska straffelovens kapitel 12 (forbrytelser mot statens selvstendighet og sikkerhet) eller 13 (forbrytelser mot statsforfatningen og de øverste statsmyndigheter, terrorisme mv.), eller vissa andra allvarliga brott listade i första stycket i § 799. För att få företa hemlig rannsakan krävs att det ska vara "af afgørende betydning for efterforskningen" att rannsakan sker utan underrättelse till den misstänkte eller annan. Misstankekravet avseende den misstänkte är samma som vid vanlig rannsakan, nämligen att sådan kan ske om någon "med rimelig grund er mistænkt" för något av de brott som nämnts nyss. Enligt tredje stycket i § 799 kan rätten besluta att det, inom en viss tidsram som bestämts, får företas ett angivet antal upprepade rannsakningar eller, om det finns särskilda skäl, ett obestämt antal upprepade rannsakningar. Rannsakan enligt dansk rätt kan rikta sig mot elektroniskt lagrad information, t.ex. innehållet i ett e-postkonto eller en användarprofil på sociala medier, och uppställer inte krav på fysisk närvaro där rannsakan sker (se Højesterets kendelse af 10. maj 2012 i sag 129/2011).

5.2.4 Preventivfallen

Några särskilda regler om preventiva tvångsmedel finns inte i Danmark. Det har i tidigare utredningar anmärkts att kravet på misstankegrad för att använda hemliga tvångsmedel under förunder-

sökning är satt något lägre än i Sverige, vilket ansetts medföra att det i Danmark inte föreligger ett lika stort behov att använda sådana metoder inom ramen för underrättelseverksamhet (se SOU 2009:1 s. 82 och 2012:44).

5.3 Finland

5.3.1 Bakgrund

I Finland regleras frågor om tvångsmedelsanvändning dels i tvångsmedelslagen, dels i polislagen och lagen om brottsbekämpning inom tullen. I den förstnämnda lagen regleras tvångsmedelsanvändning under förundersökning medan det i de två senare finns regler om tvångsmedelsanvändning för att förhindra eller avslöja brott. Regelverken är förhållandevis nya men utgör i stora delar överföringar från tidigare lagstiftning, i syfte att göra systemet för tvångsmedelsanvändningen mer enhetligt.

Det finns i Finland inte något tvångsmedel som ensamt motsvarar hemlig dataavläsning enligt våra utredningsdirektivs definition. Emellertid finns några tvångsmedel som i stora delar täcker samma område och som kan ge motsvarande uppgifter som metoden för hemlig dataavläsning kan ge, utifrån hur den definierats i utredningsdirektiven. Dessa beskrivs nedan. Först ska emellertid påpekas att den finska lagstiftningstekniken på tvångsmedelsområdet enligt förarbetena strävat efter heltäckande och exakta bestämmelser för att tillgodose grundlagskraven om att all utövning av offentlig makt ska bygga på lag och att i all offentlig verksamhet ska lag noggrant iakttas. Att regleringen utvecklats på det sättet, dvs. med heltäckande och exakta bestämmelser, bedömdes vara förenat med förbättringar i den rättsliga ställningen för de personer som är föremål för myndigheternas befogenheter liksom i rättsskyddsarrangemangen (se t.ex. propositionen RP 222/2010 rd s. 392). I någon mån har utredningen dock funnit att den finska lagstiftningstekniken på området försvårar jämförelser mellan finska och svenska förhållanden.

I de lagar som reglerar tvångsmedelsanvändning har Finland lagfäst vissa grundläggande principer som ska gälla för all tvångsmedelsanvändning i landet. Bland dessa märks proportionalitetsprincipen och principen om minsta olägenhet.

I 10 kap. tvångsmedelslagen och 5 kap. polislagen anges vilka hemliga tvångsmedel[4] som får användas i Finland och förutsättningarna för att så ska få ske. De åtgärder som nämns i dessa kapitel är teleavlyssning, inhämtande av information i stället för teleavlyssning, teleövervakning, inhämtande av basstationsuppgifter, systematisk observation, förtäckt inhämtande av information, teknisk observation (innefattande teknisk avlyssning, optisk observation, teknisk spårning och teknisk observation av utrustning), inhämtande av identifieringsuppgifter för teleadresser eller teleterminalutrustning, täckoperationer, bevisprovokation genom köp, användning av informationskällor och kontrollerade leveranser. Det kan nämnas att i lagen om brottsbekämpning inom Tullen återfinns ett antal av dessa tvångsmedel, vilka får användas under vissa förutsättningar för att förhindra tullbrott. Den lagen behandlas emellertid inte vidare här.

En allmän förutsättning för att hemliga tvångsmedel ska få användas är enligt 10 kap. 2 § tvångsmedelslagen att det kan antas att man på det sättet får information som behövs för att utreda ett brott. På motsvarande sätt krävs enligt 5 kap. 2 § polislagen att man med det avsedda tvångsmedlet kan antas få information som behövs för förhindrande, avslöjande eller avvärjande av risk för brott. För samtliga hemliga tvångsmedel gäller dessutom enligt samma bestämmelser att de får användas bara om de kan antas vara av synnerlig vikt för utredning av ett brott (tvångsmedelslagen) eller för förhindrande eller avslöjande av ett brott (polislagen). Därtill gäller enligt båda lagarna att användningen av ett hemligt tvångsmedel ska avslutas inom den tid som anges i beslutet, om syftet med användningen har nåtts eller om det inte längre finns förutsättningar för att använda metoden.

I det följande beskrivs vissa av de åtgärder som i Finland kan användas som hemliga tvångsmedel. Utgångspunkten för framställningen är förundersökningsfallen, dvs. tvångsmedelsanvändningen enligt tvångsmedelslagen. I ett avslutande avsnitt beskrivs emellertid även vad som gäller för att vissa åtgärder ska få vidtas enligt polislagen. Det bör nämnas att det enligt den finska tvångsmedelslagen finns möjlighet för förundersökningsmyndigheten att genomsöka datorer, teleterminalutrustning eller andra motsvarande tekniska

[4] I den finska polislagen benämns åtgärderna enligt lagen ”hemliga metoder för inhämtande av information”. I det följande används emellertid, i syfte att underlätta läsningen, begreppet hemliga tvångsmedel för såväl åtgärder enligt tvångsmedelslagen som enligt polislagen.

anordningar eller informationssystem på distans. Eftersom detta inte utgör ett hemligt tvångsmedel kommer förutsättningarna för sådan genomsökning inte närmare att beskrivas här (se RP 222/2010 rd s. 318 f.).

5.3.2 Teleavlyssning m.m.

Med teleavlyssning avses enligt 10 kap. 3 § tvångsmedelslagen att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i reglerna om teleövervakning. Begreppet teleterminalutrustning ska enligt förarbetena förstås som utrustning för sändning, bearbetning eller mottagande av meddelanden som är avsedd att via ledning, per radio, optiskt eller på något annat elektromagnetiskt sätt vara antingen direkt kopplad till en anslutning i ett allmänt kommunikationsnät eller att fungera i anslutning till det allmänna kommunikationsnätet direkt eller indirekt kopplad till en anslutning i ett allmänt kommunikationsnät (se RP 222/2010 rd s. 327). Med meddelande avses i bestämmelsen samtal, elektronisk post, textmeddelande, talmeddelande och annat motsvarande meddelande som i ett kommunikationsnät förmedlas mellan parterna eller till en mottagarkrets som inte är utvald på förhand (ib.).

Tillstånd till åtgärden kan 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, grov ordnande av olaglig inresa, grovt häleri, och grov skadegörelse etc.) och även allvarliga brott som inte har epitetet grov i brottsbeteckningen (såsom sabotage, kapning, brott som begåtts i terroristiskt syfte och mord etc.). Det finns också möjlighet att i Finland bevilja tillstånd till hemlig teleavlyssning beträffande viss särskilt angiven grov ekonomisk brottslighet, under förutsättning att det genom brottet har eftersträvats synnerligen stor vinning och att brottet har begåtts särskilt planmässigt. Det anförda följer av 10 kap. 3 § andra-fjärde styckena tvångsmedelslagen. Beslut om teleavlyssning fattas av domstol på yrkande av en anhållnings-

berättigad tjänsteman och tillstånd kan lämnas för högst en månad åt gången (10 kap. 5 § tvångsmedelslagen).

Som ett komplement till reglerna om teleavlyssning finns i 10 kap. 4 § tvångsmedelslagen en möjlighet till tvångsmedlet inhämtande av information i stället för teleavlyssning. Denna åtgärd ger enligt bestämmelsens första stycke, om det är sannolikt att meddelanden och tillhörande identifieringsuppgifter inte längre är tillgängliga genom teleavlyssning, brottsbekämpande myndigheter möjlighet att beslagta eller kopiera dem hos ett teleföretag eller en sammanslutningsabonnent. För att så ska få ske krävs att förutsättningarna för teleavlyssning i övrigt är uppfyllda. Åtgärden kan enligt bestämmelsens andra stycke i stället riktas mot en personlig teknisk anordning som lämpar sig för att sända och ta emot meddelanden (t.ex. en Bluetooth-hörlur) och som finns i direkt anslutning till teleterminalutrustning eller mot förbindelsen mellan en sådan anordning och teleterminalutrustning. Även i den situationen krävs att förutsättningarna för teleavlyssning i övrigt är uppfyllda.

5.3.3 Teknisk avlyssning och bostadsavlyssning

Med teknisk avlyssning avses enligt 10 kap. 16 § tvångsmedelslagen att en brottsmisstänkt persons samtal eller meddelande som inte är avsett för utomstående och i vilket avlyssnaren inte deltar upptas eller behandlas på något annat sätt med hjälp av en teknisk anordning, metod eller programvara i syfte att ta reda på innehållet i samtalet eller meddelandet eller utreda deltagarna eller den misstänkta verksamheten. Förundersökningsmyndigheten får rikta teknisk avlyssning mot en person som är misstänkt för brott och befinner sig utanför ett utrymme som används för stadigvarande boende och mot en misstänkt som befinner sig i en myndighetslokal och som berövats sin frihet på grund av brott. Avlyssningen kan utföras så att den riktas mot ett utrymme eller någon annan plats som den misstänkte sannolikt kan antas befinna sig i eller på eller besöka. En förutsättning för teknisk avlyssning är att den som avlyssningen riktas mot är skäligen misstänkt för antingen ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år eller narkotikabrott, förberedelse till brott som begås i terroristiskt syfte, deltagande i utbildning för ett terroristbrott, finansiering av terrorist-

grupp eller resa i syfte att begå ett terroristbrott (om gärningen är så allvarlig att den förutsätter fängelsestraff), grovt tullredovisningsbrott, förberedelse till tagande av gisslan och förberedelse till grovt rån.

Teknisk avlyssning (då kallad bostadsavlyssning) får enligt 10 kap. 17 § tvångsmedelslagen också riktas mot ett utrymme som används för stadigvarande boende och där den som är misstänkt för brott sannolikt befinner sig om personen avlyssningen ska riktas mot är skäligen misstänkt för något av vissa, i lagen, särskilt angivna brott.

Enligt 10 kap. 18 § tvångsmedelslagen gäller att beslut om bostadsavlyssning eller teknisk avlyssning som riktas mot en misstänkt som berövats sin frihet på grund av brott ska fattas av domstolen. Övriga beslut om teknisk avlyssning kan fattas av anhållningsberättigad tjänsteman. Tillstånd kan meddelas för högst en månad åt gången.

Vid teknisk avlyssning enligt 10 kap. 16 och 17 §§ tvångsmedelslagen får de brottsbekämpande myndigheterna tillgång till att avlyssna mer än bara den misstänktes uttalanden, eller samtal med andra som befinner sig i samma rum alternativt på samma plats. I förarbetena förutsätts nämligen att teknisk avlyssning också omfattar att man ”med en teknisk anordning avlyssnar eller upptar vad den andra parten i ett telefonsamtal säger i telefonen när avlyssningen riktas mot de ljudvågor som talet ger upphov till” (RP 222/2010 rd s. 340). Uttrycket ”samtal eller meddelande” innebär att avlyssningen inte heller är begränsad till samtal eller meddelanden som sker muntligt. I förarbetena anges att teknisk avlyssning också kan omfatta t.ex. övervakning av tangentbordet till en dator i samband med sändande av e-post, se a.a.s. 340 och RP 52/2002 rd s. 27. I denna mening kan teknisk avlyssning (och bostadsavlyssning) utgöra ett i praktiken viktigt komplement till teleavlyssning och inhämtande av information i stället för teleavlyssning när syftet med avlyssningen är att avslöja innehållet i den misstänktes kommunikation. I nyss nämnda förarbeten från 2002 klargjorde den finska regeringen i viss mening gränsdragningen mellan teknisk avlyssning och teleavlyssning samt förklarade varför behovet av utvidgad teknisk avlyssning hade uppkommit (RP 52/2002 rd s. 26 f.) enligt följande.

> Det ökade behovet av att kunna rikta teknisk avlyssning mot utrymmen som är avsedda för stadigvarande boende beror på att teleavlyssningens användbarhet vid utredningen de facto har minskat. När brottslingarna i allt högre grad blir medvetna om risken för att bli avslöjad i samband med telekommunikation kommer de att försöka undvika telekom-

munikation. Också den ovan nämnda användningen av mobiltelefoner och anonymt förhandsbetalda teleanslutningar samt ibruktagandet av kryptoteknik försvårar teleavlyssningen. Det enda sättet att ta sig förbi krypteringsarrangemangen kan i praktiken vara att utföra teleavlyssningen vid en teleterminalutrustning. Eftersom det allmänna telenätet anses upphöra vid den s.k. husfördelningen, är det i de kopplingar som görs vid teleterminalutrustningen inte fråga om teleavlyssning utan om teknisk avlyssning.

Det är med andra ord möjligt att rikta åtgärden mot t.ex. kommunikationsutrustning i syfte att fånga upp samtal eller meddelande. Vid sådan teknisk avlyssning kan åtgärden riktas inte bara mot utrustning som ägs av den misstänkte utan också mot en dator eller liknande utrustning som den misstänkte sannolikt använder.

5.3.4 Teknisk observation av utrustning

Med teknisk observation av utrustning avses enligt 10 kap. 23 § tvångsmedelslagen att en funktion, informationsinnehållet eller identifieringsuppgifterna i en dator eller i en liknande teknisk anordning eller i dess programvara på något annat sätt än enbart genom sinnesförnimmelser observeras, upptas eller behandlas på något annat sätt för att utreda omständigheter som är av betydelse för utredningen av ett brott.

Enligt förarbetena (RP 222/2010 rd s. 346) kan åtgärden användas för att observera en teknisk anordning och uppgifter i anordningen som den som är misstänkt för ett brott har lagrat där. Sådana uppgifter kan t.ex. finnas i en handling som är lagrad i anordningen. Genom teknisk observation av utrustning kan man också övervaka växelverkan mellan den brottsmisstänkte och den tekniska anordningen och inhämta identifieringsuppgifter för anordningar eller dess programvara samt information om signal- eller styrtrafik som inte hänför sig till meddelandet. En form av teknisk observation av utrustning ska vidare vara s.k. tangetbordsavlyssning, vars syfte är t.ex. att få reda på innehållet i lösenordet till en server. Åtgärden ska vara av huvudsakligen teknisk karaktär men information om innehållet i ett meddelande eller om identifieringsuppgifter får inte inhämtas med åtgärden, eftersom det då är fråga om teknisk avlyssning.

Teknisk observation av utrustning får riktas mot en dator eller en liknande teknisk anordning eller dess programvara som en person som är misstänkt för brott sannolikt använder, om personen är skäligen misstänkt för ett sådant brott som kan föranleda teknisk avlyssning enligt 10 kap. 16 § tvångsmedelslagen (se ovan). Beslut om teknisk observation av utrustning ska enligt 10 kap. 24 § tvångsmedelslagen fattas av domstolen på yrkande av en anhållningsberättigad tjänsteman. Om ärendet inte tål uppskov, får en anhållningsberättigad tjänsteman besluta om sådan observation till dess att domstol har avgjort yrkandet om beviljande av tillstånd. Ärendet ska föras till domstol så snart det är möjligt, dock senast 24 timmar efter det att tvångsmedlet började användas. Tillstånd kan lämnas för högst en månad åt gången.

Bestämmelsen om teknisk observation av utrustning kom enligt förarbetena till bl.a. för att förundersökningsmyndigheten enligt de tidigare gällande reglerna inte kunde vara säker på var en anordning användes, i och med att olika slags bärbara anordningar och andra anordningar som man kan ha med sig blivit så vanliga. Därtill fann den finska regeringen att den plats där anordningen används inte ska vara av någon betydelse vid teknisk observation av utrustning, eftersom syftet med befogenheten inte är att utreda vad som sker på den plats där anordningen finns (RP 222/2010 rd s. 346). En jämförelse kan i sammanhanget göras med reglerna om teknisk avlyssning. Enligt de bestämmelserna krävs att brottbekämpande myndigheter anger var, dvs. vilken plats, avlyssningen ska ske på.

Installation och avinstallation av anordningar, metoder eller programvara

I en särskild bestämmelse (10 kap. 26 §) i den finska tvångsmedelslagen ges vissa instruktioner om installation och avinstallation av anordningar, metoder och programvara. Där anges att en förundersökningstjänsteman har rätt att fästa en anordning, metod eller programvara som används för teknisk observation på föremål, ämnen, egendom, i utrymmen och andra platser eller informationssystem som åtgärden riktas mot, om det behövs för observationen. För att installera, ta i bruk och avinstallera anordningen, metoden eller programvaran har förundersökningstjänstemannen då rätt att i hemlighet ta sig in i ett ovan nämnt utrymme eller på en ovan

nämnd plats eller i ett ovan nämnt informationssystem samt att kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektens eller informationssystemens säkerhetssystem.

När bestämmelsen infördes angavs i förarbetena bl.a. att det i förhållande till den då gällande lagen innebar en utvidgning att, för att säkerställa installationen, ibruktagandet eller avinstallationen, man ska kunna kringgå, låsa upp eller på något annat motsvarande sätt tillfälligt passera eller störa objektets eller informationssystemets säkerhetssystem. Det ansågs därför viktigt att det uttryckligen framgick av lagen. Enligt den finska lagstiftaren skulle de möjligheter som utvidgningen innebar anses jämförliga med att man öppnar ett lås (i fysisk miljö), se RP 222/2010 rd s. 348.

5.3.5 Vissa rättssäkerhetsgarantier i den finska lagstiftningen

Liksom i rättegångsbalken föreskrivs i den finska tvångsmedelslagen att vissa särskilda rättssäkerhetsgarantier ska gälla, generellt eller i särskilda avseenden. Av dessa framgår bl.a. följande.

- Offentligt ombud ska användas i ärenden som gäller bostadsavlyssning (10 kap. 44 §).
- I vissa fall råder avlyssningsförbud (10 kap. 52 §).
- Granskning av upptagningar och handlingar ska ske utan ogrundat dröjsmål (10 kap. 53 §).
- Överskottsinformation får alltid användas för att förhindra brott och för att rikta in polisen och Tullens verksamhet och som en utredning som stöder att någon är oskyldig. Den får också alltid användas för att förhindra betydande fara för någons liv, hälsa eller frihet eller betydande miljö-, egendoms- eller förmögenhetsskada. Härutöver är det särskilt föreskrivet i vilka fall överskottsinformation får användas, särskilt såvitt avser utredande av brott. Det är också särskilt föreskrivet om utplåning av överskottsinformation (10 kap. 55–57).
- Avbrytande av åtgärd ska omedelbart ske bl.a. om det visar sig att den riktas mot fel person eller utrymme eller utrustning som den misstänkte inte använder (10 kap. 58 §).

– En misstänkt som varit föremål för åtgärd ska utan dröjsmål underrättas om detta skriftligen när ärendet har förts till åklagaren för prövning eller förundersökningen annars har avslutats eller avbrutits. Den misstänkte ska dock underrättas om ett tvångsmedel senast ett år efter det att användningen av det har avslutats. Vissa undantag finns, t.ex. avseende uppskjutande av underrättelse och underlåtelse att underrätta om det är nödvändigt för att trygga statens säkerhet eller skydda liv eller hälsa (10 kap. 60 §).

5.3.6 Preventivfallen

Som redan har nämnts är det i polislagen som användningen av hemliga tvångsmedel i Finland regleras när det gäller sådana åtgärder i syfte att antingen förhindra eller avslöja brott. Med förhindra brott avses enligt 5 kap. 1 § polislagen åtgärder som syftar till att förhindra brott, försök till brott och förberedelse till brott, när det utifrån iakttagelser av en persons verksamhet eller utifrån annan information om en persons verksamhet finns grundad anledning att anta att personen i fråga kommer att göra sig skyldig till brott, samt åtgärder som syftar till att avbryta ett redan påbörjat brott eller begränsa den direkta skada eller fara som brottet medför. Med avslöjande av brott avses enligt samma bestämmelse åtgärder som syftar till att klarlägga om det för inledande av förundersökning finns en avsedd grund, när det utifrån iakttagelser av en persons verksamhet eller utifrån annan information om en persons verksamhet kan antas att ett brott har begåtts.

Definitionerna av åtgärderna teleavlyssning, teknisk avlyssning och teknisk observation av utrustning enligt polislagen är i allt väsentligt desamma som enligt tvångsmedelslagen, se under respektive rubrik ovan. När det gäller möjligheten att vidta hemliga tvångsmedel för avslöjande av brott finns en brottskatalog som gäller för samtliga hemliga tvångsmedel enligt polislagen. För förhindrande av brott framgår i stället vid respektive bestämmelse vilka förutsättningar som måste vara uppfyllda för att tvångsmedlet ska få användas.

De hemliga tvångsmedel som nämns i polislagen får enligt brottskatalogen i 5 kap. 3 § användas för att *avslöja* något av brotten äventyrande av Finlands suveränitet, krigsanstiftan, landsförräderi, grovt

landsförräderi, spionerі, grovt spionerі, röjande av statshemlighet, olovlig underrättelseverksamhet, brott enligt 34 a kap. 1 § 1 mom. 2–7 punkten eller 2 mom. i strafflagen som begås i terroristiskt syfte (bland annat mord, dråp, grov misshandel), förberedelse till brott som begås i terroristiskt syfte, ledande av terroristgrupp, främjande av en terroristgrupps verksamhet, meddelande av utbildning för ett terroristbrott, deltagande i utbildning för ett terroristbrott, om gärningen är så allvarlig att den förutsätter fängelsestraff, rekrytering för ett terroristbrott, finansiering av terrorism samt finansiering av terroristgrupp, om gärningen är så allvarlig att den förutsätter fängelsestraff.

Vid *förhindrande* av brott är en grundläggande förutsättning för all hemlig tvångsmedelsanvändning att den som åtgärden ska riktas mot, på grund av sina yttranden eller hotelser eller sitt uppträdande, med fog kan antas göra sig skyldig till något av de brott som framgår i respektive bestämmelses brottskatalog. De brott som framgår av brottskatalogen för teleavlyssning och inhämtande av information i stället för teleavlyssning är, för att åtgärden ska kunna tillåtas för förhindrande av brott, desamma som nyss nämnts för avslöjande av brott (5 kap. 5 och 6 §§ polislagen). Polisen kan dessutom, enligt 5 kap. 5 § andra stycket, beviljas tillstånd till teleavlyssning, om det är nödvändigt för att avvärja en allvarlig fara som omedelbart hotar liv eller hälsa.

För att teknisk avlyssning eller teknisk observation av utrustning ska kunna tillgripas ska det i stället handla om ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år, narkotikabrott, förberedelse till brott som begås i terroristiskt syfte, eller deltagande i utbildning för ett terroristbrott eller finansiering av terroristgrupp om gärningen är så allvarlig att den förutsätter fängelsestraff alternativt grovt tullredovisningsbrott (5 kap. 17 och 23 §§ polislagen). Beträffande teknisk avlyssning gäller enligt 5 kap. 17 § tredje stycket, att polisen alltid har rätt att utföra teknisk avlyssning, om det är nödvändigt för att en polisåtgärd tryggt ska kunna vidtas eller sådan överhängande fara avvärjas som hotar den persons liv eller hälsa som vidtar åtgärden eller den persons liv eller hälsa som ska gripas eller skyddas. I dessa fall gäller således inte förbudet mot teknisk avlyssning riktad mot utrymmen som används för stadigvarande boende. För teknisk observation av utrustning finns ingen motsvarande regel. Åtgärden får bara riktas mot en dator eller en lik-

nande teknisk anordning som personen i fråga sannolikt använder, eller mot dess programvara.

Beträffande samtliga nu nämnda tvångsmedel, utom teknisk avlyssning, gäller att domstol beslutar i fråga om tillstånd efter ansökan av anhållningsberättigad polisman. Teknisk avlyssning får beslutas av anhållningsberättigad polisman direkt, om avlyssningen inte riktas mot en person som berövats sin frihet på grund av brott. I det senare fallet gäller att domstol ska fatta beslut. I samtliga fall kan tillstånd ges för högst en månad åt gången.

5.4 Norge

5.4.1 Allmänt

I Norge har frågan om dataavläsning varit diskuterad i olika sammanhang under i vart fall de senaste tjugo åren. Redan i förarbeten om ”kommunikasjonsavlytting” (se beskrivning av detta tvångsmedel nedan) från 1998 pekades på att polisen med dåvarande tvångsmedel inte hade möjlighet att tillägna sig information på en dator som varken lagras eller kommuniceras. I detta sammanhang uttalades bland annat följande (varvid dataavläsning kallades ”trojanske hester”), se Ot.prp. nr. 64 [1998–99] punkt 23 IV s. 156 f.

> Det har i denne forbindelse vært reist spørsmål om bruken av såkalte trojanske hester. Dette er dataprogrammer som skjuler seg inne i andre, tilsynelatende nyttige programmer eller dokumenter. Det finnes slike programmer som er laget nettopp med tanke på etterforskning. Disse installeres på den mistenktes maskin når mistenkte åpner en e-post melding han får tilsendt. Mistenkte vil ikke kunne merke at programmet blir installert. Når programmet er installert, vil det registrere all aktivitet på maskinen i en logg, som med jevne mellomrom overføres til politiet via e-post. Heller ikke dette vil den mistenkte kunne oppdage.

Uttalandena i propositionen, som visserligen tog sikte på användning av dataprogram för att registrera all aktivitet på en misstänkts dator och således inte utgjorde ett konkret ställningstagande kring huruvida sådana program kunde användas vid målinriktad avlyssning av uppgifter som kommuniceras, har i Norge tolkats som att verkställighetsmetoder som involverar hemliga ingrepp i en misstänkts dator ligger klart utanför vad som är tillåtet inom ramen för kommunikasjonsavlytting (se prop. 68 L [2015–2016] s. 226).

Mot bakgrund av bland annat det föregående har frågan om hemlig dataavläsning, som i Norge kallas dataavlesing, levt vidare. Metoden har därefter i olika sammanhang och som delvis olika metoder framhållits som önskvärd, se t.ex. majoritetens uppfattning i NOU 2004:6 s. 206 f. (där dataavlesing föreslogs som ett nytt tvångsmedel) och NOU 2009:15 s. 245 (där Metodekontrollutvalget föreslog dataavlesing som en verkställighetsmetod för redan existerande hemliga tvångsmedel).

I prop. 68 L (2015–2016), som tog avstamp i Metodekontrollutvalgets utredning, lades ett lagförlag om att dataavläsning skulle införas som ett nytt tvångsmedel fram. Lagen, som innebar införande av det nya kapitel 16 d i straffeprosessloven[5], antogs av Storetinget den 17 juni 2016 och trädde i kraft den 9 september 2016.

5.4.2 Reglerna om dataavlesing

Bestämmelserna om dataavlesing i §§ 216 o och p har följande lydelser.

> **§ 216 o.** Retten kan ved kjennelse gi politiet tillatelse til å foreta avlesing av ikke offentlig tilgjengelige opplysninger i et datasystem (dataavlesing) når noen med skjellig grunn mistenkes for en handling eller forsøk på en handling
>
> a) som etter loven kan medføre straff av fengsel i 10 år eller mer
>
> b) som rammes av straffeloven §§ 121, 123, 125, 126, 127 jf. 123, 128 første punktum, 129, 136, 136 a, 232, 254, 257, 311, 333, 337 jf. 231, eller 340 jf. 231, eller av lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v. § 5 eller av lov om utlendingers adgang til riket og deres opphold her § 108 femte ledd.
>
> Dataavlesing kan besluttes selv om straff ikke kan idømmes på grunn av bestemmelsene i straffeloven § 20 første ledd. Det gjelder også når tilstanden har medført at den mistenkte ikke har utvist skyld.
>
> Tillatelse etter første ledd kan bare gis dersom det må antas at dataavlesing vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort. § 216 c annet ledd gjelder tilsvarende.
>
> Det kan bare gis tillatelse til å avlese bestemte datasystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester som den mistenkte besitter eller kan antas å ville bruke. Avlesingen kan omfatte kommunikasjon, elektronisk lagrede data og andre opplysninger om bruk av datasystemet eller brukerkontoen.

[5] De lagrumshänvisningar som anges i detta avsnitt är, om inte annat anges, till straffeprosessloven.

> §§ 216 d til 216 k gjelder tilsvarende, likevel slik at rettens tillatelse ikke kan gis for mer enn to uker om gangen. Eventuelt utstyr som er benyttet for å gjennomføre dataavlesingen skal fjernes snarest mulig etter avlesingsperiodens utløp.
>
> **§ 216 p.** Dataavlesing etter § 216 o kan bare utføres av personell som er særlig skikket til det og som utpekes av politimesteren, sjef PST eller den som bemyndiges. Avlesingen kan foretas ved hjelp av tekniske innretninger, dataprogram eller på annen måte. § 199 a gjelder tilsvarende. Politiet kan bryte eller omgå beskyttelse i datasystemet dersom det er nødvendig for å kunne gjennomføre avlesingen. Tekniske innretninger og dataprogram kan installeres i datasystemet og i annen maskinvare som kan knyttes til datasystemet. Når retten ikke bestemmer noe annet, kan politiet også foreta innbrudd for å plassere eller fjerne tekniske innretninger eller dataprogram som er nødvendig for å gjennomføre dataavlesingen.
>
> Dataavlesingen skal innrettes slik at det ikke unødig fanges opp opplysninger om andre enn mistenktes bruk av datasystemet. Avlesingen skal utføres slik at det ikke unødig voldes fare for driftshindring eller for skade på utrustning eller data. Politiet skal så vidt mulig avverge fare for at noen som følge av gjennomføringen settes i stand til å skaffe seg uberettiget tilgang til datasystemet eller vernet informasjon eller til å begå andre straffbare handlinger.

Begreppet ”datasystem” bygger på följande definition av ”computer system” i artikel 1 a. i Europarådets konvention om IT-relaterad brottslighet.[6]

> Computer system means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

Som exempel på sådan utrustning som avses anförde den norska regeringen smarttelefoner, datorer och annan utrustning för elektronisk kommunikation som utför behandling av data med hjälp av dataprogram (se prop. 68 L [2015–2016] s. 270). Den gemensamma nämnaren för de användarkonton (brukerkontoer) som avses i bestämmelsen är att det genom användarnamn och lösenord (eller liknande uppgifter) är möjligt att från olika fysiska enheter få tillgång till informationen som är kopplad kontot. Om polisens tillgång till dataavläsning inte skulle kunna riktas mot dylika konton utan endast mot fysisk utrustning skulle, enligt de norska förarbetena,

[6] Europarådets konvention om it-relaterad brottslighet (ETS nr 185), se vidare om konventionen i kapitel 11.

kontrollen genom dataavläsning kunna bli ineffektiv när den misstänkte använde olika enheter för att ta del av informationen på användarkontot. Dessutom framhölls att avläsning som begränsar sig till ett sådant konto kan vara mindre ingripande än t.ex. avläsning av all information på en dator (ib.).

Enligt fjärde stycket i § 216 o gäller att tillstånd endast ska kunna avse ”bestemte datassystemer eller brukerkontoer til nettverksbaserte kommunikasjons- og lagringstjenester”. I begreppet bestemte ligger enligt förarbetena ett krav på att datasystemet eller användarkontot som ska avläsas måste identifieras både i ansökan och i beslut. Om det aktuella datasystemet är en mobiltelefon kommer exempelvis telefonens IMEI-nummer kunna användas för identifiering och är det ett användarkonto kan detta identifieras genom användarnamn eller e-postadress (när det är fråga om ett e-postkonto). Identifiering kan också ske genom att utrustningens fabrikat anges eller genom angivande av det ställe där utrustningen befinner sig och vem som har rådigheten över den (ib.).

Att dataavläsning bara ska kunna riktas mot datasystem som den misstänkte ”besitter eller kan antas å ville bruke” framgår av § 216 o fjärde stycket. Med ”bruke” avses det direkta användandet av en dator, smarttelefon eller annan utrustning. Endast utrustning eller användarkonton som den misstänkte använder eller kan antas använda får avläsas (a. prop. s. 270 f.)

Ett tillstånd till dataavlesing som innebär rätt till avläsning av ett ”datasystem”, t.ex. en dator, ger möjlighet att avläsa all information som finns tillgänglig genom datorn oavsett om informationen är lagrad i den eller på annat ställe. Samma sak gäller vid avläsning av ett bestämt användarkonto. Däremot ger det inte tillgång till att företa direkt avläsning av exempelvis en server hos tjänsteleverantören eller liknande, som den misstänkte ju bara indirekt använder (a. prop. s. 271).

När det gäller vilka brott som kan aktualisera dataavläsning i Norge gäller enligt första stycket i § 216 o som utgångspunkt att brottet enligt lagen ska kunna medföra, dvs. maxstraffet för brottet ska vara, fängelse i tio år eller mer (punkt a). Därtill anges särskilt vissa övriga brott där maxstraffet för brotten inte överstiger fängelse i tio år. Bland dessa finns brott avseende rikets säkerhet, narkotikabrottslighet, människohandel, grovt häleri och penningtvättbrott (punkt b). För att tillstånd ska kunna meddelas måste en person”

med skjellig grunn" kunna misstänkas för en sådan handling eller försök till sådan handling som avses i bestämmelsen. Kravet innebär enligt förarbetena att rätten måste anse det mer sannolikt att den som åtgärden ska riktas mot har begått eller försökt begå en sådan handling, än att så inte är fallet. Det måste alltså föreligga sannolikhetsövervikt, vilket enligt den norska regeringens uppfattning reducerar risken för att tvångsmedlet kommer att riktas mot personer som inte kan kopplas till kriminella handlingar (a. prop. s. 269). Liksom vid all tvångsmedelsanvändning i Norge gäller proportionalitetsprincipen, vilken är lagfäst i § 170 a. Det påpekades särskilt i förarbetena att principen får särskild betydelse i de fall tillstånd till dataavläsning begärs för brott som har väsentligt lägre straffmaximum än tio år (ib.)

Bestämmelsen i tredje stycket i § 216 o innebär en påminnelse om att dataavläsning bara ska tillåtas när det finns ett reellt behov för sådan tvångsmedelsanvändning, t.ex. för att det kan antas att mindre ingripande utredningsmetoder inte kommer att ge resultat. Det innebär emellertid inte att andra tvångsmedel måste ha prövats (och misslyckats) innan dataavläsning får tas till. I stället ska de konkreta omständigheterna i varje enskilt ärende beaktas och utifrån dessa ska det avgöras om dataavläsning i det enskilda fallet är en mer eller mindre ingripande metod än t.ex. kommunikasjonsavlytting. För att det inte ska vara omöjligt för rätten att ta ställning till frågan om samma resultat skulle kunna uppnås med en mindre ingripande metod ska åklagaren vid ansökan lämna information i detta avseende, så att rätten kan göra en reell prövning av behovet av åtgärden. Även i detta sammanhang gäller proportionalitetsprincipen. Det innebär givetvis att även om övriga förutsättningar är uppfyllda så får inte dataavläsning tillåtas om åtgärden skulle anses oproportionerlig, vilket enligt den norska regeringen tillgodoser kravet enligt artikel 8 i Europakonventionen (ib.). Hänvisningen i tredje stycket i § 216 o till andra stycket i § 216 c innebär att tillstånd till avläsning av datasystem som är tillgängligt för ett större antal personer får lämnas bara när det föreligger särskilda skäl. Samma sak gäller när datasystemet tillhör advokat, läkare, präst eller andra som använder datasystemet för att behandla information av mycket förtrolig karaktär, eller som tillhör redaktör eller journalist, såvida inte någon av de nu anförda själv är misstänkt (ib.).

Betydelsen av andra stycket i § 216 o är att tillstånd till dataavläsning får meddelas även i de fall där den misstänkte inte är tillräknelig, på grund av underårighet, psykos, avsevärd utvecklingsstörning eller svåra medvetanderubbningar, och därför inte kan ådömas straffansvar. Detta gäller även när ett sådant förhållande har medfört att den misstänkte inte kan utvisa skuld.

Av hänvisningarna i sista stycket i § 216 o följer bland annat i vilka situationer ett interimistiskt beslut får fattas och fristerna för att ställa ett sådant beslut inför rättens prövning, förutsättningarna för underrättelse till den enskilde, när avläsning ska avbrytas och hur överskottsinformation ska behandlas. I samma stycke framgår också att tiden för tillstånd till dataavläsning inte får överstiga två veckor per gång och att utrustning som använts vid åtgärden ska avlägsnas snarast möjligt efter avläsningsperiodens slut.

När det gäller verkställigheten av dataavlesing uppställs för det första vissa krav på att den som ska ansvara för avläsningen är särskilt lämpad för detta (se § 216 p första stycket första meningen). Enligt den norska regeringen finns detta krav dels för att det ska bli fråga om en så effektiv verkställighet som möjligt, dels för att förebygga och minska risken för skada på eller missbruk av de system som avläses (a. prop. s. 272).

Vidare gäller att åtgärden kan vidtas med hjälp av tekniska inrättningar, dataprogram (som kan installeras såväl i datasystemet eller i maskinvara som kan kopplas till systemet, t.ex. tangentbord, headset eller USB-minne) eller på annat sätt (§ 216 p första stycket). I dessa delar syftar bestämmelsen till att ge polisen förhållandevis stor frihet att välja val av metod vid verkställighet (a. prop. s. 271).

Polisen har, genom hänvisningen i § 216 p första stycket till § 199 a, rätt att ålägga den som befattar sig med ett system som ska avläsas att denne ska lämna nödvändiga upplysningar för att polisen ska få tillgång till systemet. Ytterligare en möjlighet för polisen att få tillgång till systemet är att begå dataintrång, vilket också är tillåtet enligt första stycket. Även fysiska intrång kan vara tillåtna enligt bestämmelsen. Detta kan enligt den norska regeringen vara särskilt viktigt när utrustningen befinner sig i ett låst utrymme och det inte synes möjligt att genomföra avläsningen via nät (ib.). Begränsningarna när det gäller fysiskt intrång är att sådant får ske när rätten inte bestämmer något annat och att utrustningen ska vara nödvändig för att genomföra avläsningen. Det senare kravet innebär enligt för-

arbetena att rätten inte bör ge polisen tillstånd att företa fysiskt intrång om åtgärden kan genomföras på annat tillfredsställande sätt, som inte kräver sådant intrång. Också proportionalitetsaspekter ska givetvis beaktas vid denna bedömning (a. prop. s. 271 f.).

I andra stycket i § 216 p finns regler som ska skydda såväl den som avläsningen riktas mot som tredje man. Enligt bestämmelsen gäller bland annat att polisen är skyldig att se till att det inte onödigtvis genom avläsningen vållas fara eller driftstörning i systemet som avläses. I detta ligger enligt förarbetena att polisen i valet mellan olika metoder kan vara skyldig att välja en mer omständlig metod om det minskar risk för skada eller driftstörning (a. prop. s. 272). Polisen är också enligt bestämmelsen skyldig att inrikta avläsningen så att det inte i onödan fångas upp information om andra än misstänkts bruk av systemet som avläses, vilket enligt den norska regeringen är tänkt som ett integritetsskydd för t.ex. familjemedlemmar som använder samma nätverk som den misstänkte (ib.).

Det bör avslutningsvis nämnas att den norska regeringen ansåg att det inte i lagtext var möjligt att beskriva verkställighetsmetoden i detalj (bland annat med hänsyn till de olika tekniska möjligheter som finns och att dessa kan förväntas förändras över tid). I sammanhanget framhölls emellertid att bestämmelserna om tvångsmedlet utgör dess yttersta gränser. Ett tillstånd till dataavläsning ger därmed inte brottsbekämpande myndigheter tillåtelse att manipulera det datasystem som avläses för att använda andra former av hemliga tvångsmedel. Således är det inte tillåtet för polisen inom ramen för ett tillstånd till dataavläsning att t.ex. aktivera en mikrofon eller kamera på en dator för att på så vis få tillgång till ljud eller bild från den plats datorn befinner sig. Avlyssning eller övervakning på det sättet ryms i stället inom reglerna om hemlig rumsavlyssning eller hemlig kameraövervakning och kräver tillstånd enligt dessa bestämmelser (a. prop. s. 264).

5.4.3 Andra relevanta norska regler

Som nämnts finns bestämmelser om kommunikasjonsavlytting i Norge. Åtgärden, som regleras i § 216 a, motsvarar väsentligen det svenska tvångsmedlet hemlig avlyssning av elektronisk kommunikation. Kommunikasjonsavlytting kan bestå i att avlyssna samtal

eller annan kommunikation till och från bestämda telefoner, datorer eller annan kommunikationsutrustning som den misstänkte besitter eller ”kan antas å ville bruke”. Som kommunikasjonsavlytting räknas emellertid också identifiering av kommunikationsanläggning med hjälp av teknisk utrustning som sker genom att samtal eller annan kommunikation avlyssnas. Metoden – som ofta kallas ”temporärmassavlyssning” – innebär att polisen under en bestämd period avlyssnar all kommunikation i ett område där en misstänkt antas befinna sig. Avlyssningen genomförs för att fastställa identiteten, t.ex. IMEI-nummer, på kommunikationsutrustning som den misstänkte använder. Tvångsmedlet kan användas med sikte på en senare begäran om ordinär avlyssning men också för att senare kunna använda andra utredningsåtgärder, såsom ”begjæring om innsyn i abonnementsopplysninger” (se prop. 68 L [2015–2016] s. 87). Det krävs att någon med ”skjellig grunn” kan misstänkas för ett brott eller försök till ett brott som kan föranleda fängelse i tio år eller mer, alternativt något av de brott som är särskilt uppräknade (i huvudsak samma som för dataavlesing) för att kommunikasjonsavlytting ska få tillåtas.

Liksom i Danmark finns i Norge möjlighet till hemlig rannsakan. Enligt § 200 a kan nämligen rätten besluta att en rannsakan får ske utan att den mot vilken åtgärden vidtas underrättas om det. Tillstånd till hemlig rannsakan får bara lämnas när åtgärden kan antas vara av väsentlig betydelse för utredningen och uppklarning annars i väsentlig grad skulle försvåras samt när det inte är en oproportionerlig åtgärd med hänsyn till ärendets art och övriga omständigheter. Beslutet om hemlig rannsakan gäller också information som finns lagrad elektroniskt i ett informationssystem, t.ex. på hårddisken i en dator. Ett annat exempel är rannsakan av virtuella användarkonton, t.ex. ett e-postkonto eller annan lagringstjänst där innehållet lagras på en extern server. I sådana fall genomförs polisens rannsakan nödvändigtvis utan fysisk närvaro (a. prop. s. 226).

För de hemliga tvångsmedlen kommunikasjonskontroll, romavlytting (rumsavlyssning) och dataavlesing finns särskilda bestämmelser i en författning som på normhierarkisk nivå motsvarar en svensk förordning.[7] I den regleras bl.a. när åklagare (Påtalemyndigheten) får meddela interimistiskt beslut och vilka uppgifter som ska

[7] Forskrift om kommunikasjonskontroll, romavlytting og dataavlesing.

antecknas i protokoll över verkställigheten. Utöver sådana uppgifter som ska antecknas vid alla de tre nämnda tvångsmedlen (t.ex. skälen för tvångsmedelsanvändningen) ska vissa uppgifter särskilt antecknas vid dataavlesing. Dessa uppgifter är följande.

1. Vilka typer av data som har lästs av, t.ex. e-post, textfiler, bilder, filmer, krypteringslösningar och lösenord.
2. När tekniskt hjälpmedel som har använts har placerats och avlägsnats.
3. Vilken typ av tekniskt hjälpmedel som har använts.
4. Om det har gjorts ett fysiskt intrång för att genomföra dataavlesingen.
5. Om polisen har brutit eller kringgått skydd i datasystemet.
6. Vilka risker datasystemet har varit utsatt för vid dataavlesingen, och information om vad som har gjorts för att avvärja fara for driftshindrande eller för skada på utrustning eller data, samt fara för att någon som en följd av genomförandet kan skaffa sig oberättigad tillgång till datasystemet eller skyddad information.
7. Eventuella kända skador som dataavläsningen har orsakat datasystemet.
8. Vilken personal som har utfört dataavlesingen.

5.4.4 Preventivfallen

Enligt § 222 d kan polisen som ett led i en utredning, när det finns rimlig grund att tro att någon kommer att begå vissa särskilt angivna brott, få tillstånd att använda exempelvis hemlig rannsakan, kommunikasjonsavlytting eller dataavlesing. De brott som kan föranleda sådan åtgärd är terroristbrott, terrorhot, mord, grovt narkotikabrott som omfattar en betydande mängd narkotika och grovt rån om brottet är ett led i en kriminell organisations verksamhet.

Enligt samma bestämmelse kan Politiets sikkerhetstjeneste (PST) ges motsvarande tillstånd som ett led i en utredning när det finns rimlig grund att tro att någon kommer att begå vissa i lagen särskilt angivna brott. Bland de brott som här avses finns i huvudsak

allmänfarliga brott och brott mot staten såsom kränkning av Norges självständighet och frihet, kränkning av Norges konstitution, angrepp på de högsta organens verksamhet, angrepp på viktiga samhällsinstitutioner, landsförräderi, angrepp på norska eller allierade styrkor, avslöjande av statshemligheter, kapning av luftfartyg eller skepp, störning av den säkra driften av järnväg eller buss, grov smittoöverföring och allmänfarlig förgiftning.

Tillstånd till sådana tvångsmedel som nu nämnts får enligt andra stycket i § 222 d lämnas endast om det kan antas att åtgärden kan ge information av väsentlig betydelse för att en brottslig handling ska kunna avvärjas eller att avvärjande av den, om åtgärden inte vidtas, väsentligen försvåras. Vidare krävs att det föreligger särskilda skäl att meddela tillstånd. Att det finns ett krav i båda de nämnda fallen på att åtgärden ska vara ett led i en förundersökning innebär att det måste – även om huvudändamålet med förundersökningen är att avvärja ett brott – finnas grund att tro att någon straffbar handling pågår eller har begåtts.

Den enda möjlighet som i Norge finns till hemlig tvångsmedelsanvändning när förundersökning inte pågår regleras i politiloven. Enligt dess § 17 d finns möjlighet för PST att av rätten få tillstånd till användning av hemliga tvångsmedel i preventivt syfte. Bestämmelsen aktualiseras när PST i sin förebyggande verksamhet behöver vidta exempelvis hemlig rannsakan, kommunikasjonsavlytting eller dataavlesing för att undersöka om någon förbereder vissa brott. Bland brotten i brottskatalogen, som omfattar färre brott än katalogen i § 222 d, upptas bland annat terroristbrottslighet och vissa brott mot staten. Tillstånd enligt bestämmelsen får lämnas endast om det finns grund att anta att åtgärden kommer att ge upplysningar av väsentlig betydelse för att kunna förebygga brottet, om förebyggande av brottet i väsentlig grad försvåras om åtgärden inte vidtas och om åtgärden med hänsyn till ärendets art och omständigheterna i övrigt inte framstår som oproportionerlig. Det krävs också, för användning av de nämnda tvångsmedlen, att det föreligger särskilda skäl att meddela tillstånd. Dessutom finns ett särskilt krav beträffande rannsakan och dataavläsning om sådan ska ske genom eller efter intrång i någons privata hem. Så får nämligen bara ske om det är fråga om utredning om förberedelse till terroristbrott, terrorforbund eller terrorhot (enligt straffeloven §§ 131, 133 och 134).

5.4.5 Hemlig dataavläsning som verkställighetsmetod i stället för tvångsmedel?

En för vår utrednings vidkommande intressant diskussion uppstod i Norge beträffande hur man skulle reglera metoden för hemlig dataavläsning. Metodekontrollutvalget (den norska utredningen) och den norska regeringen hade nämligen olika uppfattningar om detta. Eftersom både den norska utredningen och propositionen är författade i relativ närtid till vår utredning har vi funnit skäl att redovisa de olika synsätten.

Metodekontrollutvalget föreslog, i stället för att införa hemlig dataavläsning som ett nytt tvångsmedel, att dataavlesing skulle införas som en verkställighetsmetod (”gjennomføringsmåte”). Skälen för detta var att utredningen inte tyckte att det var ”dokumentert et tilstrekkelig behov for å innføre dataavlesing som nytt selvstendig tvangsmiddel”. Utredningen tecknade upp en bakgrund och beskrev tilltagande kryptering och andra sätt att skydda information som potentiella problem vid användning av befintliga tvångsmedel. Den hänvisade också till uttalanden från den norska Riksadvokaten som, främst mot bakgrund av ändrade förhållanden avseende kommunikation och kryptering, bestämt rekommenderade utredningen att föreslå en möjlighet för polisen att vidta hemlig dataavläsning. Emellertid konstaterade Metodekontrollutvalget att det inte varit möjligt att på något vis få kvantifierat eller på annat sätt närmare dokumenterat att det fanns ett verkligt behov av dataavläsning som tvångsmedel. Skälen till detta var två: dels fanns inga rutiner för rapportering av när befintliga tvångsmedel kom till korta, dels var det sällan (eller aldrig) som en utredning om brott stannade upp eller lades ned exempelvis för att polisen inte hade tillgång till hemlig dataavläsning som tvångsmedel. I stället var det i de flesta fall helt tillräckligt med de existerande tvångsmedlen. Eftersom utredningen ansåg att införande av nya tvångsmedel eller utvidgande av redan existerande sådana måste bygga på solid dokumentation av ett behov kom den således till den ovan angivna slutsatsen. Icke desto mindre fann Metodekontrollutvalget att det kunde anföras goda grunder för att dataavläsning skulle införas som en ”nødvendig teknologisk tilpassing for å kunne opprettholde effektiviteten av enkelte allerede eksisterende metoder”, dvs. som en verkställighetsmetod för bland

annat kommunikasjonsavlytting, hemlig rannsakan och beslag (se NOU 2009:15 s. 241 f. och 244).

Den norska regeringen, som i stället kom att föreslå dataavlesing som ett eget tvångsmedel, resonerade beträffande behovet kring att medvetenheten om informationsskydd och det utbud av krypteringstjänster som finns har lett till att existerande tvångsmedel tappat i effektivitet. Liksom utredningen fann inte heller den norska regeringen att det var möjligt att kvantifiera behovet av hemlig dataavläsning. Emellertid konstaterade den att utredningen och remissinstansernas yttranden över utredningen visade ett klart behov av att supplera bestämmelserna om avlyssning och hemlig rannsakan utifrån den nya rådande tekniska verkligheten. Enligt den norska regeringen var behovet än större i samband med propositionen (år 2016) än det var när Metodekontrollutvalget lämnade sitt betänkande (år 2009). Det var därför, enligt den norska regeringen, nödvändigt med ändringar för att återupprätta den effekt andra tvångsmedel haft tidigare, men också för att göra polisen bättre rustade inför de utmaningar som den tekniska utvecklingen kunde förväntas ge i framtiden, se Prop. 68 L (2015–2016) s. 259 f.

5.5 Andra länders användning av hemlig dataavläsning

Det är svårt att göra jämförelser mellan olika staters lagstiftning på tvångsmedelsområdet eftersom sådana jämförelser, för att bli rättvisande, kräver tämligen ingående kunskaper om bl.a. den processrättsliga lagstiftningen i de länder som jämförs. Utredningen har, utöver studiebesök i Norge, besökt säkerhetstjänster och brottsbekämpande myndigheter i Nederländerna, Storbritannien och Tyskland. Det huvudsakliga skälet till studiebesöken har varit att få en uppfattning av om hemlig dataavläsning, eller dess motsvarighet, är en effektiv åtgärd.

Vi har gjort bedömningen att det för vår framställning är tillräckligt med en beskrivning av de nordiska ländernas lagstiftning på området. För den som emellertid vill jämföra några andra länders lagstiftning och förslag till lagstiftning har en förtjänstfull, och såvitt framkommit vid våra studiebesök i väsentliga delar korrekt återgiven, studie gjorts av LIBE-kommittén inom Europaparla-

mentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor. Studien, som är författad på engelska, rör reglering och användning av motsvarigheter till hemlig dataavläsning i Frankrike, Italien, Nederländerna, Polen, Storbritannien och Tyskland samt i de tre icke EU-staterna Australien, Israel och USA. Bakgrunden till studien var en allt mer intensifierad debatt om vilka möjligheter som bör finnas för brottsbekämpande myndigheter att vidta åtgärder som motsvarar hemlig dataavläsning. Studien visar att metoder för hemlig dataavläsning används i de jämförda EU-staterna, i vissa fall med uttryckligt lagstöd och i andra fall utan sådant. I de stater där det inte finns explicit lagstiftning pågår för närvarande lagstiftningsarbete. Studien finns öppet tillgänglig på internet.[8]

5.6 Något om effektivitet och nytta

De studiebesök utredningen genomfört och kontakter utredningen haft med personer vid brottsbekämpande myndigheter i andra länder som har god insikt i hur de beskrivna åtgärderna används har främst syftat till att få uppgifter om hemlig dataavläsning är en effektiv åtgärd och vilken nytta den leder till. Till följd av sekretessregleringar har de personer utredningen varit i kontakt med emellertid genomgående varit förhindrade att uttala sig i dessa frågor på annat än en generell nivå. När det gäller Norge var det dessutom så att dataavlesing, vid utredningens studiebesök, inte hade varit i bruk tillräckligt länge för att kunna ge några tydliga och väl underbyggda slutsatser avseende effektivitet och nytta. Särskilt med hänsyn till den remisskritik som framfördes mot Beredningen för rättsväsendets utvecklings förslag om hemlig dataavläsning 2005 (SOU 2005:38), att utredningen inte klarlagt hur effektiv åtgärden ansågs vara i Danmark som då haft möjlighet att använda den i några få år, är det en brist i utredningen att inte kunna redovisa annat än tämligen begränsat officiellt publicerat material på området.

Med detta sagt bör dock framhållas att det, som framgått ovan, finns möjlighet att använda hemlig dataavläsning (eller motsvarande

[8] www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

åtgärd) i en rad stater. Det innebär att åtgärden i vart fall i dessa stater bedömts vara tillräckligt effektiv och ge tillräcklig nytta för att använda den där. Detta är också en genomgående ståndpunkt vid våra kontakter med företrädare för brottsbekämpande myndigheter i andra länder.

När det gäller mer explicita uttalanden om effektivitet har utredningen tagit del av rapporter från Danmark. När Danmark införde hemlig dataavläsning infördes också en rad andra lagar i vad som kallades ”anti-terrorpakke I”, vilket, som nämnts, var en reaktion på bland annat 11 septemberattackerna i USA år 2001 och syftade till att förbättra polisens möjligheter att förebygga, efterforska och bekämpa terrorhandlingar samt att stärka det straffrättsliga skyddet mot terrorism. År 2006 infördes ytterligare lagar i vad som kallades anti-terrorpakke II. Införandet av lagarna i anti-terrorpakke I och II utvärderades av den danska regeringen år 2010. I utvärderingen konstaterade det danska justitiedepartementet att de verktyg som polisen försetts med genom ”anti-terrorpakkene” (däribland hemlig dataavläsning) på ett generellt plan ”blevet anvendt med positive resultater”. Denna slutsats drogs utifrån bland annat följande utlåtande från Politiets Efterretningstjeneste (som är Danmarks motsvarighet till den svenska Säkerhetspolisen).

> Dataaflæsning omfatter bl.a. den situation, hvor politiet ved hjælp af et såkaldt ”sniffer-program” modtager kopi af samtlige indtastninger, som brugeren af edb-udstyret foretager, herunder åbning af computeren, oprettelse af nye dokumenter og regnskaber mv., nye indtastninger i allerede eksisterende dokumenter eller visse nærmere angivne indtastninger.
>
> Muligheden for dataaflæsning indebærer således, at politiet ved hjælp af edb-programmer eller andet udstyr løbende kan aflæse ikke offentligt tilgængelige oplysninger.
>
> Ved dataaflæsning får politiet adgang til tekst, herunder elektroniske meddelelser, uanset om teksten har været under forsendelse til eller fra den computer, der er genstand for dataaflæsning. Dataaflæsning udgør således også et alternativ til bl.a. ransagning, og generelt har Politiets Efterretningstjeneste et stort udbytte af de data, som opnås ved dette indgreb.
>
> Politiets Efterretningstjeneste har anvendt og anvender fortsat dataaflæsning i mange tilfælde. Dataaflæsning har vist sig at være et særdeles nyttigt efterforskningsmiddel og er bl.a. anvendt i forhold til målpersonerne i Vollsmose-sagen og Glasvej-sagen.

”Vollsmose-sagen” var ett mål där tre tilltalade dömdes för försök till terrorism genom att ha förberett framställning av en eller flera bomber att användas vid en terrorhandling. Två av de tilltalade dömdes till tolv års fängelse och den tredje till fem års fängelse. Också ”Glasvejsagen” gällde förberedelser för ett terroristattentat. Två tilltalade dömdes för försök till terrorism till tolv respektive åtta års fängelse för att ha framställt sprängämnen i en lägenhet i Köpenhamn.

I utredningens kontakter med företrädare för danska brottsbekämpande myndigheter har bilden från de redovisade rapporterna bekräftats. Anklagemyndigheten har också framhållit att dataaflæsning är ett ”meget nyttigt” verktyg för att komplettera den verktygslåda av tvångsmedel som retsplejeloven ger möjlighet att använda. Åtgärden är särskilt viktig för att bestämmelserna om hemlig rannsakan riktad mot elektroniskt lagrad information och telefonaflytning inte ska bli verkningslösa, t.ex. på grund av ny teknik och förbättrad kryptering.

När det gäller uppgifter från andra stater än Danmark har det, som nämnts, varit svårt att få fram konkreta sådana. Ett genomgående drag vid de kontakter utredningen haft med företrädare för brottsbekämpande myndigheter i andra stater är dock att åtgärden har potential att ge stor utredningsnytta i de fall den kan användas eftersom det då är möjligt att samla in väsentligt mer information av betydelse för utredningen än vad som är möjligt utan den. Liksom i Danmark tar de skäl som främst framhållits sikte på möjligheten att för brottsbekämpande myndigheter med hjälp av åtgärden, eller dess motsvarigheter, i klartext kunna ta del av uppgifter som annars skulle vara oläsbara.

6 Ny teknik och dess betydelse för utredningen

6.1 Inledning

I utredningsdirektiven anges att förutsättningarna för att bekämpa brott har förändrats. Som skäl för detta nämns bland annat att ökad internationalisering i kombination med teknikutveckling och en tilltagande internetanvändning inneburit att kriminaliteten delvis har ändrat karaktär.

Att användningen av internet och internetbaserade lösningar för kommunikation i många avseenden suddat ut traditionella gränser för olika territorier är allmänt känt. I nästa kapitel redovisas några olika områden där detta haft betydelse för brottsutvecklingen. Här ska i stället fokus främst vara på teknikutveckling och tilltagande internetanvändning.

Sedan BRU:s betänkande med förslag om bland annat hemlig dataavläsning kom 2005 har en rad tekniska innovationer förändrat vårt sätt att använda internet. Flera undersökningar görs årligen avseende användning av teknik och internet. I detta kapitel kommer vi att redovisa delar av några sådana undersökningar för att tydliggöra hur den för utredningen relevanta teknikutvecklingen sett ut och vad den inneburit för användningen av internet i några olika avseenden.

I SOU 2005:38 anfördes kryptering som ett skäl till att det fanns behov av hemlig dataavläsning. Också i denna utrednings direktiv anges att en allt högre grad av kryptering av internetbaserad kommunikation försvårat arbetet med vissa befintliga hemliga tvångsmedel, t.ex. hemlig avlyssning av elektronisk kommunikation. Detta eftersom den information som brottsbekämpande myndigheter får del av vid sådan avlyssning inte sällan är oläsbar. Om det förhåller sig på detta sätt och i vilken utsträckning kommer vi att återkomma till senare i betänkandet när de brottsbekämpande myndigheternas

behovsbeskrivningar presenteras samt i vår analys av behovet av hemlig dataavläsning. Dessförinnan har vi dock funnit skäl att i detta kapitel, mycket förenklat, redogöra för vad som avses med kryptering och hur kryptering används, såväl av helt legitima skäl som av kriminella för att dölja sin brottslighet.

6.2 Användning av internet, elektronisk kommunikation och digitala lagringsmedier

Hemlig dataavläsning föreslogs som ett nytt tvångsmedel redan 2005, bland annat på grund av den snabba tekniska utvecklingen. Denna utveckling – kanske i synnerhet utvecklingen av internetbaserade kommunikationstjänster och mobil tillgång till internet – har sedan dess fortsatt vara väldigt snabb. Över 75 procent av de svenska hushållen har t.ex. i dag tillgång till åtminstone en smarttelefon. När förslaget om hemlig dataavläsning kom var begreppet smarttelefon, såsom vi känner det i dag, knappast spritt i de breda massorna och en telefon som då kallades för smarttelefon skulle vid en jämförelse med dagens telefoner inte anses vara särskilt intelligent. Exempelvis lanserades den första modellen av iPhone år 2007.

Sociala medier och kommunikationstjänster som användes vid tiden för 2005 års förslag är till stora delar helt utbytta mot nya och det ökade smarttelefonanvändandet har lett till stora utbyggnader av det mobila telenätet. Inledningsvis kan således sägas att den ökade teknikanvändning och snabba teknikutveckling, som 2005 anfördes som några av skälen för förslaget, inte har stannat av utan snarare accelererat.

Det finns ingenting som tyder på att kriminella, i synnerhet personer involverade i organiserad brottslighet, utnyttjar den nya tekniken i mindre omfattning än allmänheten i övrigt.[1] Samtidigt finns inga för utredningen kända specifika undersökningar avseende kriminellas teknikanvändning. I det följande redovisas därför delar av några undersökningar beträffande bland annat svenska folkets teknik- och internetvanor.

[1] Se t.ex. rapporten *Myndighetsgemensam lägesbild om grov organiserad brottslighet 2016–2017*, Nationella underrättelsecentrumet (NUC) inom den myndighetsgemensamma satsningen mot den grova organiserade brottsligheten, s. 8.

6.2.1 Om undersökningarna

SOM-institutet vid Göteborgs universitet grundades år 1986 med syftet att genomföra frågeundersökningar och arrangera seminarier inom ämnesområdet Samhälle, Opinion och Massmedia. Institutet drivs i samarbete mellan Institutionen för journalistik, medier och kommunikation (JMG) och Statsvetenskapliga institutionen vid Göteborgs universitet. Varje år svarar mellan 10 000 och 20 000 svenskar på SOM-institutets frågor som rör allt från politik och massmedier till ämnen som livsstil, hälsa och fritidsvanor. Den nationella SOM-undersökningen är den mest omfattande undersökningen och har genomförts varje höst sedan 1986 med ett slumpmässigt urval personer boende i Sverige. Det som redovisas i detta avsnitt är hämtat från SOM-institutets rapport *Svenska trender 1986–2015* (benämns i det följande SOM-rapporten). Rapporten, vars mätningar genomförs som flera delundersökningar med olika inriktningar där varje delundersökning 2015 hade ett urval om 3 400 personer i åldersintervallet 16–85 år, finns publicerad på institutets webbsida.[2]

Rapporten *Svenskarna och internet* ges ut årligen av Internetstiftelsen i Sverige, IIS, en oberoende allmännyttig organisation som verkar för positiv utveckling av internet i Sverige. Rapporten är baserad på IIS egen primärdatainsamling som undersöker svenskarnas användning av internet och visar hur informations- och kommunikationsteknik används och påverkar enskilda individer, familjer och samhället. Inför rapporten år 2016 intervjuades drygt 3 000 personer från 12 år och uppåt under perioden februari–april 2016. Intervjuerna innehöll frågor om bland annat de intervjuade personernas bakgrundsdata, tillgång till teknik, användning av traditionella medier och framför allt användning av internet i olika former.[3] Svenskarna och internet benämns i det följande SOI samt med angivande av årtal för att tydliggöra vilken rapport vi hänför oss till.

I ett avslutande avsnitt i denna del redovisas kortfattat något om lagring av information via internet. Informationen där är främst hämtad från Statistiska centralbyråns (SCB) rapport *Privatpersoners användning av datorer och internet 2014*. Det är en rapport om privatpersoners användning av datorer och internet som grundas på

[2] http://som.gu.se/digitalAssets/1579/1579860_svenska-trender-2015.pdf
[3] Se www.soi2016.se/om-rapporten/om-arets-rapport/ där det också framgår att författarna till rapporten år 2016 är Pamela Davidsson och Olle Findahl.

undersökningar som SCB gör årligen på uppdrag av EU:s statistikorgan Eurostat och Näringsdepartementet. Undersökningen är en urvalsundersökning och vänder sig till personer i åldern 16 till 85 år. Uppgifterna i undersökningen har samlats in genom telefonintervjuer. I 2014 års rapport ingick en särskild temamodul som handlade om lagringstjänster på internet och andra molntjänster.[4]

6.2.2 Tekniktillgången

När det gäller tekniktillgång i de svenska hushållen framgår av SOM-rapporten att 90 procent av hushållen vid mätningarna 2015 hade tillgång till en dator, 89 procent till internet, 76 procent till en smarttelefon och 57 procent till en surfplatta. Av SOI 2016 bekräftas bilden av en stor tillgång till teknik och internet i hemmen. Enligt den hade nämligen 93 procent av svenskarna tillgång till internet, 92 procent till dator, 91 procent till bredband, 81 procent till smarttelefon och 65 procent till surfplatta år 2016. Dessutom framgår av den rapporten att 58 procent av befolkningen det året hade tillgång till såväl smarttelefon och surfplatta som dator i hemmet.

Båda rapporterna vittnar också om en snabb ökning av tekniktillgången i hemmen. Särskilt snabb har den de senaste åren varit när det gäller smarttelefoner och surfplattor. Mätningarna vid SOM-institutet beträffande sådan utrustning startade år 2010 och det kan konstateras att det varit en närmast explosionsartad utveckling. 2010 hade 19 procent av hushållen tillgång till en smarttelefon medan blott två procent hade tillgång till surfplatta vilket alltså kan jämföras med 76 respektive 57 procent 2015. Denna utveckling bekräftas av IIS-rapporteringen. Såvitt avser hushållens tillgång till internet och persondatorer har även denna varit ökande sedan 2010, om än inte i lika snabb takt. 2010 hade enligt SOM-rapporten drygt 80 procent av hushållen tillgång till internet och persondator, siffrorna var något högre enligt SOI 2016. Om man går tillbaka ytterligare 10 år, dvs. till år 2000 var internettillgången enligt SOM:s mätningar drygt 50 procent samtidigt som tillgången till persondator var cirka 60 procent.[5]

[4] *Privatpersoners användning av datorer och internet 2014* s. 1.
[5] *Svenska trender 1986–2015* s. 58 och *Svenskarna och internet 2016* s. 9 och 16.

6.2.3 Internetanvändningen

Internetanvändningen är ytterligare ett område där det skett en markant förändring under senare år. Bland hela befolkningen (16–85 år) var det enligt SOM-rapporten cirka 87 procent som använde internet minst flera gånger i veckan år 2015. I SOI 2016 framgår att 82 procent av befolkningen använder internet dagligen hemma och att av befolkningen upp till 55 år så var den andelen över 90 procent. Det finns stora skillnader mellan dels unga och gamla, dels hög- och lågutbildade när det gäller internetanvändningen. Bland unga (16–19 år) har 96 procent i SOM-rapporten svarat att de använder internet minst flera gånger i veckan medan samma svar från äldre (65–85 år) var 67 procent. Av de högutbildade använder enligt SOM-rapporten 95 procent internet minst flera gånger i veckan, vilket kan jämföras med 58 procent för lågutbildade. Även när det gäller internetanvändningen har det skett en ordentlig utveckling. 2005 sade sig, enligt SOM-rapporten, omkring 50 procent av befolkningen använda internet minst flera gånger i veckan.[6]

En tydlig utvecklingslinje syns också när det gäller utnyttjandet av smarttelefoner för att använda internet. Enligt SOI 2017 använder i dag 76 procent av svenskarna dagligen internet i sina smarttelefoner. Detta kan t.ex. jämföras med 5 procent 2010 och 38 procent 2012. I åldrarna 12–45 är det över 90 procent av smarttelefonägarna som använder telefonen för internet dagligen.[7]

6.2.4 Kommunikation

Av samtliga svarande i SOM-rapporten använde 80 procent internet för informationssökning åtminstone någon gång i veckan. I motsvarande utsträckning använde 79 procent internet för e-posthantering och 58 procent för sociala medier. Motsvarande siffror för 2010 var cirka 65 procent för informationssökning, knappt 70 procent för e-posthantering och cirka 40 procent för sociala medier.[8]

Enligt SOI 2017 är e-post och direktmeddelanden[9] alltjämt dominerande när det gäller den dagliga kommunikationen på internet.

[6] *Svenska trender 1986–2015* s. 59 och *Svenskarna och internet 2016*, s. 11 ff.
[7] *Svenskarna och internet 2017* s. 13 och 21, jfr även *Svenskarna och internet 2016* s. 19 f.
[8] *Svenska trender 1986–2015* s. 60.
[9] T.ex. via appar som Messenger eller iMessage.

2017 skickar 97 procent av internetanvändarna någon gång e-post och 69 procent av samma urvalsgrupp gjorde det dagligen. Motsvarande andelar för direktmeddelanden är 83 procent någon gång och 48 procent dagligen. Det syns en tydlig skillnad mellan olika åldrar när det gäller användningen av direktmeddelanden. Drygt 80 procent av användarna upp till 25 år och 69 procent av 26–35 åringarna använder sådana för sin kommunikation dagligen. Sedan sjunker graden av användning med stigande ålder. Det dagliga användandet av direktmeddelanden har ökat med minst 10 procentenheter i alla åldersgrupper år 2016 och 2017.[10]

Enligt SOI 2017 ökar andelen internetanvändare som ringer eller tar emot samtal via internet. 2017 är andelen som gör det någon gång 67 procent. 16 procent svarade att de ringde eller tog emot samtal via internet dagligen. Dessa siffror kan t.ex. jämföras med 2010 då 24 procent någon gång ringde eller tog emot samtal via internet och fyra procent gjorde så dagligen.[11]

6.2.5 Privata konton på internet

Av SOI 2015 framgår att internetanvändarna då i genomsnitt hade tio privata konton där lösenord måste anges för tillgång till kontot. Antalet konton var något högre än tio i åldrarna 16–45 år och något lägre för den äldre delen av befolkningen och 12–15-åringarna.[12]

Det sociala nätverk som dominerar är Facebook, vilket 74 procent av internetanvändarna i dag utnyttjar, varav 53 procent dagligen. Den aktivitet som är vanligast nyttjad bland de som Facebook erbjuder är användande av meddelandetjänsten Messenger, vilken 81 procent av Facebookanvändarna uppger att de nyttjar.[13] Även andra sociala nätverk används emellertid. Tydliga åldersskillnader kan noteras. Exempelvis använder långt över hälften av internetanvändarna i åldersgruppen 16–25 år (81 procent) Instagram[14]

[10] *Svenskarna och internet 2017* s. 36–39.
[11] *Svenskarna och internet 2017* s. 39.
[12] *Svenskarna och internet 2015* s. 40 ff.
[13] *Svenskarna och internet 2017* s. 43.
[14] Instagram är ett socialt nätverk på vilket användarna i huvudsak, på olika vis, kommunicerar med bilder eller videor.

någon gång medan motsvarande för åldersgruppen 46–55 år är under hälften (46 procent).[15]

6.2.6 Lagring av uppgifter i molntjänster

Det finns en rad olika sätt att lagra elektroniska uppgifter. Det vanligaste har under relativt lång tid varit att spara uppgifterna antingen direkt på datorns hårddisk eller på extern hårdvara, t.ex. ett USB-minne eller en extern hårddisk. Det har också varit vanligast att program som ska användas på en dator eller mobiltelefon har varit installerade på enheten. Under senare år har emellertid möjligheter för lagring och användning av programvara tillkommit. I dag krävs därför inte att den som vill spara uppgifter gör så till sin dator eller extern hårddisk eller liknande. Inte heller krävs att program som ska köras på en dator är installerade där. Det som krävs är i praktiken i stället en internetuppkoppling. Genom de s.k. molntjänster som tillhandahålls online kan lagring av data i dag ske på internetservrar och programvara kan användas över internet i stället för att vara installerad lokalt. Exempel på lagringstjänster som finns i dag är iCloud, Dropbox och Google Drive. Fördelarna med att lagra information och använda internetbaserade programvaror är bland annat att dessa är tillgängliga från olika tekniska enheter, vilket innebär att användaren inte måste använda en och samma dator eller mobiltelefon för att komma åt informationen, att man på så vis sparar lagringsutrymme på sin egen enhet, att det upplevs vara en säkrare form av datalagring och en möjlighet för användaren att skydda sig mot förlust av data.

I Statistiska centralbyråns rapport *Privatpersoners användning av datorer och internet 2014* framgår att nästan en tredjedel av personerna i åldersgruppen 16–85 år hade använt lagringsutrymme på internet under första kvartalet 2014. Skillnaderna var stora mellan olika åldersgrupper. Bland 25–34-åringarna hade 55 procent använt sådant lagringsutrymme medan det bland personer över 55 år var under 20 procent som hade gjort så.[16]

[15] Se *Svenskarna och internet 2017* s. 48.
[16] *Privatpersoners användning av datorer och internet 2014* s. 87.

6.3 Kryptering

6.3.1 Vad är kryptering?

Enligt Nationalencyklopedin innebär kryptering att ”i kommunikationssystem åstadkomma sekretess (dölja information för obehöriga) och/eller autenticitet (säkerställa äkthet hos information) genom att utnyttja en för de obehöriga användarna hemlighållen nyckel”.[17] I andra sammanhang har kryptering beskrivits som ”en metod för att förvandla information till oläslig rappakalja” och att man genom komplicerade matematiska algoritmer kan skapa krypterade meddelanden som är extremt svåra att knäcka.[18]

Människor har sedan mycket lång tid tillbaka använt metoder för att dölja innehållet i sin kommunikation för obehöriga utomstående. I takt med den tekniska utvecklingen har sådana metoder blivit allt mer svårgenomträngliga. Från de äldsta kända chiffersystemen, som är över två tusen år, till dagens sofistikerade krypteringsmetoder för säker datakommunikation är steget oerhört långt. Samtidigt vilar de på i huvudsak samma principer. Grundläggande är att budskapet som ska skyddas förändras till sitt innehåll så att det inte ska gå att förstå för utomstående. Vidare är det grundläggande att mottagaren har nyckeln för att kunna låsa upp och därigenom förstå budskapet.

Inom kryptologin, som är den kollektiva termen för kryptografi (vetenskapen som behandlar konstruktionen av krypteringssystem) och kryptoanalys (processen som används för att ta reda på innehållet i chiffertext utan kännedom om den riktiga dekrypteringsnyckeln), används följande grundläggande terminologi. Klartext kallas det meddelande som ska krypteras (eller ett meddelande som har dekrypterats). Den operation som används för att maskera innehållet kallas kryptering. Krypterad klartext benämns chiffertext, kryptotext eller kryptogram. De regler som används för att kryptera klartextmeddelanden kallas krypteringsalgoritmer. Vanligen är en kryptotext en funktion av inte bara en mer eller mindre allmän krypteringsalgoritm och klartexten. Därtill är den också en speciell krypteringsnyckel som är en, för varje användare, speciell kod. För

[17] *Nationalencyklopedin*, kryptering, www.ne.se/uppslagsverk/encyklopedi/lång/kryptering (hämtad 2016-10-17).
[18] Sus Andersson, *Lär dig kryptering*, s. 3. Elektroniskt tillgänglig via www.iis.se/docs/lar-dig-kryptering.pdf.

att i mottagaren återskapa den ursprungliga klartexten krävs en dekrypteringsalgoritm och en mot den speciella krypteringsnyckeln svarande dekrypteringsnyckel. Den som utan dekrypteringsnyckel försöker ta reda på klartexten kallas forcör.[19]

Det finns en rad olika metoder för kryptering och många är vidareutvecklingar av tidigare metoder och algoritmer. I takt med att datorer utvecklas som kan pröva enorma mängder dekrypteringsnycklar för forcörer (t.ex. brottsbekämpande myndigheter) i jakt på den som omvandlar chiffertexten till klartext utvecklas nya, synnerligen komplexa, metoder och algoritmer för ännu säkrare kryptering.

6.3.2 Hur används kryptering i praktiken?

Informationssamhället kräver ett skydd för mycket av såväl lagring av information som kommunikation som sker elektroniskt. Privatpersoner, myndigheter, företag och stater har många och olika legitima behov av att hålla sin kommunikation och information dold från obehöriga. Exempelvis är nog den som ska göra en överföring av pengar via bankens app på mobiltelefonen intresserad av att uppgifterna lämnas till banken och inte till någon annan. På motsvarande vis vill banken veta att det faktiskt är kontoinnehavaren och inte en bedragare som skickat uppgifterna/uppdraget. Journalister som ska skydda sin källa vill vara säkra på att kommunikationen kan ske säkert och en myndighetsanställd som ska skicka ett e-postmeddelande innehållande känsliga uppgifter är intresserad av att ingen annan än rätt mottagare kan öppna meddelandet.

På alla nivåer finns således ett påtagligt och högst befogat behov av att skydda information. Mot bakgrund av detta har en rad tjänster utvecklats. Många myndigheter och företag använder exempelvis s.k. VPN-anslutningar[20] som bland annat möjliggör för anställda – även när de inte är på arbetsplatsen – att ta del av informationen på arbetsplatsens lokala nätverk via internet. Genom en sådan anslutning verifieras arbetsgivare och arbetstagare för varandra och en skyddad anslutning upprättas. I hemmiljö används ofta trådlösa nätverk som inte sällan är skyddade genom krypteringstjänster så att endast den

[19] Christer Frank, *Kryptografi – en introduktion*, Studentlitteratur 2011, s. 17 f.
[20] VPN är en förkortning för virtuellt privat nätverk (eng. Virtual Private Network).

som känner till nätverksnyckel och eventuellt lösenord kan koppla upp sig mot nätverket. Vid köp i webbutiker via internet sker ofta kryptering för att skydda bland annat kreditkortsinformation. Det har också blivit allt vanligare med krypterade webbsidor genom s.k. TLS-kryptering.[21] De anförda fallen utgör exempel på situationer då kryptering förekommer för att obehöriga utomstående inte ska komma åt information.

Det har också utvecklats enkla, billiga och användarvänliga krypteringstjänster för den som önskar skydda sina meddelanden. Dels finns särskild programvara som den som vill kryptera sina meddelanden med kan införskaffa, dels har det blivit allt vanligare att leverantörer av meddelandetjänster har en inbyggd funktionalitet i programvaran som antingen på begäran från användaren eller, vilket torde vara det vanligaste, beträffande all kommunikation utför kryptering. Som exempel kan nämnas några av de allra populäraste tjänsterna; Facebooks Messenger, WhatsApp och Instagram, Microsofts Skype och MSN, Googles Gmail och Apples iMessage och FaceTime samt Twitter, Snapchat, Signal och Viber, vilka alla har, eller strävar efter att ha, en användarvänlig inbyggd krypteringstjänst i programvaran för att hindra utomstående att ta del av kommunikationen. Samtliga dessa tjänster finns tillgängliga som särskilda appar på smarttelefoner.

Det kan nämnas att Google på sin webbplats fortlöpande presenterar statistik avseende kryptering av inkommande och utgående e-posttrafik från och till andra e-postleverantörer (dvs. där användare av Googles e-posttjänst Gmail har skickat eller mottagit meddelanden till eller från en annan e-postleverantör). Statistiken anger hur stor andel av sådan trafik som är krypterad. Bara under de senaste åren har det enligt Googles rapporter skett en väsentlig ökning av andelen e-post som skickas med krypterad överföring (TLS-kryptering). I slutet av 2013 var cirka 30 procent av såväl inkommande som utgående trafik till och från Gmail skyddad med krypterad överföring medan det i oktober 2017 var cirka 89 procent av inkommande och utgående e-post som skyddades på motsvarande vis.[22]

[21] TLS är en förkortning för Transport Layer Security och är en vidareutveckling av SSL (Secure Socket Layer). I många fall används därför i dag förkortningen SSL synonymt med TLS. Om det i början av en webbadress anges *https* i stället för *http* används TLS-kryptering.
[22] Uppgifterna är hämtade från www.google.com/transparencyreport/saferemail/ ?hl=sv den 20 oktober 2017. Där uppger Google också att alla meddelande som skickas att alla e-post-

I kölvattnet av den diskussion som finns om personlig integritet på internet har också ett flertal internetbaserade e-postlösningar som utlovar insynsskydd från såväl brottsbekämpande myndigheter som hackare och andra dykt upp. Exempel på det anförda är Protonmail och svenska Countermail vilka båda marknadsför sig bland annat som både lättanvända och väldigt säkra. I vart fall Countermail-konton har förekommit i en rad brottsutredningar om allvarlig brottslighet.[23]

Också behovet av att skydda information lagrad i datorer, servrar, mobiltelefoner och annan teknisk utrustning har tillgodosetts genom att det utvecklats en rad krypteringstjänster. Exempel på sådana tjänster är Microsofts tjänst Bitlocker, som finns inbyggd i flera av Microsofts operativsystem, och Apples Filevault. Samtliga smarttelefoner har också en inbyggd krypteringslösning, vilken kräver lösenkod eller motsvarande för att informationen i enheten ska vara möjlig att ta del av.

Den omständigheten att det finns helt legitima behov för att skydda information har alltså lett till att det utvecklats goda möjligheter att på ett enkelt sätt använda kryptering. Sådana möjligheter står givetvis inte till buds endast för goda krafter utan även kriminella använder sig i högre utsträckning av olika lösningar för att skydda sin kommunikation. Det har inneburit att de brottsbekämpande myndigheterna i dag i hög utsträckning får del av krypterade uppgifter i stället för information i klartext vid hemlig avlyssning av elektronisk kommunikation samt har fått svårare att vid undersökningar av t.ex. beslagtagna mobiltelefoner ta del av innehållet i dem.

Vid utredningens studiebesök hos polisen har det från avdelningen för samordnad teknisk inhämtning (STI)[24] vid Nationella operativa avdelningen framhållits att endast en mycket liten del av den internetkommunikation som avlyssnas efter tillstånd till hemlig avlyssning av elektronisk kommunikation kan läsas eller lyssnas av i klartext beroende på den höga krypteringsgraden och att krypteringen sker end-to-end, dvs. så att bara sändare och mottagare kan

meddelanden som skickas mellan Gmails egna användare är krypterade, varför statistiken endast avser kommunikation med andra e-postleverantörer.

[23] Se t.ex. Hovrättens för Västra Sverige domar den 29 januari 2016 och 25 november 2016 i målen B 4773-15 och B 3847-16 och Svea hovrätts dom den 9 augusti 2013.

[24] STI ansvarar för driften av det system som de brottsbekämpande myndigheterna använder för bl.a. verkställighet av hemlig avlyssning av elektronisk kommunikation.

läsa meddelandena. Det är enligt samma källa en tydlig skillnad jämfört med bara för något år sedan och en väsentlig skillnad mot för 8–10 år sedan, då i stort sett ingen internetkommunikation var krypterad. Internetkommunikation kan exempelvis vara samtal och meddelanden via en mobiltelefons appar eller en dators program (såsom WhatsApp, Skype eller iMessage) och vanlig surf till webbsidor. Av den internettrafik på ett mobiltelefonabonnemang som avlyssnas med stöd av reglerna om hemlig avlyssning av elektronisk kommunikation uppskattar representanter för STI att knappt tio procent av det insamlade kan läsas i klartext, och således ge information i ärendet. Av dessa knappa tio procent utgör enligt samma källa merparten surfande hos nyhetsbyråer (vanligen via tidningstjänsters appar) och på pornografiska webbsidor, eftersom dessa typiskt sett ännu inte är krypterade. Värdet av att kunna se vilket innehåll på sådana sidor som den misstänkte tar del av är i normalfallet mycket litet, även om det i vissa fall kan tänkas vara av intresse när den misstänkte i tidningsappar söker på händelser denne själv är misstänkt för.

Eftersom dagens krypteringsmetoder håller synnerligen hög säkerhet, i meningen svårgenomtränglighet för forcörer, får således de brottsbekämpande myndigheterna i de allra flesta fall tillgång endast till ”oläslig rappakalja” genom hemlig tvångsmedelsanvändning och därmed inte till den eftertraktade klartexten som tvångsmedelsbeslutet ger rätt att ta del av.

6.3.3 Något om Deep web, Darknet, Tor och andra anonymiseringstjänster

På senare år har ett fenomen som är anknutet till frågan om kryptering kommit upp till diskussion allt oftare i t.ex. brottsutredningar och vid rättegångar. Fenomenet kallas för Darknet och är en del av vad som kan kallas ett dolt internet. I detta avsnitt finns en kort förklaring av begreppet och vilket samband det har med frågorna om kryptering.[25]

Internet är en sammankoppling av datorer som utgör världens största datornätverk. All kommunikation över internet sker med kommunikationsprotokollet Internet Protocol (IP). Varje dator som

[25] Informationen i detta avsnitt är huvudsakligen hämtad från *Internetguide #39 Kom igång med Tor!* som finns tillgänglig på www.iis.se/docs/kom_igang_med-tor.pdf

kopplar upp sig mot internet får sig tilldelad åtminstone en IP-adress av nätverksadministratören eller internetleverantören. Starkt förenklat kan sägas att internettrafik, bland annat på grund av IP-adresserna, är spårbar till användare.

Deep web utgör de delar av internet som inte är allmänt tillgängliga via vanliga sökmotorer, t.ex. på grund av att de är lösenordsskyddade eller har ett krypterat innehåll. Den personliga sidan på Facebook är ett exempel på en sida som kräver inloggning och som därför inte är sökbar i en vanlig sökmotor och således utgör en del av Deep web. Det är okänt hur omfattande Deep web är men det har bedömts vara väsentligen större än de sökbara delarna av internet.[26]

Delar av Deep web brukar kallas för Darknet, vilket är krypterade nätverk som möjliggör för användarna att kommunicera utan att varken kommunikationen eller användarna kan spåras, eller i vart fall att sådan spårning väsentligen försvåras. Det troligen mest kända av dessa nätverk är Tor (namnet är en akronym av ”the onion router”, vilket i sig är passande eftersom informationen som skickas skyddas i olika lager). För tillgång till Tor krävs en särskild webbläsare, en s.k. Tor-browser. Sådana finns lätt tillgängliga för de flesta vanliga operativsystem. Principen bakom anonymiseringen i Tor är att användaren dirigeras genom ett gratis och världsomspännande nätverk bestående av några tusen datorer som skickar trafik mellan sig. När man kopplar upp sig mot nätverket skickas trafiken mellan tre av dessa och sedan vidare till slutdestinationen. All trafik som ens dator skickar och tar emot via Tor krypteras i tre lager, på ett sätt som gör att ingen av de tre datorerna kan koppla trafiken till den som kopplat upp sig.

Tor har sina rötter i ett utvecklingsprojekt i den amerikanska marinen och den ursprungliga idén med projektet var att skydda myndigheters kommunikation. I dag utvecklas mjukvaran, vars källkod är öppen, emellertid av en ideell stiftelse registrerad i USA. Bland finansiärerna bakom Tor har bland annat svenska Sida funnits. Skälet till detta var att Tor ansågs som ett viktigt verktyg i länder med totalitära regimer. Med Tor kunde medborgarna få möjlighet att använda internet utan att avslöja vilka de är eller för att undvika censur.

[26] Se Europols rapport *TE-SAT 2016* s. 17.

Andra anonymiseringstjänster

Under senare år har en rad kommersiella tjänster som kan tillgodose anonymisering på internet dykt upp. Sådana tjänster marknadsförs ofta som ett sätt för enskilda att bevara sin integritet på internet. Det kan antas att intresset för dessa tjänster ökat i takt med en allt mer intensifierad debatt om integritet, massövervakning och osäkerheter avseende den egna identiteten på internet.

Det finns som sagt ett flertal olika anonymiseringstjänster tillgängliga för den som önskar agera på internet ”under radarn”. Det skulle inte leda denna framställning framåt att presentera de olika metoder som används. Gemensamt för tjänsterna är emellertid att de använder krypteringsteknik, ibland i kombination med annan teknik, för att kunderna ska bli svårare att upptäcka och identifiera i sina aktiviteter på internet. Inte sällan sker anonymisering genom att användarna tilldelas samma IP-adress och möjligheter att använda sig av VPN-anslutningar. I många fall kan användarna av tjänsterna dessutom vara anonyma även för företaget som tillhandahåller tjänsten genom att betala kontant eller med virtuella valutor.

6.3.4 I vilken utsträckning använder kriminella kryptering?

Av naturliga skäl finns ingen tillförlitlig statistik beträffande kriminellas användning av krypteringstjänster. Emellertid framhålls från olika håll att användningen av sådana tjänster minskar effektiviteten i de brottsbekämpande myndigheternas användning av befintliga tvångsmedel.[27]

Europol har i en rapport från 2015 konstaterat bland annat följande om kriminellas – främst terroristorganisationers – användning av kryptering.[28]

> Individuals and groups involved in terrorist and extremist activities use encryption or obfuscation in order to evade interception of their communications by law enforcement and intelligence agencies. Terrorist groups encourage their followers to cover their traces with encryption software. Al-Qaeda and IS have gone as far as to develop their own tools. However, the use of these seems to be waning. More recently, terrorists, like other criminals, are exploiting the opportunities for

[27] Se t.ex. Åklagarmyndighetens *Redovisning av användningen av vissa hemliga tvångsmedel under 2015* (Dnr ÅM-A 2016/0093), s. 7.
[28] *TE-SAT 2016* s. 17.

> secure communication provided by smartphone applications and other software, thereby abusing the efforts made by companies to ensure privacy and data protection for their customers. The development and accessibility of such software provide terrorists with the opportunity to communicate covertly without the burden of developing and maintaining their own tools. Terrorist groups publicise numerous detailed guides about how to remain anonymous and use mainstream tools and apps securely.

Även Darknet, främst Tor, synes användas i hög utsträckning av kriminella. På flera håll har bilder av Darknet målats upp som ett nätverk där alla typer av olagliga produkter och tjänster finns tillgängliga. Exempelvis hävdas att det genom Darknet är möjligt att beställa mord eller droger.[29] Även beträffande Darknet har Europol yttrat sig i den nyss citerade rapporten. Under rubriken The Cyber Dimension, ett avsnitt som behandlar riskerna för s.k. cyberterrorism, anges följande.[30]

> Traditionally, criminal forums and marketplaces operated in the open or Deep Web. However, Darknets such as Tor – a freely available anonymity network – are increasingly becoming host to such sites, commonly known as hidden services. These offer a place to acquire almost any illicit commodity or service such as narcotics, weapons – including firearms and explosives – forged documents, stolen IDs, stolen credit card information and hacking tools, including zero-day exploits. Key services include infrastructure-as-a-service such as secure hosting services, which provide a high level of resilience against law enforcement interventions, virtual private networks (VPNs) and proxy services that play an important role in providing anonymity, and botnet rentals to launch, for instance, Distributed Denial of Service (DDoS) attacks or large-scale online banking attacks. Hacking services, including support for advanced attacks such as economic espionage, and money laundering services are other examples of criminal offerings that are available online.

Det finns domar i Sverige som bekräftar att det via Darknet åtminstone skett omfattande drogförsäljning i landet.[31] Frågan om kriminellas användning av kryptering kommer i viss mån utvecklas vidare nedan i kapitel 7.

---

[29] Se t.ex. www.dn.se/kultur-noje/pa-natets-morka-sida/

[30] *TE-SAT 2016* s. 17. Det bör nämnas att DDoS (som omnämns i citatet) står för distributed denial of service och är en större attack mot ett nätverk eller datorsystem, ofta utfört av hackare med hjälp av kapade uppkopplade datorer. Zero-day exploits är ett inom it-kretsar vedertaget begrepp för utnyttjande av vissa säkerhetsbrister i programvara.

[31] Se t.ex. Hovrätten för Nedre Norrlands dom den 15 september 2015 i mål nr B 553-15 och Hovrätten för Västra Sveriges dom den 25 november 2016 i mål nr B 3847-16.

7 Brottsutvecklingen av betydelse för utredningen

7.1 Inledning

Frågan om brottslighetens ändrade karaktär är enligt direktiven av betydelse för denna utredning. I detta kapitel ska därför fokus riktas mot hur brottsutvecklingen sett ut på några för utredningen relevanta områden. Det är emellertid svårt att avgöra hur omfattande en redovisning av hur den moderna brottsligheten ser ut ska vara. En allt för vidlyftig framställning kan leda till att kärnan, dvs. de för utredningen relevanta områdena, försvinner i mängden information. Samtidigt kan en allt för begränsad redogörelse innebära risk för att relevanta aspekter och konsekvenser av brottsutvecklingen inte framträder så tydligt som är önskvärt. För att uppnå någon slags balans i framställningen försöker vi i kapitlet att beskriva den moderna brottsligheten och dess utveckling ur två perspektiv. Det ena handlar om hur och i vilken omfattning modern teknik i dag används i olika typer av kriminalitet och det andra om hur några fält inom modern kriminalitet har utvecklats på ett mer generellt plan.

När det gäller det första av de valda perspektiven, dvs. i vilken mån teknik används i brottslighet har vi ansett det vara av relevans både att tekniken används i själva brottsligheten (t.ex. dataintrång och barnpornografibrottslighet) och att den används så att bevisning kan säkras om förestående eller begångna brott (t.ex. kontakter mellan kriminella via meddelandetjänster). Perspektivet behandlas i avsnitten 7.2 och 7.3.

I direktiven nämns terroristbrottslighet och organiserad brottslighet särskilt. Det finns ett angeläget samhälleligt intresse av att komma till rätta med dessa brottskategorier. Så är givetvis fallet även vid annan allvarlig brottslighet, t.ex. dödligt våld. Vårt andra perspektiv tar därför sikte på nuläge och utvecklingstendenser inom

dessa tre fält. I de avsnitt (7.4 och 7.5) som behandlar dessa frågor är framställningen inte lika teknikorienterad som i de tidigare avsnitten.

7.2 It-relaterad brottslighet

Det har i olika sammanhang förts fram förslag till vad som ska anses vara it-relaterad brottslighet.[1] I Brå-rapporten *It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem* används följande definition.[2]

> It-relaterad brottslighet innebär att brottet har it-inslag genom att it är närvarande på någon av följande tre nivåer.
>
> 1. It är *målet* och en förutsättning för brottets genomförande, till exempel dataintrång.
>
> 2. It är *medlet* och har understött brottet, till exempel genom att ett socialt forum använts för att hota någon.
>
> 3. It kan, utan att vara mål eller medel, ha *beröring* med brottet. Detta genom att digitala spår[3] har lämnats som kan användas som bevisning vid ett brott som begåtts utanför it-miljö.

Samtliga tre nivåer är i allra högsta grad relevanta för vår utredning. När begreppet it-relaterad brottslighet fortsättningsvis används i betänkandet avses därför den betydelse som framgår av den nu givna definitionen.

Av rapporten[4] framgår först att en oerhörd ökning skett av antalet anmälda brott som kan identifieras som it-relaterade utifrån den brottskodning som sker hos polisen vid anmälan (studien av den officiella kriminalstatistiken). Ökningen under perioden 2006–2015 var 949 procent. I absoluta tal var den observerade ökningen störst när det gäller brottstypen datorbedrägeri och därefter bedrägeri med hjälp av internet. Mellan år 2006 och 2015 ökade antalet anmälda datorbedrägerier från cirka 6 200 till 67 100 och bedrägerier med

[1] Se t.ex. Riksrevisionens rapport *It-relaterad brottslighet – polis och åklagare kan bli effektivare* (RiR 2015:21) s. 17 och där angivna hänvisningar.
[2] Se Brå-rapport 2016:17 s. 19. När vi i det följande i betänkandet använder begreppet it-relaterad brottslighet gör vi det i samma mening som enligt rapportens definition.
[3] Digitala spår eller digital bevisning är information som antingen är överförd via eller lagrad i binär form.
[4] Metoden som användes i studien framgår på s. 21 ff. i Brå-rapporten 2016:17.

hjälp av internet från 1 500 till 24 100.[5] Brå framhåller att möjligheten att följa den it-relaterade brottslighetens utveckling med hjälp av kriminalstatistiken är starkt begränsad och att det inte går att, med hjälp av den anförda statistiken, dra några slutsatser om it-inslagen för brott med övriga brottskoder. Det går enligt Brå 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.[6]

Studien visar också att it-inslagen i de polisanmälda brotten totalt sett har mer än fördubblats mellan åren 2006 och 2014 (från 7 till 17 procent). Enligt Brå bör nivåerna emellertid tolkas med stor försiktighet då de ”med all sannolikhet utgör en kraftig underskattning” av den totala andelen brott med it-inslag.[7] Det kan också anmärkas att majoriteten av de förundersökningsledare som Brå intervjuade inom ramen för studien anser att det i dag snarare är regel än undantag att det finns potentiell digital bevisning i ärendena. Den digitala bevisningen kan t.ex. utgöras av beslagtagna mobiltelefoner som innehåller någon slags information som kan styrka brott, våld som har filmats med en mobiltelefon, butiksrån eller snatterier som har filmats med en övervakningskamera eller data från en masttömning.[8]

Bakom den generella ökning som observeras i polisanmälningarna ligger enligt Brås bedömning att ett antal faktorer spelar in. En viktig faktor är att det har skett en ökning av brott som per definiton har it-inslag (t.ex. datorbedrägeri, bedrägeri med hjälp av internet, dataintrång). En annan faktor är att utvecklingen av sociala medier avspeglas i ökningar av hot, ofredanden och andra brott som sker via sådana kommunikationsvägar. En tredje faktor är att andelen brott som har filmats av övervakningskameror tycks ha ökat, vilket gäller för flera typer av brott (t.ex. våldsbrott, stöld och skadegörelse). En fjärde faktor som enligt Brå förklarar den ökning av it-inslag som observeras i polisanmälningarna är att polisens beslag av misstänkta personers mobiltelefoner tycks ha ökat, t.ex. vid narkotikabrott.[9]

Brå har också i studien undersökt utvecklingen av antalet it-beslag. Med begreppet avses beslagtaget gods som registrerats i Polisens

[5] A. Brå-rapport s. 30 f.
[6] A. Brå-rapport s. 29 f.
[7] A. Brå-rapport s. 32.
[8] A. Brå-rapport s. 33.
[9] A. Brå-rapport s. 39.

ärendehanteringssystem i någon av undergrupperna[10] *Mobiltelefon*, *Datautrustning/Tillbehör/Programvara* eller *Dator/PC/Mac*. Av studien framgår att det även beträffande it-beslag har skett en ökning. År 2014 registrerades 72 382 beslag i huvudgruppen *Bokföring/Data/Kontor/Telefoni*, vilket kan jämföras med 53 883 beslag år 2008. Det motsvarar en ökning på 34 procent. Ökningen förekommer i samtliga undergrupper av huvudkategorin som Brå har studerat. Den procentuella ökningen är störst inom undergruppen *Dator/PC/Mac* där ökningen motsvarar 64 procent sedan 2008. I undergruppen *Mobiltelefon* ökade beslagen med 59 procent och i *Datautrustning/Tillbehör/Programvara* var ökningen 26 procent under den aktuella tidsperioden. Detta kan jämföras med den totala ökningen för beslag (för samtliga huvudgrupper) under samma tidsperiod, som var 8 procent.[11] Att antalet it-beslag ökat bekräftades också av flera av de personer som Brå intervjuade i studien. Intervjupersonerna var även överens om att bevisen som it-beslagen kan generera många gånger har mycket stor betydelse för utredningen och att det finns en underutnyttjad potential i den information som ligger lagrad i till exempel mobiltelefoner.[12]

Även beträffande studien av it-beslag konstaterade emellertid Brå att det fanns betydande osäkerhetsfaktorer. Bland annat framhöll Brå att det utifrån statistiken inte går att utläsa om det beslagtagna föremålet har lämnats in för it-undersökning eller inte. Vidare framhölls att skälet till att ett föremål tas i beslag inte framgår av begärda data och att det utifrån materialet inte går att utläsa om det har skett en förändring av komplexiteten av de beslagtagna föremålen som lämnas in för undersökning (t.ex. ökad förekomst av krypterade data) eller av mängden data i den beslagtagna utrustningen.[13]

[10] Beslagtaget gods registreras enligt Brå-rapporten i Polisens ärendehanteringssystem i en huvudgrupp och därefter i en undergrupp. I systemet finns huvudgrupper som Droger/Narkotikaredskap, Fordon/Fordonstillbehör/Trafik/Flyg och Bokföring/Data /Kontor/Telefoni. Inom den sist angivna huvudgruppen finns bland annat de angivna undergrupperna.
[11] A. Brå-rapport s. 39 f.
[12] A. Brå-rapport s. 41.
[13] A. Brå-rapport s. 39.

7.3 Europols rapportering om it-brottslighet

Inom Europol finns sedan 2013 arbetsgruppen European Cybercrime Center (EC3) som arbetar med att stärka de brottsbekämpande myndigheternas möjligheter att motverka it- brottslighet[14]. EC3 ger årligen ut rapporten *Internet Organised Crime Threat Assessment (IOCTA)* i vilken Europol år för år redogör för trender, tendenser och fokusområden när det gäller it-brottslighet. I det följande ska ett antal trender och tendenser redovisas för att ge en bild av hur modern brottslighet kan se ut. Det bör nämnas att Europol uppskattar kostnaderna för it-brottslighet inom EU till 265 miljarder euro årligen. På global nivå uppskattas kostnaderna uppgå till omkring 900 miljarder euro.[15]

7.3.1 Sabotageprogram

Ett område som under flera år lyfts fram som ett problem i IOCTA-rapporterna är sabotageprogram (eng. malware). Med sabotageprogram avses oönskad programvara i dator, mobil eller annan teknisk utrustning. Såväl sabotageprogrammen i sig själva som problemen som omgärdar dessa är mångfacetterade. Förenklat kan dock problemen förklaras med att kriminella förmår användare av teknisk utrustning att, medvetet eller omedvetet, installera oönskad programvara i utrustningen. Sabotageprogrammet som installerats kan därefter vidta åtgärder med innehållet i utrustningen, såsom att kryptera filer eller söka efter viss information.

I IOCTA 2016 slås fast att de största svårigheterna avseende sabotageprogram för närvarande är s.k. ransomware (sabotageprogram som gör utrustningen obrukbar och kräver användaren på en lösensumma för att utrustningen ska fungera igen) och s.k. information stealers (sabotageprogram som från utrustningen stjäl information, vilken därefter kan användas i kriminella syften, t.ex. lösenord). Den typ av ransomware som enligt Europol på senare tid blivit det mest framträdande hotet för såväl medborgare som företag och myndigheter är s.k. cryptoware. När ett sådant program har installerats krypteras alla eller vissa filer i utrustningen varefter

[14] Vi använder termen it-brottslighet i denna del för det engelska begreppet cybercrime.
[15] www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

användaren får information om att det enda sättet att komma åt filerna igen är att betala en lösensumma. Typiskt sett ska summan betalas i en virtuell valuta (vanligen kryptovalutan Bitcoin), vilket försvårar spårningen till de kriminella som ligger bakom aktionen. Dessutom är det vanligt att beloppet som ska betalas ökar över tid om betalning inte sker.

Tidigare har sabotageprogram främst varit framtagna för och riktade mot datorer. I IOCTA 2016 lyfter emellertid Europol fram att det finns tydliga indikationer på att sabotageprogram som tar sikte på smarttelefoner håller på att få ett genombrott i kriminell verksamhet.[16]

7.3.2 Sexuella övergrepp mot barn via internet

Ett annat område som IOCTA-rapporteringen belyser är utnyttjandet av barn i sexuella syften på internet. Enligt IOCTA 2016 är det även i dessa sammanhang fråga om olika typer av problem och kriminalitet. Den gemensamma nämnaren är emellertid att kriminaliteten bottnar i användandet av internet som plattform för att kommunicera, lagra och dela barnpornografiskt material för personer som på olika sätt utnyttjar barn.

Ett av de huvudsakliga hoten på området är enligt Europol nätbaserade sexuella tvång och utpressningar (eng. sexual coercion and extortion online). Typfallet vid dessa gärningar är att förövaren på något sätt, via främst sociala medier och onlinespel som barn och unga använder, vinner barnets förtroende och därefter utnyttjar barnets sårbarhet och utsatthet i syfte att komma över en bild eller video av sexuell karaktär. Detta leder till en fas där förövaren utövar utpressning mot barnet. Beroende på om gärningsmannens drivkraft är av sexuell eller ekonomisk karaktär varierar handlandet. I det förra fallet utövas utpressning i syfte att komma över mer material medan utpressningen i det senare fallet handlar om att barnet ska betala för att materialet inte ska spridas.[17]

Inom området för utnyttjandet av barn i sexuella syften på internet rapporteras också om ett ökat antal direktsända sexuella över-

[16] IOCTA 2016 s. 10 och 17 ff.
[17] IOCTA 2016 s. 24.

grepp (eng. live streaming of child sexual abuse). Med detta avses att förövare via internet beställer och därefter i realtid regisserar (och via en datorskärm ser) ett sexuellt övergrepp mot ett barn någon annan stans i världen. Övergreppet kan både ”skräddarsys” enligt förövarens önskemål och spelas in för att sedan spridas. Denna typ av beteende bidrar till en ökad spridning av, i dessa kretsar, mycket eftertraktat barnpornografiskt material på internet. Anonymiteten vid sådana övergrepp som nu har beskrivits kan garanteras med s.k. end-to-end-kryptering. Genom sådan kryptering kan inte ens den tjänsteleverantör som tillhandahåller exempelvis videosamtalet veta vad som sprids bland dess användare. Detta hämmar enligt Europol bevisinsamlandet och försämrar möjligheterna att i brottsförebyggande syften vidta åtgärder mot problemet. Tidigare har dylika övergrepp som nu beskrivits främst skett i Sydostasien men enligt IOCTA 2016 syns nu tendenser på att problemet sprider sig till att omfatta även andra delar av världen. Ett gemensamt drag bland dessa länder är att de är fattiga, har begränsat skydd för barn och unga och att det där är lätt att komma åt barn. Det finns också, enligt Europol, bevis för en länk mellan direktsända övergrepp och efterföljande resande i syfte att på plats själv utnyttja barn sexuellt liksom för att personer som varit på plats och utnyttjat barn i ett senare skede begår den nu beskrivna typen av övergrepp på distans.[18]

Ett annat problem som lyfts fram i IOCTA 2016 är den ökande medvetandegraden i detta segment av kriminella om vilka åtgärder brottsbekämpande myndigheter kan vidta och vilka tekniska möjligheter dessa har. Liksom andra it-brottslingar använder sexualförbrytare olika tjänster för att dölja sin brottsliga verksamhet. Bland dessa tjänster finns exempelvis IP-anonymisering, kryptering för kommunikation och för utrustning, program som kan förstöra filer eller enheter (s.k. wiping software) och molnlagring. Det är i dag mer regel än undantag att sådana tjänster används och det är således inte som tidigare bara ”sofistikerade” förövare som utnyttjar den moderna tekniken. Dessutom ger Darknet och liknande tjänster inte bara möjlighet för förövare att sprida och ta emot barnpornografiskt material. De ger också förövare chansen att utbyta tekniker för att

[18] IOCTA 2016 s. 26.

minska eller begränsa brottsbekämpande myndigheters chanser att komma åt dem.[19]

7.3.3 Dataintrång och nätverksattacker

Bland de tjänster som finns tillgängliga i den ”digitala undre världen” är enligt IOCTA 2016 en av de populäraste s.k. DDoS-attacker (se förklaring i not 30 i avsnitt 6.3.4). Sådana attacker, eller rättare sagt hot om sådana attacker, används inte sällan i utpressningssyfte genom att den som attackerar informerar den som är måltavla för attacken t.ex. att dennes webbsida kommer att bli överbelastad och därmed oanvändbar om den attackerade inte betalar en lösensumma. På senare tid har DDoS-attacker blivit allt kraftfullare. Som ett exempel på detta kan nämnas att det när IOCTA 2015 publicerades var ovanligt med attacker som översteg 100 gigabits per sekund (Gbps). Under senare delen av 2015 rapporterades om attacker som översteg 300 Gbps och 2016 angreps både BBC:s och Donald Trumps webbsidor med attacker som översteg 600 Gbps. Ju högre ”överföringshastighet” attackerna utförs med desto större skada orsakas genom att det blir svårare för den vars webbsida attackeras att värja sig mot attacken. De senare attackernas intention var att demonstrera effektiviteten hos nya ”DDoS-verktyg”. Sådana verktyg, vilka ofta kallas ”booters” eller ”stressers”, finns lättillgängliga som tjänster på internet och har stått för en betydande del av DDoS-attackerna som rapporterats till de brottsbekämpande myndigheterna. Motiven för DDoS-attacker varierar; i hög utsträckning handlar det, som nämnts, om utpressningsmotiv men det finns också exempel på ren illvilja och attacker med oklara motiv.[20]

Hälften av EU:s medlemsstater har rapporterat till Europol att det där förekommit utredningar rörande DDoS-attacker. En nästan lika stor andel av medlemsstaterna har indikerat att de har varit involverade i utredningar om attacker mot privata nätverk. Främst har det varit fråga om hackande och utnyttjande av nätverkens sårbarheter men också bland annat användande av sabotageprogram har konstaterats. Målen för sådana attacker har främst varit att

[19] IOCTA 2016 s. 26.
[20] IOCTA 2016 s. 35.

antingen stjäla information eller begå bedrägerier men också i dessa fall har attacker av ren illvilja kunnat konstateras.[21]

7.3.4 Attacker mot samhällsviktig infrastruktur

Ett område som redovisas särskilt i IOCTA-rapporteringen är attacker mot samhällsviktig infrastruktur (eng. attacks on critical infrastructure). Definitionen av samhällsviktig infrastruktur är att driftstörningar eller förstörelse av dessa skulle ha en försvagande effekt på samhället. Attacker av sådant slag som nu diskuteras kan t.ex. innebära att angriparen får tillgång till kunskap om hur specifika kontrollsystem fungerar. Detta kan i sin tur leda till riktade attacker som utnyttjar de sårbarheter som uppmärksammats, med systemkollaps som följd. Sabotageprogram skulle potentiellt kunna manipulera kontrollen av kraftnät, finansiella tjänster, försvar eller sjukvårdsregister vilket kan få katastrofala följder i den ”riktiga världen” i form av exempelvis fysisk skada, strömavbrott eller störningar i en hel stads vattentillgångar. Under 2015 rapporterade, enligt IOCTA 2016, brottsbekämpande myndigheter runtom i Europa om en rad attacker mot samhällsviktig infrastruktur. Som exempel nämns bland annat att det ukrainska kraftnätet angreps i december 2015 med trojaner som var ämnade att attackera vissa funktioner i kontrollsystemen, att ett tyskt kärnkraftverk i april 2015 attackerades med hjälp av sabotageprogram som, om det hade haft den rätta tillgången till internet, hade kunnat fjärrstyras samt att ett tyskt stålverk angreps i slutet av 2014 vilket var det första bekräftade fallet där en sådan attack lett till förstörande av fysisk utrustning.[22]

7.3.5 Internet och terrorism

Enligt IOCTA 2016 är användandet av sociala medier den mest rapporterade terroristaktiviteteten på internet. Terroristgrupper använder sådana sociala medier som plattform för en rad aktiviteter såsom rekryteringskampanjer, propaganda, uppviglande till terroristattentat och för att ta på sig ansvar för utförda attentat. Sociala medier

[21] IOCTA 2016 s. 36.
[22] IOCTA 2016 s. 39 f.

har enligt Europol varit en nyckelfaktor för terroristgrupperingars möjligheter att sprida sina budskap, bland annat avseende vad man uppnått. De har också använts i radikaliserings- och självradikaliseringsprocesser. Vissa brottsbekämpande myndigheter i Europa har på senare tid noterat en växande trend i självradikaliseringsprocessen, kanske möjliggjord genom den snabba och enkla tillgången till propaganda på internet. Sådan propaganda tycks, enligt Europol, förenkla radikaliseringen av ensamagerande terrorister (eng. lone actors), vilka kan tilltalas av extremistideal framför datorn och ledas till att genomföra terroristattacker i sina hemländer. Samtidigt pekar Europol på att det inte finns några empiriska belägg för att internet är bland de bakomliggande orsakerna till extremism. Inte heller finns avgörande bevis som stöder tesen att individer kan radikaliseras av påverkan från internet utan influenser utanför den uppkopplade världen. Icke desto mindre påpekas i rapporten att internet kan möjliggöra att en person blir ytterligare förankrad i en radikaliseringsprocess. För det första genom att internet tillhandahåller stora mängder extremist- och terroristmaterial som kan förstärka individens ideologiska uppfattningar och ge näring åt dennes argument. För det andra genom att individen själv selektivt kan välja mellan tillgängligt material på internet och då välja bort sådant material som inte är i linje med dennes tänkande samt endast ta åt sig av sådant som bekräftar hens redan existerande uppfattning. Dessutom, för det tredje, är det sannolikt enklare för individen att på internet bli vän med likatänkande, som gärna vill diskutera och kommunicera frågor av angivet slag, än vad det är i den fysiska världen utanför internet. Detta gör, enligt Europol, att internet och sociala medier, i vart fall generellt sett, kan anses vara utrymmen där individer som redan är på väg mot radikalisering kan validera sina åsikter och få erkännande och bekräftelse från andra. I sådana fall är internet en möjliggörare (eng. enabler) för (själv-) radikalisering.[23]

Andra områden som särskilt redovisats i IOCTA 2016 beträffande kopplingen mellan internet och terrorism är Darknet, kryptering och it-attacker. Enligt rapporten är Darknet en resurs som i allt högre utsträckning används av terrorister. Även om brottbekämpande myndigheter inte har rapporterat en tydlig trend indikerar utredningar som skett efter terroristattacker att terrorister blivit medvetna

[23] IOCTA 2016 s. 49 f.

om potentialen i Darknetmiljön; att kunna kommunicera med liten risk för upptäckt av brottbekämpande myndigheter och att kunna handla illegala varor och tjänster. Det framstår vidare enligt Europol som en trend med Darknetforum engagerade i terroristideal. Framväxten av sådana forum kan tillskrivas ökningen av tekniskt skickliga individer med anknytning till terroristorganisationerna som delar och sprider sina idéer inom dessa forum. Detta har resulterat i ett antal mindre it-attacker mot mål i Västvärlden. Även om dessa attacker inte haft någon större påverkan framhåller Europol att det finns tendenser som pekar på att terroristgrupper, i takt med att deras kunskap i it-frågor växer och erfarenheter utbyts, bygger en större kapacitet på området.[24]

Brottsbekämpande myndigheter i Europa har också rapporterat ett ökat användande av krypteringsmetoder bland terrorister, inkluderande användningen av krypterade kommunikationsappar. Terroristgrupper använder krypterings- och anonymiseringstjänster för att dölja sina identiteter när de kommunicerar, planerar attacker, köper olagliga varor och genomför ekonomiska transaktioner. Enligt Europol uppvisar terroristerna när det gäller säkerhetsåtgärder i dessa avseenden stora likheter med personer som via internet utnyttjar barn för sexuella ändamål och andra it-brottslingar. Det finns också bevis för att terroristgrupper delar information mellan varandra om hur man förblir ”ospårbar” i syfte att undvika myndigheterna. Ett exempel på detta är den s.k. OPSEC-manualen, som detaljerat förklarar hur man håller sig säker på internet. Manualen är framtagen av en terroristgrupp och spridd bland andra. Även användningen av flerlagerskryptering, såsom VPN och Tor, har enligt rapporten ökat bland terrorister som vill göra sig mer svårfunna på internet.[25]

7.4 Redogörelsen för brottsutvecklingen i SOU 2012:44

I betänkandet *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44) finns en omfattande redogörelse över brottsutvecklingen i Sverige på vissa områden. I detta avsnitt sammanfattas vad som där angavs

[24] IOCTA 2016 s. 50.
[25] IOCTA 2016 s. 50 f.

beträffande terroristbrottslighet, organiserad brottslighet och dödligt våld utifrån det andra av våra två perspektiv, se avsnitt 7.3.1.[26]

7.4.1 Terroristbrottslighet

Den teknologiska utvecklingen och den ökade rörligheten för människor och varor har lett till viktiga förändringar av terroristgruppernas modus operandi sedan 1990-talet. Organisationsstrukturen hos dagens terroristorganisationer skiljer sig från strukturen hos traditionella sådana organisationer på flera områden. Dagens terroristorganisationer karakteriseras av överlappande och sammankopplade transnationella och globala nätverk som i sin tur består av mindre grupper eller celler med ett mindre antal personer. Nätverken är decentraliserade och geografiskt utspridda över hela världen. Den decentraliserade nätverksstrukturen innebär att de mindre grupperna inte vet vilka andra grupper som är med i nätverken. Nätverken har en platt struktur utan tydligt ledarskap, och medlemskapet är flytande till sin karaktär (s. 188 f.).

Under senare år har andelen individer som är födda i Europa och som begått islamistiska terroristdåd ökat. Denna trend kan tyda på att islamistiska terroristgrupper lyckats etablera en mobiliseringsbas för framtida terrorister även i Europa. Ökningen kan ses mot bakgrund av vissa europeiska länders kontraterrorismåtgärder. En annan mobiliseringsgrund kan vara den sorg och ilska som vissa europeiska muslimer upplever till följd av den stundom brutala behandling som invånarna i Irak och Afghanistan utsatts för i samband med USA:s invasion av de båda länderna. För europeiska länder som deltagit i den USA-ledda koalitionsstyrkan i Irak eller i ISAF-styrkan i Afghanistan kan risken för attentat på hemmaplan också ha ökat. För Sveriges del blev det högst tydligt i och med det misslyckade terroristattentatet i december 2010 då ett av attackens motiv enligt

[26] I avsnittet sammanfattas redogörelsen i SOU 2012:44 s. 175–237 utifrån för vår utredning relevanta faktorer. De referenser/källor som låg till grund för den redogörelsen anges inte i vår text. I stället finns hänvisningar i slutet av varje stycke till de sidor i det tidigare betänkandet som sammanfattats. På respektive av dessa sidor finns bakomliggande referenser angivna. En fullständig förteckning över referenserna finns i det betänkandet på s. 865 ff. Det bör noteras att det i SOU 2012:44 anges att redogörelsen över brottsutvecklingen i det betänkandet utarbetats huvudsakligen inom Brå. Vidare ska noteras att när det i detta avsnitt anges nutidsförhållanden avses förhållandena år 2012.

självmordsbombaren var Sveriges militära närvaro i Afghanistan (s. 191).

Dagens terrorister har dragit stor nytta av den decentraliserade kommunikationsstruktur som råder på internet liksom floran av moderna kommunikationsmedel. Den nya informationsteknologin har gjort det möjligt att till låga kostnader samla in och dela med sig av information om olika metoder och strategier, att koordinera attacker och att få nödvändiga resurser. Webbaserade kommunikationsforum fungerar också som en viktig propagandakanal. Att dokumentera terrorattacker har blivit lika viktigt som attackernas fysiska resultat. Genom att lägga upp videofilmer på attentat, självmordsbombares sista ord, länkar till andra terroristgrupper m.m. på bloggar, hemsidor och via diskussionsforum sprider terroristgrupper sin mission till en större skara människor. Vissa forskare och praktiker hävdar också att internet blivit en allt viktigare källa till självradikalisering, dvs. att individer som på internet intresserar sig för våldsförhärligande beskrivningar och ideologier själva blir en del av den våldsbejakande extremistiska miljön. Analyser av terroristattacker visar dock att det snarare är regel än undantag att aktioner föregåtts av någon form av reell kontakt och inte enbart via teknologiska kommunikationsmedel. Säkerhetspolisens kartläggning av islamistiska våldsbejakande extremister i Sverige visade också att omkring 80 procent av de våldsbejakande islamistiska extremister som finns i Sverige hade någon form av social länk till varandra. Detta pekar på att islamistiska våldsbejakande extremister, åtminstone i Sverige, umgås inom mer traditionella sociala nätverk (s. 192 f.).

Mångfalden av kommunikationsmedel har gjort det möjligt för terrorister att ständigt förändra sitt sätt att kommunicera. Den kommersiella tillgången på krypteringsmetoder används för att försvåra underrättelsetjänsternas arbete. Till följd av att västerländska underrättelsetjänster kommit att övervaka digitala kommunikationsmedel i större utsträckning efter 11 septemberattacken har terroristgrupper delvis återgått till att använda traditionella medel som kurirer (s. 193).

Terroristgruppernas nätverksstruktur har visat sig vara särskilt effektiv i det decentraliserade kommunikationssamhället. Kombinationen av korta beslutsvägar och snabba kommunikationsmedel tillåter de informationsbaserade terroristnätverken att snabbt aktivera en mindre grupp, mobilisera resurser eller ändra sina planer om hinder uppstår. Enligt flera forskare är det också just kombinationen

av snabbhet och flexibilitet som gett dagens terroristnätverk ett övertag mot de hierarkiskt informationsbaserade underrättelsetjänsterna (s. 196 f.).

Svårigheterna för myndigheter är följaktligen att det finns större globalt sammankopplade terroristnätverk, mindre terroristgrupper och enskilda terrorister. Dessutom är de mindre grupperna och de enskilda terroristerna inte nödvändigtvis kopplade till några tydliga grupperingar och nätverk. Tidigare pekades på svårigheten att ta fram särskilda ”terroristprofiler” eller att rikta in sig mot specifika grupper. Med andra ord ställer det krav på en bred underrättelseinhämtning i kombination med en välutvecklad förmåga att identifiera personer som utgör ett hot om terroristdåd utifrån den skara människor som visserligen delar terroristernas åsikter men inte begår faktiska terroristbrott. Med hänsyn till att terroristmålen dessutom är mer utspridda och oförutsägbara talar mycket för att det är ett slöseri med resurser att bevaka samtliga tänkbara mål. Även skyddet av egendom och personer förutsätter därför en hög grad av flexibilitet som bygger dels på den nyss nämnda underrättelseinhämtningen, dels på djupgående analyser och dynamiska hotbildsbedömningar av mål (s. 197).

7.4.2 Organiserad brottslighet

Kriminalitet som bedrivs i organiserade former innebär alltid en utmaning för rättssamhället. Samtidigt är det enklare för myndigheterna att övervaka en mer eller mindre kontinuerlig verksamhet med flera personer involverade jämfört med enstaka brott som begås av en ensam gärningsperson. Flera gärningspersoner i en löpande kriminell verksamhet är också i behov av att kommunicera med varandra för att lösa uppkommande problem och lägga grunden för nästa operation. Organiserad brottslighet handlar därför i hög grad om att hemlighålla en verksamhet, både faktiska gärningar och kommunikation. I allmänhet läggs stora resurser ned för att dölja brottsligheten för myndigheterna. Utmaningen för rättsväsendet är därför att med hjälp av hemliga tvångsmedel och andra åtgärder kartlägga den kriminella verksamheten och binda de centrala personerna vid brott (s. 212).

Förr som nu förknippas organiserad brottslighet främst med kriminella entreprenörers handel av förbjudna, ”skattefria” eller ransonerade varor och tjänster. Tvärt emot mediernas bild handlar det mer om affärer och långt mindre om hot, våld och död. Såväl alkohol som narkotika och dopningspreparat liksom tobak, koppleri, människohandel och stölder med efterföljande häleriverksamhet ingår i den organiserade brottslighetens sortiment. Det gör även i någon mån spel och svartarbete i större skala. Dessutom kan olika tjänster utföras, t.ex. indrivning och penningtvätt (s. 213).

Även om alkohol- och cigarettsmuggling varit viktig för organiserad brottslighet, inte minst på det internationella planet, är olika narkotikapreparat de dominerande varorna. Sedan narkotikastrafflagens tillkomst på 60-talet har det straffbara området utvidgats och straffen skärpts och narkotika blivit en viktig kriminalpolitisk fråga som behållit sin prioritet sedan dess. De hårdföra insatserna mot narkotika har dock fört med sig en del oförutsedda konsekvenser. De kriminella marknadsaktörerna har anpassat sig till myndigheternas motåtgärder. Småskalighet, nätverksstruktur och säkerhetsarrangemang har medfört att narkotikaentreprenörerna varit förhållandevis framgångsrika, även om det skett till priset av långvariga fängelsestraff för åtskilliga gärningspersoner (s. 214).

Smuggling och distribution ställer krav på organisation, logistik och kontakter. Allt detta innebär för mycket besvär, engagemang och kostnader för att gärningspersoner ska nöja sig med en enda smuggeltur. Dessutom vill marknaden ha mer, och pengar finns att tjäna. Verksamheter byggs därför upp, utvecklas, byter skepnad och förändras beroende på marknadens svängningar, myndigheternas åtgärder och hur regleringar utvecklas. Det är verksamheten och dess behov av kompetens, kapital, kontakter och logistik som gör det nödvändigt att brottsligheten bedrivs i en organisatorisk struktur. Följaktligen är det inte organisationen som kommer först utan de kriminella aktiviteternas behov, även om åtskilliga av dagens gäng – med eller utan motorcyklar – följer en delvis annorlunda logik. När exempelvis en smugglingsoperation av narkotika genomförs tar den sig organisatoriska former. Någon ger order, kurirer anlitas för riskfyllda uppgifter, andra gör rekognoseringar och liknande förberedelser, särskilda mottagare tar emot partiet och delar upp det. När väl partiet är i hamn, testat och distribuerat går organisationen ned i vänteläge. Organisationens kärna hanterar de ekonomiska frågorna

och sköter betalningar. Medhjälpare sysslar med annat. Proceduren upprepas ofta senare, men medarbetarna kan skifta, liksom sättet att ta in partiet på. Den lösa organisatoriska strukturen är flexibel. I managementtermer är narkotikamarknaden en tämligen primitiv ekonomi som inte ger utrymme för stordriftsfördelar. Verksamheten bedrivs i en ”fientlig” omgivning. Tull och polis lägger stora resurser på att övervaka smugglingsoperationerna och göra beslag. Det innebär begränsade möjligheter att växa. Under dessa spelregler verkar narkotikaentreprenörerna (s. 215).

Organiserat svartarbete kan på ett helt annat sätt än narkotikabrottslighet bedrivas öppet. Dessutom sker arbetet i en legal inramning. Ny teknik och modern styrning gör att arbetet är rationellt. Dessutom har bygg- och anläggningsbranschen pålitligare och resursstarkare beställare än narkotikamarknadens köpare. Sammantaget genererar därför organiserat svartarbete mycket pengar. Illegal hantering av varor som tobak och alkohol är också förhållandevis lönsamt. Ett skäl är att de saknar narkotikans kriminella laddning. Följaktligen kan därför sådana varor hanteras på ett mera öppet sätt (s. 215 f.).

Strategier för att dölja den kriminella verksamheten, skydda huvudmän, varor och pengar, skaffa information och till och med påverka myndighetspersoner är centrala frågor för organiserad brottslighet. I den kriminella miljön finns därför ett stort intresse av att följa myndigheternas arbete, bygga upp kunskap om deras rutiner och på lämpligt sätt anpassa verksamheten och utveckla motstrategier. Även om det finns åtskilliga exempel på kriminell anpassning, är dock den allmänna bilden att gärningspersonerna gör minsta möjliga och väljer enkla lösningar. Påståenden som att kriminella alltid ligger ”steget före” och att myndigheterna alltid ”hamnar på efterkälken” är därför missvisande. Åtskilliga av de personer som är involverade i brottsligheten kännetecknas av bristande långsiktighet, längtan efter snabba pengar och ett festande liv. Det är omständigheter som inte alltid främjar ett högt säkerhetstänkande, och när garden sjunker får hemlig tvångsmedelsanvändning sin stora chans. Ett drag hos organiserad brottslighet är dock förmågan att i varierande grad neutralisera myndigheternas arbete. (s. 217 f.).

Personer i den kriminella miljön är i hög grad beroende av varandra. Lojalitet är därför en viktig byggsten, och ofta rekryteras medarbetare på grundval av gemensamma band genom uppväxt, bekantskapskrets och liknande. Eftersom vissa uppgifter i brottsuppläggen

är tillfälliga och andra är särskilt riskfyllda anses det ofta vanskligt att helt förlita sig på lojalitet i kombination med ett bakomliggande hot om intern bestraffning. Insatserna är för höga. En vanlig organisatorisk metod är därför att projekten bygger på en kärna av personer som litar på varandra. Sedan anlitas mer eller mindre utomstående, t.ex. narkotikakurirer, för olika uppgifter. Sådana personer har inte mycket att berätta för myndigheterna (s. 218 f.).

Som vid annat företagande kräver kriminell verksamhet kommunikation. På ett sätt är behovet ännu större än vid legal verksamhet. Mycket kan gå fel i kriminella projekt, och situationer uppstår som måste hanteras och pareras. Det stora kommunikationsbehovet ska dock vägas mot att gärningspersonerna anser sig ha en förhållandevis god uppfattning om hur polis och tull arbetar. De flesta räknar därför med att hemlig avlyssning av elektronisk kommunikation är allmänt förekommande. Även hemlig rumsavlyssning uppfattas som ett realistiskt hot. Det är dock inte ovanligt att myndigheternas förmåga och resurser överskattas. Motsatsvis förekommer också att övermod leder till att myndigheternas förmåga underskattas. Det finns exempel på gärningspersoner som rakt in i polisens dolda mikrofoner skryter om hur de lyckats överlista myndigheterna. Personer involverade i organiserad brottslighet ägnar stor möda åt att kommunicera utan att myndigheterna ska kunna avlyssna samtal. Ett vanligt förfaringssätt är att ha många telefoner och oregistrerade kontantkort. För att ytterligare minska risken används kodord, och samtalen sker i förtäckta ordalag. Främmande språk, ibland med ovanliga dialekter, förekommer också. För att polisen ska ha svårt att forcera kommunikation använder vissa kriminella webbaserade krypterade telefonitjänster. Några har även tillgång till satellittelefon. Mail används också, och det finns exempel på hur gemensamma mailkonton utnyttjas för att undgå att meddelanden sänds mellan konton. Slutsatsen är att organiserad brottslighet är särskilt svårbekämpad, och inte minst det förhållandevis höga säkerhetstänkandet hos gärningspersonerna innebär att myndigheterna måste använda ett brett spektrum av kartläggnings- och spaningsmetoder. Det går knappast att förlita sig på en metod, utan flera åtgärder måste sättas in för att bygga det pussel som kännetecknar polisens arbete mot organiserad brottslighet. Flera metoder innebär också att det finns en öppenhet från myndigheternas sida att dra

nytta av de situationer när garden sänks, misstag begås och rutiner inte följs (s. 220 ff.).

I takt med att samhället mobiliserar mot organiserad brottslighet är ett rimligt antagande att motstrategierna utvecklats. Ökad försiktighet och ännu säkrare kommunikationer bör vara svar på myndigheternas åtgärder (s. 227).

7.4.3 Dödligt våld

Under 2000-talet begicks i genomsnitt 90 brott per år av fullbordat dödligt våld, vilket motsvarar en minskning med omkring 25 procent sett i förhållande till befolkningsutvecklingen i jämförelse med perioden från mitten av 1970-talet till 1990-talet. Det vanligaste brottsscenariot är att de inblandade känner varandra väl, antingen som partner och familjemedlem eller som bekant och vän. Närmare två tredjedelar av det fullbordade dödliga våldet sker i anknytning till familje- eller partnervåld och spontanbråk eller någon form av mindre dispyt mellan bekanta. Affektbrott begås ofta under alkoholberusning, och kniv är det våldsmedel som används mest. Kvinnor utgör merparten av alla offer för familje- och partnervåld, medan i brottskategorin spontanbråk och dispyter är offren främst män. I båda kategorierna är gärningspersonen i regel en man (s. 227 f.).

Samtidigt som fullbordade dödliga våldsbrott minskar har andelen sådana brott som kategoriseras som kriminella konflikter ökat. Kategorin innefattar olika former av konflikter. Det kan omfatta allt från två missbrukare som hamnar i en dispyt över småskaliga knarkskulder till massmedialt mer uppmärksammade kriminella uppgörelser. Till skillnad från affektbrott begås dessa brott i större utsträckning utomhus och med illegala skjutvapen. Enligt Brottsförebyggande rådet tyder senare års ökning av illegala skjutvapen och fler kriminellt relaterade dödliga våldsbrott i viss mån på att det dödliga våldet mellan vuxna män håller på att ”professionaliseras” (s. 228).

Affektbrott är svåra att förebygga. Brotten är spontana och sker ofta inomhus. Dessutom, eftersom brotten främst sker mellan tidigare bekanta och familjemedlemmar, är det svårt för utomstående att få insyn i den kommunikation som sker innan brottet begås. De förebyggande åtgärderna som visat sig mest effektiva består därför företrädesvis av socialpolitiska åtgärder. Mot denna bakgrund tycks

hemliga tvångsmedel främst vara till nytta i utredningar av redan begångna affektbrott. Beträffande brottskategorin kriminella konflikter bör det betonas att tidigare forskning pekat på att även våldsbrott kopplat till organiserad brottslighet ofta är affektbrott och därför, på nyss nämnda grunder torde vara svåra att förebygga med preventiva tvångsmedel (s. 229).

7.5 Utvecklingen från 2012 till i dag

De tendenser som nyss redovisats gör sig i allt väsentligt gällande även i dag. Emellertid har ytterligare fem år förflutit sedan Utredningen om vissa hemliga tvångsmedel lämnade sitt betänkande varför det är angeläget att redovisa faktorer som kan sägas ha påverkat eller riskerar att påverka brottsutvecklingen i Sverige.

7.5.1 Terroristbrottslighet

Risken för terroristattentat i Sverige

Konflikterna i Mellanöstern har påverkat Sverige och Europa på flera sätt. Säkerhetspolisen, som i Sverige ansvarar för kontraterrorism (dvs. underrättelsearbete och vidtagande av åtgärder för att förhindra terroristattentat i Sverige och mot svenska intressen utomlands) har i allmänt tillgängliga källor publicerat bland annat följande. De pågående konflikterna i Mellanöstern var under 2015 den i särklass mest drivande faktorn bakom terrorismen. Ett exceptionellt högt antal svenskar har anslutit sig till sunniextremistiska terroristgrupper verksamma i Syrien och Irak. De flesta som reser är unga män mellan 18 och 30 år, födda i Sverige med minst en förälder född utomlands och saknar eller har låg inkomst. En tredjedel har kriminell bakgrund. Under 2015 ökade dock antalet kvinnor och barn som reste. Personer som ansluter sig till terroristgrupper kan inspirera andra att ansluta sig eller begå terroristbrott i Sverige. Den stora majoriteten reser till Syrien för att ansluta sig till Daesh[27]. De som överlever och väljer att återvända har samlat på sig ny kunskap, nya kontakter,

[27] Daesh benämner sig själv Islamiska staten (IS) och har tidigare benämnts Isis och Isil. Se vidare nedan.

sänkt sin våldströskel och kan bli statusgestalt för andra extremister. De återvändare som fortfarande anser att ideologin är korrekt fortsätter troligtvis att verka i Sverige inom stödverksamhet eller radikalisering. En del är traumatiserade eller ångerfulla. Ett fåtal utgör ett attentatshot. Internet är en betydelsefull kontaktyta och inspirationskälla. Ju fler kontakter som knyts i terrorismsyfte i Sverige och utomlands desto fler fall och svårupptäckta aktörer kommer Säkerhetspolisen ha att göra med.[28]

Chefen för Säkerhetspolisen ansvarar för vilken terrorhotnivå på den s.k. hotnivåskalan som ska gälla i Sverige vid varje givet tillfälle. Från hösten 2010 och fram till terroristattentaten i Paris i november 2015 gällde terrorhotnivå 3, vilket innebär förhöjd risk för terroristattentat. Under perioden från november 2015 till och med den 2 mars 2016 gällde i stället terrorhotnivå 4, som betyder att det är hög risk för terroristattentat i Sverige. Sedan det senare datumet har nivå 3 gällt igen.

Den information som chefen för Säkerhetspolisen lägger till grund för beslutet om vilken hotnivå som ska gälla kommer bland annat från Nationellt centrum för terrorhotbedömning (NCT), som är en permanent arbetsgrupp med personal från Säkerhetspolisen, Försvarets radioanstalt (FRA) och Militära underrättelse- och säkerhetstjänsten (Must). NCT:s uppgift är att göra strategiska bedömningar av terrorhotet mot Sverige och svenska intressen på kort och lång sikt. I NCT:s rapport *Helårsbedömning* år 2017 (NCT-rapporten), där terrorhotet mot Sverige från islamistiskt motiverad terrorism bedöms utgöra ett förhöjt hot, anges bland annat följande. Sverige kommer sannolikt att betraktas som ett legitimt mål för våldsfrämjande islamistiska aktörer såväl i Sverige som utomlands. Det finns ett fåtal aktörer som troligen både kommer ha avsikt och förmåga att genomföra våldshandlingar som skulle kunna rubriceras som terroristattentat i Sverige. Bland dessa finns dels de som rest och återvänt efter att ha stridit med våldsfrämjande islamistiska grupper, dels individer som inte rest, men som inspirerats av våldfrämjande islamistisk propaganda. De våldsfrämjande islamisterna i Sverige inspireras huvudsakligen av en våldsfrämjande ideologi enligt vilken terroristattentat mot mål i västvärlden anses legitima och som förmedlas av grupper som t.ex. Daesh och al-Qaida. Flera andra

[28] Se www.sakerhetspolisen.se/kontraterrorism/hot-och-hotbild.html

europeiska länder är utpekade mål för Daesh och gruppen prioriterar troligen vissa stater före Sverige vid styrd attentatsplanering.

Syrien och Irak är fortsatt de främsta resmålen för svenskar som vill ansluta sig till våldsfrämjande islamistiska grupper. Under det senaste året har antalet resenärer till våldsfrämjande islamistiska grupper minskat. Nedgången är sannolikt ett resultat av flera faktorer, däribland den skärpta kontrollen av den turkiska gränsen och Daeshs alltmer trängda militära läge. Majoriteten av de svenska resenärerna som befinner sig i Syrien och Irak har anslutit sig till Daesh, men under 2016 har de flesta nya resenärerna i första hand anslutit sig till Jabhat Fatah al-Sham eller närliggande grupper. Jabhat Fatah al-Sham kallade sig tidigare för Jabhat al-Nusra eller Nusrafronten och har varit en del av al-Qaidas nätverk. Ett mindre antal av de individer som återvänt från träning eller strid med våldsfrämjande islamistiska grupper kommer troligen att utveckla avsikt att genomföra attentat även mot mål i västvärlden, främst i hemlandet eller i angränsande länder.

Daesh

Den sunniextremistiska rörelsen Daesh existerade från början som en del i al-Qaidas nätverk, men bröt sig loss 2013 under namnet Isis (Islamiska staten i Irak och Syrien) och har även kallat sig Isil (Islamiska staten i Irak och Levanten). I slutet av juni 2013 bytte rörelsen namn till IS (Islamiska staten) – då den ansåg sig ha raderat ut gränsen mellan Irak och Syrien. I juni 2014 utropade organisationen officiellt ett sunnimuslimskt kalifat. Utvecklingen av Daesh har gått mycket snabbt och farhågorna för vad organisationen kan åstadkomma har ökat. Från att tidigare ha nämnts främst som en al-Qaidainspirerad grupp bland flera[29] framhålls nu från vissa håll att Daesh utgör den ledande aktören inom global våldsfrämjande islamism.[30]

Sedan kalifatet utropades har Daesh utfört eller inspirerat till åtminstone 50 attacker i 18 länder. Attackerna har dödat 1 100 personer och skadat mer än 1 700. Flertalet av Daeshs attacker har genomförts

[29] Se t.ex. *Säkerhetspolisens årsbok för 2014* s. 33.
[30] Se t.ex. NCT:s rapport *Helårsbedömning* år 2016 s. 2.

i Mellanöstern eller Nordafrika, men även Europa har drabbats av attackerna.[31]

Flera Europeiska jihadister har, enligt Europol, framstående positioner inom Daesh och kommer sannolikt upprätthålla kontakt med terroristnätverk i sina hemländer. Attackerna i Paris i november 2015 introducerade enligt Europol Daeshs taktik med användande av mindre vapen i kombination med personburna improviserade spränganordningar i självmordsvästar, vilka konstruerats för att orsaka omfattande förödelse. Sättet på vilket attackerna förbereddes och utfördes – kartlagt av återvändare som högst troligt fick direktiv från Daeshs ledning, och inkluderande lokala rekryter för genomförandet – har lett Europol till bedömningen att liknande attacker kan komma att genomföras i EU.[32]

Från flera håll framhålls särskilt Daeshs (och al-Qaidas) förmåga att rekrytera nya sympatisörer via internet och sociala medier. I regeringens skrivelse Förebygga, förhindra och försvåra – den svenska strategin mot terrorismen anges följande i avsnittet rörande hotbilden mot Sverige och svenska intressen.[33]

> Internet och sociala medier är centrala verktyg för den globala al-Qaida-inspirerade rörelsen i spridandet av propaganda och för radikalisering och rekrytering. Företrädare för denna rörelse har uppmanat till mindre attentat utförda med enkla medel som stick- och huggvapen, enklare skjutvapen eller bilar. På sociala medier ses också tecken på att den retorik som al-Qaida och Isil använder normaliseras, även hos mycket unga personer i Sverige. Enskilda personer i Sverige radikaliseras via internet och riskerar att drivas till att begå våldshandlingar här eller utomlands. Vidare finns en utveckling med attentat eller attentatsförsök där avsikten bottnar i individuella motiv. Sådan avsikt kan uppstå i samband med upplevda begränsningar i eller upplevda kränkningar av den individuella friheten.

Motsvarande beskrivningar beträffande Daeshs förmågor har lämnats även i andra sammanhang. I Europols rapport *European Union Terrorism Situation and Trend Report (TE-SAT) 2016* anges t.ex. att Daesh bedriver en i flera avseenden framgångsrik propaganda genom internet och sociala medier. Främst används, enligt Europol, internet och sociala medier alltså för spridning av propagandamaterial, men

[31] TE-SAT 2016 s. 6.
[32] TE-SAT 2016 s. 6.
[33] Regeringens skrivelse 2014/15:146 s. 4.

rekrytering av nya terrorister och finansiering är verksamheter som också märkts bland terrororganisationernas aktivititer på internet.[34]

Propagandan är också i hög utsträckning skräddarsydd för olika åhörare. Det finns exempel på att Daesh har sänt ut propaganda på flera olika språk, anpassad till respektive målgrupps kulturella bakgrund. Daeshmedlemmar av olika ursprung framträder t.ex. därvid i olika videomeddelanden och riktar sig mot sina landsmän för att dessa ska ansluta sig till organisationen eller utföra terroristattentat i sina hemländer.[35]

I TE-SAT-rapporten för 2017 konstateras att det under 2016 skedde en minskning av individer som reste till konfliktzonerna i Syrien och Irak för att delta i jihadisternas verksamhet. Antalet återvändare till EU bedöms också öka om Daesh, som det numera verkar, besegras militärt eller kollapsar. En sådan ökning av återvändare bedöms av Europol stärka de inhemska jihadiströrelserna i EU och i konsekvens med det öka hotet från dessa.

Skärpta regler för terroristbrottslighet

Sedan 2012 har en rad lagändringar skett på området som gäller terrorism och terroristrelaterad brottslighet. Lagen om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet har ändrats i två omgångar. Bland annat har viss ny brottslighet lagts till i katalogen beträffande brottslighet som ska anses särskilt allvarlig.[36] Dessutom har det straffbelagts att motta utbildning avseende särskilt allvarlig brottslighet (tidigare var det endast kriminaliserat att utbilda för särskilt allvarlig brottslighet) och att resa eller påbörja resa i terrorismsyfte.[37] Vidare har ändringar skett i lagen om straff för terroristbrott till följd av vissa nya brottsbeteckningar (synnerligen grovt vapenbrott och grovt olaga hot). Därtill har underlåtenhet att förhindra terroristbrott kriminaliserats.[38] I lagen om straff för finansiering av särskilt allvarlig brottslighet i vissa fall har det straffbelagts

[34] TE-SAT 2016 s. 16 f. Se också avsnitt 7.3 ovan.
[35] TE-SAT 2016 s. 16.
[36] Se prop. 2013/14:212 s. 33.
[37] Se prop. 2015/16:78 s. 70 ff. jämförd med prop. 2009/10:78 s. 60 f.
[38] Se bland annat prop. 2015/16:113 s. 101.

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.[39]

De nu nämnda ändringarna har fått följdeffekter i den meningen att fler brott än vad som gällde 2012 ingår i den katalog av brott, för vilka misstanke av viss grad ska föreligga, som kan föranleda hemlig avlyssning av elektronisk kommunikation och viss annan tvångsmedelsanvändning.

Nationell strategi mot terrorism och andra åtgärder

I augusti 2015 antog regeringen en ny strategi mot terrorism, *Förebygga, förhindra och försvåra – den svenska strategin mot terrorism* (skr. 2014/15:146). Denna ersatte den tidigare strategin Ansvar och engagemang – en nationell strategi mot terrorism (skr. 2011/12:73). Som namnet antyder delas arbetet med att undvika att terrorattentat genomförs i Sverige in i tre områden; förebyggande, förhindrande och försvårande. I strategins sammanfattning anges följande.

> Ett särskilt fokus ligger på området Förebygga. Åtgärderna på detta område syftar till att motverka radikalisering och rekrytering till extremist- och terroristgrupper och att påverka individers avsikt att begå eller stödja terroristbrottslighet. På så sätt kan man minska basen för rekrytering till terrorism. Området Förhindra handlar om att motverka och minska förmåga och möjlighet att begå terroristattentat medan Försvåra handlar om att skapa och upprätthålla skydd för individer och minska samhällets sårbarhet för terroristattentat. Om ett terroristattentat ändå genomförs måste samhället också kunna hantera konsekvenserna av det.

Utförda terroristattentat

Som redan nämnts har sedan 2012 flera angrepp mot mål såväl i som utanför Europa utförts av terrorister. I spåren av situationen i Mellanöstern har en rad allvarliga terrordåd under perioden utförts i de områdena. Med anledning av att utredningen i denna del syftar till att klarlägga behovet av ett nytt hemligt tvångsmedel i Sverige har vi

[39] Se prop. 2015/16:78 s. 69.

emellertid begränsat oss till att redogöra för några av de illdåd som skett i Europa under senare tid.

Under 2015 rapporterades 211 misslyckade, omintetgjorda eller genomförda terrorattacker i EU. Attackerna resulterade i 151 dödsfall, varav den absoluta merparten var effekter av terrordåden i Paris i januari och november. Huvuddelen av de rapporterade attackerna (som kategoriserats[40]) var s.k. separatistisk terrorism (68 fall), följt av attacker kopplade till islamistisk extremism (17), vänsterextremism (13) och högerextremism (9). Klart dödligast av attackerna var den islamistiska extremismen som ledde till 150 dödsfall, varav 148 vid angreppen mot Paris i januari och november. Det bör anmärkas att de 17 attackerna utförda av islamistiska extremister bestod av angreppen i Paris (15 attacker vid två tillfällen) och angrepp i Danmark (två attacker av en gärningsman samma dag).[41]

Attackerna i Paris var alltså de som orsakade mest skada 2015. I januari attackerades satirtidningen Charlie Hebdo av två bröder som var anslutna till grupperingen al-Qaida i Arabiska Peninsula (AQAP) vilket ledde till döden för tolv personer. Två dagar senare dödades fyra personer efter att de tagits som gisslan i en judisk butik av en person som sa sig tillhöra Daesh. Den 13 november dödades 130 personer och 368 skadades när terrorister under kort tid angrep flera olika mål i Paris, bland annat nationalarenan Stade de France där en landskamp i fotboll pågick och den fullsatta konsertlokalen Bataclan.

Under 2016 och 2017 har ytterligare en rad terrorangrepp inträffat i Europa. Bryssel drabbades den 22 mars då tre explosioner inträffade på morgonen; två vid flygplatsen Zaventem och en på ett tunnelbanetåg vid stationen Maalbeek. I attacken dödades 32 personer samt de tre självmordsbombarna. Över 300 personer skadades. Daesh har tagit på sig ansvaret för attackerna.

På Frankrikes nationaldag den 14 juli 2016 körde en lastbil genom folkmassor som samlats för att fira och se på fyrverkerier. Över 80 personer dödades och över 200 skadades. Daesh har tagit på sig dådet.

[40] Det bör anmärkas att Storbritannien, som är det land som rapporterat flest attacker (103 st.), inte redovisar vilken tillhörighet terroristen haft.
[41] TE-SAT 2016 s. 10.

Den 19 december 2016 använde sig ytterligare en terrorist av nyss nämnda modus när denne i Berlin körde in i en folksamling vid en julmarknad varvid minst 12 personer omkom och 48 skadades. Även detta attentat har Daesh tagit på sig ansvaret för.

Även Storbritannien har drabbats i samband med attacker i Manchester och London under våren 2017. I samband med attackerna har över 30 personer omkommit. Också i bl.a. Finland (Åbo), Ryssland (Sankt Petersburg) och Spanien (Barcelona) har attacker med dödlig utgång skett under 2017.

Under utredningen har ett attentat också skett i Sverige. På eftermiddagen den 7 april 2017 kördes en lastbil in på den välbesökta gågatan Drottninggatan i Stockholm med följden att fem personer avled och många personer skadades. En gärningsman greps och är för närvarande häktad, på sannolika skäl misstänkt för terroristbrott.

7.5.2 Organiserad brottslighet

Kriminella nätverk och grupperingar

Sedan SOU 2012:44 författades har Brå, efter ett regeringsuppdrag, i rapporten *Kriminella nätverk och grupperingar – polisers bild av maktstrukturer och marknader* (Rapport 2016:12) gjort försök att tydligare definiera begreppet organiserad brottslighet och att underlätta analysen av den kriminella miljön. Detta har skett genom att Brå i rapporten skapat fyra grupp- och nätverkskategorier som kan sägas återfinnas inom vad som traditionellt ansetts utgöra organiserad brottslighet. De fyra kategorierna är:

– Självdefinierade grupper
– Externfinansierade grupper
– Icke-namngivna grupper
– Projektbaserade konstellationer

Självdefinierade grupper omfattar grupper som själv lyfter fram sin grupptillhörighet i form av namn, attribut och medlemskap. Exempel på dessa är mc-gäng som Hells Angels eller Bandidos. *Externdefinierade* grupper är grupper som inte själva beskriver sin grupptillhörighet genom namn symboler och attribut utan i stället tilldelas

namn, av antingen polisen eller media, såsom Backagänget i Göteborg. *Icke-namngivna* grupper är ett samlingsnamn för olika typer av relationsbaserade nätverk som varken har ett självtilldelat namn eller ett externt tilldelat namn. När personer från en eller flera av dessa grupp- eller nätverkskategorier går samman för att utföra ett vinstdrivande kriminellt projekt bildas något som omfattas av den fjärde kategorin, *projektbaserade konstellationer*.[42] Trots skillnaderna mellan olika grupper och nätverk finns enligt Brå en central universell beståndsdel som genomsyrar dem alla: skrämselkapital.

Enligt Bråsstudie har kartan för den kriminella miljön i Sverige ritats om de senaste tjugo åren. Det nya är att antalet sammanslutningar i den kriminella miljön kraftigt ökat samtidigt som det också har tillkommit självdefinierade grupper med namn och attribut som tydligt visar grupptillhörighet. Enligt Brå har särskilt själv- och externfinansierade grupper blivit något av ett föredöme och en inspirationskälla i den kriminella miljön. Mediernas rapportering har ytterligare bidragit till att lyfta fram konceptet med grupperingar. När väl stenen är i rullning har myndigheterna haft svårt att hejda utvecklingen. Lojaliteten inom grupperingarna är emellertid många gånger illusorisk. Även om de som tillhör samma sammanslutning kan backa upp varandra när det gäller, är det mycket vanligt att personer i den kriminella miljön är självcentrerade och sätter sig själva i främsta rummet. Det är också ett av skälen till den mobilitet mellan olika grupper och nätverk.

Syftet med grupperingarna är enligt Brå ytterst sällan att fungera som kriminella organisationer i betydelsen att vinstdrivande brottslighet utförs av dess medlemmar tillsammans och i viss bestämd ordning, ungefär som vilket företag som helst. I stället är det de enskilda individerna som ser fördelar med att ingå i en gruppering (t.ex. trygghet och kontakter).

Från samhällets sida har tillväxten av grupper och nätverk blivit ett problem. Särskilt själv- och externdefinierade grupper samt icke namngivna grupper med koppling till förorter och familjer utmanar myndigheternas förmåga att upprätthålla lag och ordning. Konflikter som uppstår mellan individer och grupper i den kriminella miljön leder till skjutningar på allmän plats. Det kan leda till att människor känner otrygghet och kan minska legitimiteten hos samhällets

[42] Brå-rapporten 2016:12, s. 28 f.

institutioner. Särskilt gäller det de socialt utsatta områden där grupper har fått för stort handlingsutrymme. Sammanfattningsvis finns det därför enligt Brå starka skäl att motverka grupperingarna.[43]

Polisens bild av organiserad brottslighet

I en rapport från maj 2015 har polisen redovisat en nationell lägesbild över organiserad brottslighet i Sverige. Rapportens syfte var bland annat att öka kunskapen om organiserad brottslighet. I rapporten delade Polismyndigheten in kriminella aktörer i följande fyra kategorier.

- Kriminella aktörer baserade i Sverige
- Kriminella aktörer baserade i Sverige och i utlandet
- Kriminella aktörer baserade i utlandet
- Ideologiskt motiverade brottsaktiva aktörer.

Enligt rapporten är de flesta *kriminella aktörer baserade i Sverige* bosatta här och svenska medborgare. Även om de är baserade i Sverige har de ofta internationella kontakter som används för att underlätta och möjliggöra brott. Gemensamt ursprung och gemensam uppväxt är förtroendeskapande och sammanhållande faktorer för kriminella nätverk. I Sverige finns ett flertal utsatta geografiska områden som har problem med lokala kriminella nätverk. I områdena har sådana nätverk en märkbar negativ påverkan på tryggheten. Brottsligheten i vissa områden blir alltmer avancerad och de lokala kriminella nätverkens påverkan sprids då även utanför området. Kontaktnät mot utlandet ger förutsättningar för brottslighet inom många områden. Till exempel möjliggörs människohandel och människosmuggling till Sverige primärt av kriminella nätverk som baseras på ursprung och kontakter i utlandet. I stor utsträckning gäller detta även narkotika- och vapensmuggling. Inom Sverige begår nätverken även andra brott. [44]

När det gäller *kriminella aktörer baserade i Sverige och utlandet* är den internationella dimensionen och hur förankring både i utlandet

[43] Brå-rapporten 2016:12, s. 20 f.
[44] *Polisens rapport om organiserad brottslighet 2015* s. 6.

och i Sverige påverkar brottsligheten enligt rapporten utmärkande för dessa kriminella nätverk. Internationella kontakter till hemländer, forna hemländer eller personer med samma ursprung boende i andra länder är därvid en central aspekt. Kontakterna utnyttjas i olika kriminella syften och möjliggör eller förenklar vissa typer av brott, till exempel smugglingsbrott. Kriminella nätverk som är baserade i både Sverige och Afrika, Sydamerika, västra Balkan eller Sydostasien ägnar sig till stor del åt narkotikabrottslighet. Kriminella nätverk baserade i Sverige och på västra Balkan ägnar sig även åt vapensmuggling. Även människohandel bedrivs av kriminella aktörer som är baserade i Sverige och utlandet. Människohandel inom EU med EU-medborgare har ökat de senaste åren. Gärningsmän och offer kommer vanligtvis från samma land.[45]

Kriminella aktörer baserade i utlandet uppehåller sig enligt rapporten i Sverige enbart för att begå brott. En stor del av mängdbrotten i Sverige begås av sådana nätverk.[46]

De *ideologiskt motiverade brottsaktiva aktörerna* har enligt rapporten en ideologisk drivkraft bakom sin brottslighet.[47]

Enligt rapporten har en ökad våldsanvändning bland kriminella individer noterats, vilket är ett av de största problemen kopplade till organiserad brottslighet. Våldet från kriminella aktörer ökar både i omfattning och grovhet. Det är alltså fler personer som är mer benägna att använda våld samtidigt som våldet blir grövre. Användandet av grovt våld blir enligt rapporten också vanligare bland yngre personer. Vidare bedöms i rapporten tillgången till skjutvapen vara stor bland kriminella. De hanterar och brukar således skjutvapen i allt större omfattning och dessutom har konverterade skjutvapen och automatvapen blivit vanligare.[48]

I rapporten tas också upp det faktum att it-brott och it-relaterad brottslighet i dag är en fullt integrerad del av organiserad brottslighet. Tjänster för olika tekniska brottsupplägg eller genomförande av it-attacker kan köpas och hyras. Detta gör att kriminella individer och nätverk snabbt kan höja sin kapacitet. Överbelastningsattackers

[45] *Polisens rapport om organiserad brottslighet 2015* s. 7.
[46] *Polisens rapport om organiserad brottslighet 2015* s. 7.
[47] *Polisens rapport om organiserad brottslighet 2015* s. 7.
[48] *Polisens rapport om organiserad brottslighet 2015* s. 7 f.

antal och skadeverkningar ökar och det finns enligt rapporten exempel på överbelastningsattacker som påverkat samhällsfunktioner.[49]

Som en konklusion anges i rapporten att kriminell samverkan är föränderlig. Olika modus, samverkansformer och samhällsförändringar ger möjlighet till nya brott. De tydligaste slutsatserna enligt rapporten är att kriminell samverkan är gränslös, att organiserad brottslighet breder ut sig samtidigt som den blir mer specialiserad samt att den tidigare förutspådda övergången till allt mer ekonomisk brottslighet och bedrägerier har skett.[50]

Drogmarknaden och den organiserade brottsligheten

Den illegala handeln med narkotika är ett globalt problem och ett allvarligt hot mot säkerhet och utveckling i delar av världen och utgör en central del i den organiserade brottsligheten i Sverige och internationellt. I en rapport som Polismyndigheten och Tullverket gemensamt arbetat fram anges bl.a. följande om den aktuella drogsituationen i Sverige.[51]

Marknaden för olaglig narkotika och andra droger utgör en mycket dynamisk kriminell marknad i Europa. Likt den legala marknaden drivs utvecklingen framåt på grund av marknadskonkurrens och tekniska innovationer där världshandelns globala flöden och transporter utnyttjas av de kriminella nätverken, och där aktörerna ständigt utvecklar sina metoder för att undkomma upptäckt och lagföring. Även om Sverige i princip uteslutande är ett konsumtionsland av droger krävs det i hög utsträckning internationellt samarbete mot den gränsöverskridande narkotikabrottsligheten för att begränsa tillgången på narkotika i Sverige.

Drogmarknaden har under 2000-talet uppvisat stora förändringar, nationellt och internationellt. Narkotikabrott i alla dess former utgör ett s.k. ingripande- och spaningsbrott vilket medför att nivåerna på den upptäckta narkotikabrottsligheten är beroende av myndigheternas förmåga att upptäcka, ingripa och förebygga den illegala verksamheten. Narkotikahandeln på internet tenderar att öka i

[49] *Polisens rapport om organiserad brottslighet 2015* s. 9.
[50] *Polisens rapport om organiserad brottslighet 2015* s. 11.
[51] *Drogsituationen i Sverige – Lägesbild i Sverige 2013–2016.* Informationen i avsnittet återfinns i rapporten på s. 7–12.

omfattning och formerna för handeln är föränderliga, delvis som en respons på rättsvårdande myndigheters åtgärder. En ökad konkurrens mellan säljare medför högre krav på tillförlitlighet, kvalitet och prissättning.

Nätförsäljningen har medfört att drogerna i dag är lättillgängliga, och inte geografiskt bundna, vilket avspeglas i att antalet beslag som görs i post- och kurirflödet har ökat stadigt. Drogerna på internet exponeras för nya målgrupper och utmanar den traditionella bilden av narkotikamarknadens aktörer. Tillskottet på nya missbruksubstanser på internet, flera som utgör starkare alternativ till de traditionella drogerna medför stora risker för konsumenterna. 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 nätet.

Aktörer som organiserar införseln av narkotika till Sverige har ofta kontakter till flera preparatrelaterade nätverk. De köper in partier med flera olika droger som sedan hanteras parallellt av de kriminella aktörer och nätverk i Sverige som smugglar, distribuerar och säljer narkotikan. Metoderna för smuggling och distribution av narkotika är ständigt föränderliga och den illegala handeln av narkotika styrs av vinstdrivande faktorer och av de kriminellas riskbedömningar av olika alternativa tillvägagångssätt. Förmågan att arbeta långsiktigt mot strategiska länder och att identifiera aktörer i hela kedjan från smuggling och distribution till försäljning på gatunivå är av central betydelse för att bekämpa den organiserade narkotikabrottsligheten.

Även om narkotika i hög utsträckning ingår som en del i de kriminella nätverkens multikriminalitet utgör den ofta basen i den illegala verksamheten. Narkotikan spelar en viktig roll i unga personers koppling till organiserad brottslighet och i etablerandet av en kriminell identitet. Yngre individer nyttjas ofta till att sälja narkotika i lokala kriminella nätverk och i andra typer av nätverk, exempelvis inom den kriminella mc-miljön. De kriminella nätverk i Sverige som i hög utsträckning är involverad i narkotikasmuggling till Sverige har ofta goda kriminella kontaktytor i Europa och kapacitet att bedriva om- fattande smuggling. Narkotikan utgör vidare en gemensam nämnare i de kriminella aktörernas kontaktnät där de internationella kontakterna är av särskild betydelse.

Förekomsten av narkotika påverkar vidare den upplevda tryggheten i lokalsamhällen. Det sker bland annat genom den öppna narkotikaförsäljningen som pågår i anslutning till bostadsområden och centrumanläggningar i vissa lokalområden, och som involverar ungdomar i området. I kriminella konflikter och uppgörelser, som tar sig uttryck i den offentliga miljön med risk för skada på personer som rör sig där, förekommer narkotika många gånger som en möjlig motivbild. Ofta i form av obetalda skulder eller i konkurrenssituationer där syftet är att etablera, vidmakthålla eller expandera marknadsandelar.

Den webbaserade drogmarknaden har under 2000-talet visat på en omfattande tillväxt, och det finns indikationer på att personer i Sverige i högre utsträckning än i andra länder köper narkotika på internet. Problematiken med den webbaserade droghandeln har varit känd för myndigheterna sedan slutet av 1990-talet. Fenomenet utgör en utmaning för de brottsbekämpande myndigheterna liksom för narkotikapolitiken i stort, oavsett om internet används direkt för att sälja och köpa narkotika eller indirekt för marknadsföring, för opinionsbildning eller för att dela erfarenheter. Webbaserade drogmarknader är extra svåra att kontrollera eftersom tillverkare, leverantörer, återförsäljare, webbhotell och betaltjänster ofta finns i olika länder. Samtidigt har komplexiteten ökat, och fortsätter öka, med kryptovaluta, anonymiserad internettrafik och dolda marknadsplatser.

Fram till 2011 bestod näthandeln framför allt av preparat som inte var narkotikaklassade i försäljningslandet. Även de traditionella och narkotikaklassade preparaten såldes via internet men försäljningen skedde mer dolt och inte i samma omfattning. Köpare och säljare kunde vid denna tid komma i kontakt med varandra, men en enskild säljare hade svårt att nå de bredare massorna. Detta förändrades 2011 då marknadsplatsen Silk Road startades på Tornätverket (se avsnitt 6.3.3), ett kryptonätverk där säljare anonymt kan annonsera ut narkotika till försäljning. Utvecklingen medförde att de traditionella drogerna kom att få ett större utrymme på nätet och att inrikeshandeln, droger som säljs av svenska säljare och som levereras inom Sverige, påtagligt har ökat i betydelse. När Silk Road stängdes ned 2013 av FBI fanns där över 100 svenska säljare, varav 35 aktiva. Marknaden kom därefter att delas upp mellan ett antal aktörer där den svenska marknadsplatsen för droger, Flugsvamp, har

varit avgörande för ökningen av den svenska inrikeshandeln. Det finns i dag runt 300 säljare på marknadsplatsen varav 85 är aktiva. Kryptomarknaden för illegala droger (som sker på Darknet) uppskattas i internationella studier endast utgöra en nischad del av den totala drogmarknaden men är stadigt växande. Antalet transaktioner som kan härledas till narkotika på kryptomarknaden (Darknet) bedöms ha tredubblats sedan Silk Road stängdes 2013, samtidigt som intäkterna fördubblats. Nationellt bedöms försäljningen av narkotika vara påtaglig i förhållande till andra europeiska länder och nya trender identifieras ofta först i Sverige.

Säljarna i den webbaserade droghandeln inkluderar allt från tidigare dömda grova narkotikabrottslingar välkända i den kriminella miljön till personer utan tidigare, för myndigheterna, känd brottserfarenhet. Inledningsvis är en säljare ofta inriktad på en särskild, eller en grupp, av missbrukssubstanser medan de mest etablerade säljarna kan erbjuda ett brett och marknadsanpassat utbud. Skillnaderna i omsättningen, och i det ekonomiska överskottet, är stora mellan olika säljare och få nätsäljare har förmåga att omsätta omfattande mängder. Med fler aktörer på marknaden ses också en ökad konkurrens.

Kriminellas säkerhetsmedvetande

Som framgått tidigare i texten synes kriminella anpassa sitt agerande utifrån de förutsättningar som råder, t.ex. beroende på vilka metoder de vet (eller tror) att brottsbekämpande myndigheter använder och hur effektiva dessa metoder är. Som exempel har bland annat nämnts den s.k. OPSEC-manualen som tagits fram av terrorister för att undgå upptäckt på internet och sexualförbrytares diskussioner på Darknet i samma syfte.

Bilden av att personer inom organiserade kriminella nätverk är säkerhetsmedvetna har förstärkts av de studiebesök som utredningen gjort. Vid besök hos Polisen har personer vid Nationella operativa avdelningens (NOA) avlyssnings- och analysverksamhet framhållit ett flertal exempel som talar starkt för ett ökat säkerhetsmedvetande hos kriminella när det gäller frågor relevanta för utredningen. Ett givet exempel i sammanhanget är den omständigheten att antalet samtal som kan avlyssnas i dag är väsentligt färre än

vad de var bara för ett antal år sedan, beroende på att dessa i dag genomförs via appar som krypterar samtalen i stället för via traditionell telefoni eller mobiltelefoni. Dessutom har det uppgetts för oss att en kommentar som hörs flera gånger dagligen i de samtal som alltjämt går att avlyssna mellan två misstänkta är ”vi går över till WhatsApp” eller liknande kommunikationsmedel (vilka är krypterade) när det framgår att de avlyssnade ska tala om kriminella aktiviteter. En annan indikation på säkerhetsmedvetandet är att det bland beslagtagna mobiltelefoner har påträffats telefoner som har krypterats särskilt av kommersiella företag för att uppnå en nivå av kryptering som inte tidigare noterats. Dessutom har det förklarats för oss att det går trender i vilken utrustning som används utifrån vad som är känt om säkerhetsbrister i olika tekniska utrustningar. Exempelvis ansågs bland kriminella grupperingar under en tid Blackberrytelefoner vara helt ogenomträngbara. När emellertid vissa åtgärder vidtogs från de brottsbekämpande myndigheternas sida för att komma till rätta med denna problematik spreds ryktet om det bland kriminella och de brottsbekämpande myndigheterna kunde se en övergång till teknisk utrustning från andra varumärken i stället. De uppgifter vi således fått vid studiebesöken stämmer väl överens med vad experterna från de brottsbekämpande myndigheterna anfört i sina behovsbeskrivningar, se beträffande detta i kapitel 8 och i bilaga 2.

7.5.3 Dödligt våld

Ändrad karaktär på det dödliga våldet i Sverige?

Som redovisats ovan har det dödliga våldet[52] i Sverige varit tämligen konstant under de senaste 20 åren. 2015 var dock ett undantag i negativ riktning då 112 personer föll offer för dödligt våld. Detta motsvarar en ökning med 24 procent jämfört med det genomsnittliga antalet offer för dödligt våld under 2000-talet. År 2016 föll 106 personer offer för dödligt våld. Det är också högre än det genom-

[52] Med dödligt våld avses fullbordade mord, dråp, barnadråp och misshandel med dödlig utgång. Fall som av rättsväsendet bedömts som nödvärn undantas. Med konstaterade fall avses anmälda brott om dödligt våld (dödsfall) där man kunnat konstatera att det med stor sannolikhet är dödligt våld som är dödsorsaken. Med fall avses unika individer som fallit offer för dödligt våld. Endast fall där gärningen har begåtts i Sverige och har anmälts till polisen eller annan brottsutredande myndighet ingår i statistiken.

snittliga antalet offer. En förklaring som Brå framhöll i en kommentar till ökningen år 2015 var att antalet offer i ärenden med fler än ett fall hade ökat, från tio personer i fem ärenden år 2014 till 22 personer i nio ärenden år 2015. Brå konstaterade också att andelen brott där skjutvapen var involverade ökat under den senaste femårsperioden i jämförelse med tiden dessförinnan. Under 90-talet och 00-talet användes skjutvapen i omkring 20 procent av fallen medan statistiken för perioden 2011–2015 vittnar om att skjutvapen i stället använts i omkring 28 procent av fallen. År 2015 användes skjutvapen i 29 procent av fallen.[53] År 2016 användes skjutvapen i 28 procent av fallen.

I Brå-rapporten *Det dödliga våldet i Sverige 1990–2014 – En beskrivning av utvecklingen med särskilt fokus på skjutvapenvåldet* framgår att andelen offer för dödligt skjutvapenvåld i Sverige till följd av kriminella konflikter ökat väsentligt sedan början av 1990-talet. Från att ha stått för 18 procent under perioden 1990–1995 till att under perioden 2008–2013 stå för 48 procent.[54]

Även om kriminella konflikter innefattar mer än konflikter inom ramen för organiserad brottslighet och det enligt Brås studie inte går att säga exakt vilken typ av motiv inom de kriminella konflikterna som blivit vanligast och inte heller att uttyda 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.

En gemensam nämnare för mycket av det dödliga skjutvapenvåldet inom ramen för kriminella konflikter är enligt rapporten att det verkar ha föregåtts av någon form av planering – även om de bakomliggande motiven kan vara nog så bagatellartade. Det dödande våldet har alltså mycket sällan utförts omedelbart i den situation där konflikten med offret först uppstått. Utifrån vittnesmålen i utredningarna förefaller gärningspersonen i stället ha sökt upp offret i en ny situation.[55]

[53] Se Brås rapport *Konstaterade fall av dödligt våld – en genomgång av anmält dödligt våld 2015*.
[54] Se *Det dödliga våldet i Sverige 1990–2014 – En beskrivning av utvecklingen med särskilt fokus på skjutvapenvåldet* (Rapport 2015:24) s. 32. Procentsatsen anger den procentuella andel som kriminella konflikter stod för av allt dödligt skjutvapenvåld. Övriga kategorier (vilka samtliga minskat vid jämförelse mellan de två perioderna) är familje-/partnervåld, spontanbråk/dispyter, rån-/inbrottsmord samt övrigt/okänt.
[55] Brå-rapport 2015:24 s. 34.

8 Uppgifter från brottsbekämpande myndigheter

8.1 Inledning

I direktiven anges att utredningen vid genomförande av uppdraget ska inhämta upplysningar från företrädare för berörda myndigheter och organ, bl.a. Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket. Utredningen ska också särredovisa dessa myndigheters behov av hemlig dataavläsning.

Utredningen har under sitt arbete haft mycket kontakter med representanter för de brottsbekämpande myndigheterna avseende bland annat behovet av hemlig dataavläsning och hur en sådan metod praktiskt skulle kunna användas. Främst har dessa kontakter bestått av löpande samtal och e-postkorrespondens med utredningens experter. Emellertid har även studiebesök gjorts vid flera av de i expertgruppen representerade myndigheterna. För kartläggningen av behovet av hemlig dataavläsning har utredningen dessutom hämtat in behovsbeskrivningar från utredningens experter som till vardags arbetar vid de brottsbekämpande myndigheterna.

I detta kapitel sammanfattas de uppgifter som lämnats i behovsbeskrivningarna.[1] Dessförinnan redovisas emellertid något om hur de tvångsmedel som finns i dag används och vilken nytta de bedöms medföra i den brottsbekämpande verksamheten. Kapitlet avslutas med en uppsamling av olika uppgifter som framkommit vid utredningens kontakter med företrädare för de brottsbekämpande myndigheterna som vi bedömt vara av betydelse för frågor som rör hemlig dataavläsning.

[1] Behovsbeskrivningarna finns i återgivna i helhet i bilaga 2.

8.2 Användningen av hemliga tvångsmedel i Sverige

Årligen redovisar regeringen till riksdagen användningen av vissa hemliga tvångsmedel. Redovisningen sker efter att Åklagarmyndigheten i samverkan med Ekobrottsmyndigheten, Polismyndigheten, Tullverket och Säkerhetspolisen tar fram en årlig rapport som ges in till Regeringskansliet. Av redovisningarna och, avseende den hemliga tvångsmedelsanvändningen år 2016, Åklagarmyndighetens rapport framgår bland annat följande.

År 2012 meddelades 7 643 tillstånd till hemliga tvångsmedel under förundersökning. Motsvarande antal under åren 2013–2016 var 7 417 (2013), 8 052 (2014), 9 582 (2015) och 10 428 (2016). I omkring 1 000 förundersökningar per år används hemliga tvångsmedel. Det innebär att det endast är i en mycket liten andel av alla förundersökningar som hemliga tvångsmedel används.

Vanligast bland de hemliga tvångsmedlen är hemlig övervakning av elektronisk kommunikation. Sådan övervakning omfattade 2 022 personer i 4 398 tillstånd år 2014, 2 104 personer i 5 959 tillstånd år 2015 och 2 290 personer i 6 800 tillstånd år 2016. Hemlig avlyssning av elektronisk kommunikation omfattade 1 235 personer i 3 564 tillstånd år 2014, 1 158 personer i 3 465 tillstånd år 2015 och 1 253 personer i 3 456 tillstånd år 2016. Motsvarande antal för hemlig kameraövervakning var 89 personer i 69 tillstånd år 2014, 122 personer i 114 tillstånd år 2015 och 117 personer i 143 tillstånd år 2016. För hemlig rumsavlyssning var antalen 21 personer i 16 tillstånd år 2014, 51 personer i 44 tillstånd år 2015 och 55 personer i 54 tillstånd år 2016.[2]

När det gäller vilken typ av brottslighet som misstankarna avsett kan konstateras såvitt avser t.ex. hemlig avlyssning av elektronisk kommunikation att år 2015 avsåg cirka 60 procent av tillstånden narkotikabrott/narkotikasmuggling, 24 procent våldsbrott, 4 procent ekonomisk brottslighet, 2 procent tillgreppsbrott, 2 procent sexualbrott/människohandel och 8 procent avsåg andra brott.[3] Fördelningen är nästan identisk för användningen av hemlig avlyssning av elektronisk kommunikation 2016.[4]

[2] Regeringens skrivelse 2016/17:69 s. 16 ff. och Åklagarmyndighetens rapport den 31 maj 2017, dnr ÅM 2016-308.
[3] Regeringens skrivelse 2016/17:69 s. 17.
[4] Åklagarmyndighetens rapport den 31 maj 2017, dnr ÅM 2016-308 s. 5.

I underrättelseverksamheten har Polismyndigheten möjlighet att under vissa förutsättningar (se kap. 3) använda hemlig avlyssning eller övervakning av elektronisk kommunikation och hemlig kameraövervakning enligt reglerna i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen). Under åren 2014–2016 har den möjligheten inte utnyttjats av Polismyndigheten vid något tillfälle.[5]

Det finns också möjlighet för Polismyndigheten och Tullverket att inhämta vissa uppgifter från operatörer enligt lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Så har skett 647 gånger år 2014, 698 gånger år 2015 och 688 gånger år 2016. I Tullverkets verksamhet har det uteslutande handlat om inhämtning beträffande grov narkotikasmuggling (121 tillstånd år 2014, 200 år 2015 och 234 år 2016). I Polismyndighetens verksamhet har tillstånden också primärt rört grov narkotikabrottslighet (inklusive smuggling). Över hälften av besluten har under 2014–2016 gällt sådan brottslighet. Även beträffande annan allvarlig brottslighet, såsom synnerligen grovt vapenbrott, grovt rån och mord, har beslut enligt inhämtningslagen meddelats av Polismyndigheten.[6]

Såvitt avser nyttan med de hemliga tvångsmedlen under förundersökning anförs bland annat följande i redovisningen år 2015.

> Av redovisningen framgår att användningen av hemlig avlyssning av elektronisk kommunikation avseende 65 procent av de misstänkta har varit till nytta. Motsvarande siffror för hemlig rumsavlyssning var 48 procent och för hemlig kameraövervakning 42 procent. […]Fördelningen av de olika formerna av nytta visar att hemlig avlyssning av elektronisk kommunikation, i likhet med föregående år, främst har haft betydelse genom att uppgifterna har stärkt misstankarna mot den misstänkte, använts som underlag vid förhör eller lett till ytterligare tvångsmedel mot den misstänkte. Bland de lägst frekventa av alla redovisade nyttor är att uppgifterna har lett till att en misstänkt har avförts från utredningen. Beträffande hemlig rumsavlyssning har tvångsmedlet

[5] Se regeringens skrivelse 2016/17:69 s. 28 och Åklagarmyndighetens rapport den 31 maj 2017, dnr ÅM 2016-308 s. 29.
[6] Se bilaga till Åklagarmyndighetens rapport den 31 maj 2017, dnr ÅM 2016-308.

> främst haft betydelse genom att uppgifter från tvångsmedlet har lett till stärkta misstankar mot den misstänkte.[7]

Det bör i sammanhanget påpekas att det är komplext vad som ska anses utgöra nytta. Begreppet, och svårigheter med detta, har diskuterats vid tidigare tillfällen.[8] Som exempel på tillfällen då de brottsbekämpande myndigheterna bedömt åtgärderna vara till nytta kan emellertid nämnas att det genom tvångsmedelsanvändningen framkommit uppgifter som använts i förhör, uppgifter som stärkt misstankarna mot misstänkt, uppgifter som lett till annan tvångsmedelsanvändning mot misstänkt eller annan och när det framkommit överskottsinformation.

Inför 2016 års redovisning angav Åklagarmyndigheten, som i samverkan med andra brottsbekämpande myndigheter förser regeringen med underlaget till den årliga redovisningen, bland annat följande som ett problem vid hemlig tvångsmedelsanvändning.

> Kriminella personer som är medvetna om att de kan komma att avlyssnas tenderar att övergå från telefonsamtal till att med hjälp av annan elektronisk utrustning kommunicera på sådant sätt att vedertagen avlyssning inte är möjlig. Värdet av hemlig avlyssning av elektronisk kommunikation minskar och för att nå eftersträvat resultat måste andra tillgängliga hemliga tvångsmedel användas, t.ex. hemlig kameraövervakning och hemlig rumsavlyssning. Behovet av att kunna avlyssna annan datatrafik har ökat och kan förväntas fortsätta att öka.[9]

Resonemanget utvecklas ytterligare i Åklagarmyndighetens rapport från 2017, i vilken nyttan av den hemliga tvångsmedelsanvändningen 2016 konstaterades ha minskat i vissa avseenden jämfört med tidigare år. I rapporten anges bl.a. följande.

> Det föreligger förhållandevis stora skillnader mellan de olika nyttoparametrarna för 2016 och 2015. Att uppgifterna har utgjort underlag i förhörssituation, att uppgifterna har medfört att effektiv spaning har kunnat genomföras och att uppgifterna har bidragit till att annat tvångsmedel använts mot den misstänkte är de nyttor som förekommer i en större andel ärenden 2016 än 2015. Det som är gemensamt för dessa nyttor är att tvångsmedlet medfört att förundersökningen kunnat drivas

[7] Regeringens skrivelse 2015/16:49 s. 28. Det ska anmärkas att nyttan avseende hemlig övervakning av elektronisk kommunikation, liksom nyttan avseende inhämtning enligt inhämtningslagen, redovisas genom exempel i stället för med siffror avseende nyttoeffekter.
[8] Se t.ex. SOU 2007:22 s. 186 och SOU 2012:44 s. 481.
[9] Åklagarmyndighetens skrivelse till regeringen *Redovisning av användningen av vissa hemliga tvångsmedel under 2015* (Dnr ÅM-A 2016/0093).

framåt på ett bättre sätt. Övriga nyttor har minskat i varierande grad. Två av de nyttor som har minskat mest är dels att uppgifterna från tvångsmedlet har åberopats som bevisning i stämningsansökan (minskning från 41 % till 32 %), dels att misstankarna stärkts (minskning från 56 % till 46 %) Dessa förhållanden skulle kunna tas till intäkt för att värdet av hemlig avlyssning av elektronisk kommunikation generellt sätt har minskat från 2015 till 2016.

Kriminella personer som är medvetna om att de kan komma att avlyssnas tenderar att övergå från telefonsamtal till att med hjälp av annan elektronisk utrustning kommunicera på sådant sätt att vedertagen avlyssning inte är möjlig. Den tekniska utvecklingen som innebär en övergång från traditionella telefonsamtal och sms till kommunikation via s.k. chattappar i smarta mobiltelefoner innebär också i sig en minskning av nyttan av hemlig avlyssning av elektronisk kommunikation. Dessa appar har oftast inbyggd kryptering som gör att vanliga avlyssningsmetoder i många fall blivit verkningslösa.

Värdet av hemlig avlyssning av elektronisk kommunikation minskar således och för att nå eftersträvat resultat måste andra tillgängliga hemliga tvångsmedel användas, t.ex. hemlig kameraövervakning och hemlig rumsavlyssning. Behovet av att exempelvis kunna avlyssna eller avläsa annan datatrafik har ökat och kan förväntas fortsätta att öka.[10]

Det bör nämnas att den i avsnittet redovisade statistiken avser Polismyndighetens, Tullverkets och Ekobrottsmyndighetens verksamheter. I regeringens skrivelse år 2016 redovisades för första gången uppgifter om Säkerhetspolisens hemliga tvångsmedelsanvändning. Av den redovisningen framgår att det i Säkerhetspolisens verksamhet, med stöd av bestämmelserna i både rättegångsbalken och preventivlagen, under år 2015 fattades totalt 377 beslut om hemlig avlyssning eller övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning. Under samma år fattade Säkerhetspolisen 109 beslut med stöd av inhämtningslagen. Motsvarande siffror för 2016 var 307 beslut om hemlig avlyssning eller övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning samt 167 beslut om inhämtning enligt inhämtningslagen. De aktuella siffrorna avser såväl de initiala besluten som förlängningar av dessa (efter en månad).[11]

Det kan också nämnas att vi vid våra studiebesök hos de brottsbekämpande myndigheterna stött på kritiska röster avseende den årliga nyttoredovisningen. Dessa har gjort gällande att redovisningen

[10] Åklagarmyndighetens rapport den 31 maj 2017, dnr ÅM 2016-308 s. 10.
[11] Åklagarmyndighetens rapport den 31 maj 2017, dnr ÅM 2016-308 s. 29 f.

är ett trubbigt instrument. Den verkliga (eller faktiska) nyttan skulle enligt de som uttalat sig i denna fråga kunna vara väsentligt högre om ändamålsenliga verktyg fanns för att få ut den fulla potentialen av tvångsmedelsbestämmelserna och tvångsmedelstillstånden. Som exempel har anförts problemet med krypterad kommunikation. Detta problem framkommer inte så tydligt som vore önskvärt i den årliga nyttorapporteringen eftersom varje liten nytta vid avlyssningen räknas. Det innebär att en åtgärd kan anses ha varit till nytta även när i stort sett all kommunikation som avlyssnats varit krypterad, om bara en liten mängd klartextinformation som erhållits har lett till någon av de nyttoeffekter som efterfrågas i underlaget. Nyttan som uppstått är då 100-procentig eftersom frågeställningen i någon mening är binär; dvs. antingen nytta eller ingen nytta. Detta gäller trots att den faktiska nyttan bara är en bråkdel av vad den kan antas vara om man i stället fick tillgång även till resterande del av kommunikationen.

8.3 Behovsbeskrivningar från de brottsbekämpande myndigheterna

Den samlade bilden av de behovsbeskrivningar utredningen fått in är att några av de tvångsmedel som brottsbekämpande myndigheter får använda inte ger så mycket information som de skulle kunna ge. Det finns flera orsaker till detta men en förklaring som lyfts fram särskilt, och som enligt beskrivningarna också gör att det finns ett behov av hemlig dataavläsning, är relaterad till kryptering. En annan omständighet som särskilt lyfts fram i behovsbeskrivningarna är den ökade graden av anonymisering, med vilket avses medvetet eller omedvetet förhindrande för de brottsbekämpande myndigheterna att avlyssna och övervaka kommunikation.

De brottsbekämpande myndigheterna har när det gäller den minskade betydelsen av befintliga tvångsmedel framhållit att det i många fall snarare beror på tur eller misstag i den misstänktes informationshantering än skicklighet och ändamålsenliga verktyg om ett ärende blir framgångsrikt. Säkerhetspolisen har exempelvis anfört att det är oerhört otillfredsställande att framgång i utredningar av grov brottslighet kopplad till nationell säkerhet ska bygga på tur, särskilt som tur är väldigt sällan förekommande.

Det är emellertid inte bara minskad betydelse eller förmåga hos de befintliga tvångsmedlen som lyfts fram som skäl för hemlig dataavläsning. Också den omständigheten att det i dag inte finns laglig möjlighet till att vidta vissa åtgärder har framhållits i behovsbeskrivningarna. Till detta återkommer vi nedan.

Avsnittet tar i det följande (8.3.1–8.3.5), utifrån olika typer av uppgifter som hemlig dataavläsning skulle kunna användas för att hämta in, upp de behovsområden som de brottsbekämpande myndigheterna nämnt i behovsbeskrivningarna och avslutas därefter (8.3.6) med en redovisning av ett antal typfall på situationer där hemlig dataavläsning enligt behovsbeskrivningarna skulle kunna vara av betydelse för utredningar.

8.3.1 Krypterad och anonymiserad kommunikation

Ett genomgående drag i behovsbeskrivningarna är att dessa tar upp frågan om krypterad kommunikation och de negativa effekter krypteringen har på värdet av befintliga hemliga tvångsmedel (hemlig avlyssning och övervakning av elektronisk kommunikation samt inhämtning enligt inhämtningslagen). Över 90 procent av den internetkommunikation som i dag avlyssnas av Polismyndigheten och Tullverket är krypterad. Således är mindre än tio procent av denna kommunikation möjlig att fånga upp i klartext efter tvångsmedelstillstånd. Säkerhetspolisen har uppgett att problematiken med kryptering och anonymisering (se nedan) förekommer i samtliga ärenden som Säkerhetspolisen har.

Det har framhållits att i stort sett samtliga appar och program som används för kommunikation i dag har inbyggda funktioner för skydd och säkerhet som minskar värdet av hemlig avlyssning av elektronisk kommunikation. I behovsbeskrivningarna har de brottsbekämpande myndigheterna också anfört att bara under de senaste åren har man kunnat se en kraftig ökning av den krypterade kommunikationen.

Flera av de brottsbekämpande myndigheterna har angett att den kommunikation som alltjämt kan avlyssnas är för brottsutredningarna (eller, när det är fråga om brottsförhindrande verksamhet, ärendena) tämligen ointressant. Det har också förts fram att ett vanligt fenomen när den avlyssnade ska diskutera något förmodat

intressant för ärendet så sägs eller skrivs uttryckligen att man ska gå över till säker kommunikation. I många fall sker detta så explicit som att den misstänkte eller den som denne kommunicerar med exempelvis uttrycker: ”Vi går över till WhatsApp”.

När det gäller anonymisering avses bland annat att användaren av ett mobiltelefonabonnemang använder WiFi-surf i stället för internetanvändning via abonnemanget, vilket medför att den kommunikationen inte kan fångas upp vid hemlig avlyssning av elektronisk kommunikation. Andra förfaranden som avses med anonymisering är användandet av anonyma, förbetalda kontantkort och särskilda internettjänster som medför att användarens IP-adress byts mot en anonym adress, vilket kan ske i flera led (jfr t.ex. beskrivningen i avsnitt 6.3.3).

Konsekvenserna av den ökade krypteringen och anonymiseringen är stora enligt de brottsbekämpande myndigheterna. Tullverket har exempelvis anfört att ett flertal utredningar redan från början väljs bort alternativt läggs ned efter en tid eftersom någon annan väg till framgång i utredningarna inte finns. Det har också anförts att konsekvensen av problematiken vid utredningar riktade mot organiserad brottslighet, som har en hierarkisk struktur, inte sällan blir att de som befinner sig i toppen av hierarkin klarar sig undan myndigheterna. Detta trots att de brottsbekämpande myndigheterna anser sig ha en god bild av vilka dessa personer är. I stället är det de som befinner sig i de lägre skikten (i narkotikaärenden t.ex. missbrukare, langare och kurirer) som kan kommas åt. Det medför att brottsligheten kan fortsätta i stort sett oförändrad trots de brottsbekämpande myndigheternas insatser eftersom elementen i de nedre delarna i hierarkin i hög utsträckning anses utbytbara. Ytterligare konsekvenser är att utredningar som trots kryptering inte läggs ned är väsentligt mer tidskrävande och därmed kostsammare än andra utredningar och dessutom mer sällan leder till att brottsmisstänkta åtalas och döms.

8.3.2 Krypterade enheter

En annan aspekt av den ökande krypteringen är kryptering av teknisk utrustning. Sådan kryptering vållar enligt behovsbeskrivningarna stora problem för de brottsbekämpande myndigheterna när den tekniska utrustningen ska undersökas efter att den tagits i

beslag. Enligt Polismyndigheten har kryptering av databärare ökat markant de senaste åren. Myndigheten har anfört att detta gör att det krävs mer resurser och ställs högre krav på planering inför tillslag, såsom spaning och offensiv taktik vid själva tillslaget, för att t.ex. hinna fram till en dator innan den stängs av och blir krypterad. När så har skett blir innehållet i den tekniska utrustningen nämligen oläsbart vid en analys. Säkerhetspolisen har påpekat att verktygen för kryptering numera är standard för alla att använda och att de ofta ingår som en del i operativsystemen och endast kräver enkla handgrepp hos användare. Enligt Tullverket är det en allt vanligare fråga från it-forensikerna som ska undersöka ett beslag hur väl skyddad informationen är. Tullverket har också påpekat att mobiltelefoner och surfplattor i stort sett alltid är krypterade och därmed i praktiken omöjliga att komma åt informationen i utan lösenkod.

Det har varit svårt att få fram konkreta uppgifter om hur vanligt förekommande det är med krypterad teknisk utrustning. Säkerhetspolisen har anfört att problematiken förekommer i stort sett i samtliga dess ärenden. Tullverket har angett att det finns geografiska skillnader i landet. Högst andel krypterade enheter finns i storstadsområdena (Stockholm, Göteborg och Malmö) där omkring 50–80 procent av de beslagtagna enheterna är krypterade medan det i exempelvis Norrlandsregionen endast förekommer kryptering vid cirka 10 procent av beslagen. Tullverket har också anfört att merparten av de krypterade beslagen utgörs av låsta mobiltelefoner. Experterna från Polismyndigheten har gjort gällande att det är mer regel än undantag att mobiltelefoner är skyddade av lösenkod eller biometriskt skydd (t.ex. upplåsning genom avläsning av fingeravtryck). Man har dock anfört att även i fall där lösenordet varit känt och mobiltelefonen gått att analysera så har chatthistorik och viss annan information ändå inte kunnat läsas eftersom appar i mobiltelefoner använder sig av egen kryptering i stor utsträckning. Det innebär att innehållet i appar inte kan analyseras och information som kan vara av värde i förundersökningen inte kan tillvaratas.

De metoder som finns tillgängliga i dag för att komma åt innehållet i krypterade enheter har av flera experter angetts till antingen s.k. brute force, vilket innebär att man med hjälp av särskilda program och algoritmer gissar lösenordet, att den misstänkte frivilligt lämnar ut lösenordet eller att lösenordet på annat sätt kan kommas åt, t.ex. genom att det finns en lapp med lösenordet vid ett

beslag i gärningsmannens bostad. Det bör nämnas att det genom brute force, enligt uppgift från Åklagarmyndigheten, i praktiken är omöjligt att gissa lösenordet om detta inte är av enkel beskaffenhet. De brottsbekämpande myndigheternas samlade konklusion kan således sägas vara att det är mycket ovanligt, i synnerhet när det är fråga om teknisk utrustning som förekommit i organiserad brottslighet eller terroristsammanhang, att man får tag i de lösenord eller nycklar som behövs för att komma åt information i krypterade enheter med dagens metoder.

8.3.3 Lagrade uppgifter

Under en brottsutrednings gång och, kanske ännu oftare, i underrättelseverksamhet kan det av olika anledningar finnas goda skäl att ta del av vad den misstänkte lagrar elektroniskt. En anledning till att det finns behov av att ta del av lagrade uppgifter utan den misstänktes kännedom om åtgärden som experterna från Polismyndigheten framfört är att det blivit allt vanligare med raderings- och rensningsprogram. Sådan programvara gör att endast den användarhistorik som skrivits efter senaste rensningen finns kvar i den tekniska utrustningen vid ett beslag. Om datorn har rensats på natten och tillslaget sker på morgonen finns inte mycket användarhistorik kvar i utrustningen. Sådan användarhistorik som avses är exempelvis chattar, besökta webbsidor eller filer som har använts. Även lösenord kan ibland återfinnas genom användarhistoriken.

Det kan också, särskilt i underrättelsesituationer, finnas skäl att löpande under ett ärende ta del av vad den misstänkte lagrar eftersom denna information kan göra att det är möjligt att exempelvis avstyra ett terroristattentat eller förhindra fortsatt brottslig verksamhet, se särskild Säkerhetspolisens behovsbeskrivning i bilaga 2.

Ytterligare ett, för de brottsbekämpande myndigheterna framträdande bekymmer när det gäller lagrade uppgifter, är att elektronisks uppgifter som kan vara av intresse för ett ärende inte nödvändigtvis lagras lokalt på datorn. I stället är det inte ovanligt att den enskilde använder s.k. molntjänster, dvs. tjänster som utnyttjar möjligheterna att lagra uppgifterna på annan plats än lokalt för att sedan tillgängliggöra den i den tekniska utrustningen på användarens begäran. Ett problem med molntjänster, ur de brottsbekämpande

myndigheternas synvinkel, är att det inte sällan är så att det inte går att veta var uppgifterna finns. Det kan ställa till praktiska problem både såvitt avser jurisdiktionsfrågor (dvs. om svenska myndigheter har rätt att bereda sig tillgång till uppgifterna) och frågor om hur den brottsbekämpande myndigheten ska komma åt uppgifterna.

8.3.4 Identifiering och positionering

Det förekommer i brottsutredningar att det finns kännedom om att viss teknisk utrustning, typiskt sett en mobiltelefon, kan knytas till en plats för ett brott på ett sådant sätt att den kan antas tillhöra en misstänkt. På motsvarande vis förekommer i underrättelseverksamhet att kommunikation sker mellan teknisk utrustning vars ägare/besittare är okänd men som är av intresse i ärendet och en enhet som tillhör en annan person av intresse i underrättelseverksamheten. När, som i dessa fall, det inte är känt vem som förfogar över en viss enhet av betydelse i ett ärende behöver de brottsbekämpande myndigheterna, enligt behovsbeskrivningarna, en möjlighet att ta reda på detta. Genom hemlig dataavläsning skulle den brottsbekämpande myndigheten kunna aktivera t.ex. den tekniska utrustningens kamera eller mikrofon. På så vis skulle det finnas bättre möjligheter att identifiera den misstänkte.

En annan åtgärd som, vilket Säkerhetspolisen framhållit, skulle kunna vidtas genom hemlig dataavläsning är att den brottsbekämpande myndigheten aktiverar GPS-funktionen på den tekniska utrustningen så att det genom lokalisering av den misstänkte blir möjligt att identifiera den misstänkte. Aktivering av en teknisk utrustnings GPS-funktion (eller annan funktion som kan möjliggöra lokalisering/positionering) behöver emellertid inte vara begränsad bara till situationer där den misstänktes identitet är okänd. Även i situationer där den misstänkte är känd för den brottsbekämpande myndigheten kan det ur utredningssynpunkt vara viktigt att veta var hen befinner sig eller i vilka miljöer denne rör sig.

8.3.5 Nya möjligheter för vissa andra hemliga tvångsmedel

Det har inte från någon av de brottsbekämpande myndigheterna uttryckligen angetts att hemlig rumsavlyssning eller hemlig kameraövervakning fungerar särskilt dåligt på grund av förändrade tekniska förutsättningar, motsvarande exempelvis den effekt som kryptering haft för värdet av hemlig avlyssning av elektronisk kommunikation. Om förändringar skett till det (för de brottsbekämpande myndigheterna) negativa synes detta snarare bero på att kriminella blir allt mer medvetna om vilka metoder de brottsbekämpande myndigheterna använder. Tullverkets expert har t.ex. anfört att det ofta händer att möten och känsliga samtal undviks för att inte riskera eventuell s.k. buggning i förutsägbara rum eller bilar och att mötena i stället genomförs flexibelt och oannonserat på allmänna och öppna platser.

Även om inget särskilt behov till följd av minskat värde hos hemlig rumsavlyssning eller hemlig kameraövervakning framhållits har representanter från olika brottsbekämpande myndigheter anfört att eftersom hemlig dataavläsning skulle kunna innefatta verkställande av dessa åtgärder så bör en sådan möjlighet ges. Tullverkets expert har anfört att verket anser att reglerna om hemlig rumsavlyssning bör ses över och ändras så att åtgärden riktas mot en misstänkt person och utan krav på plats.

8.3.6 Typfall som visar på behov

Som nämnts har experterna från de brottsbekämpande myndigheterna ombetts att komma in med exempel som tydliggör och konkretiserar i vilka situationer hemlig dataavläsning enligt myndigheternas uppfattning behövs och hur åtgärden skulle kunna användas. I detta avsnitt redovisas de typfall som Säkerhetspolisen har anfört tillsammans med en förklaring på vad som skulle kunna åstadkommas i respektive typfall genom hemlig dataavläsning. För att inte framställningen ska få en allt för stor inriktning mot Säkerhetspolisens verksamhet har en del av typfallen förändrats till att avse även andra brottsbekämpande myndigheters verksamheter.

Det bör nämnas att typfallen i sitt ursprungliga skick (se Säkerhetspolisens behovsbeskrivning i bilaga 2), enligt uppgift från Säkerhetspolisen, är autentiska situationer som avidentifierats och, i vissa

fall modifierats, för att de inte ska gå att härleda till en särskild händelse eller utredning. Även de andra brottsbekämpande myndigheterna har lämnat exempel och typfall från sina verksamheter. Dessa framgår också i behovsbeskrivningarna i bilaga 2.

Typfall 1

Säkerhetspolisen har information om att fem personer kan vara i färd med att planera terroristattentat i Sverige. De fem männen bor på visst avstånd från varandra och använder elektronisk kommunikation i kontakten mellan dem. Vid verkställighet av hemlig avlyssning av elektronisk kommunikation hör Säkerhetspolisen hur personerna pratar med varandra om alldagliga saker men också att de ibland säger att ”vi tar Skype”. Det kan starkt misstänkas att man då pratar om de brott som planeras. Eftersom Skype, liksom t.ex. Twitter, Viber och Facebook, är en krypterad tjänst, kan Säkerhetspolisen inte få del av innehållet i kommunikationen.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information och om utrustningens position (GPS) både historiskt och i realtid.

Typfall 2

En privatperson tar kontakt med Säkerhetspolisen och informerar om att han blivit kontaktad av en man via en social medietjänst på internet. Så småningom har det framgått att mannens avsikter med kontakten har varit att få hjälp med information som bedöms vara av betydelse vid attentatsplanering mot Sverige. Vid kontakter med internetoperatören framgår att kontot som mannen använt vid kontakten tillhör en för Säkerhetspolisen känd person. Vid spaning får Säkerhetspolisen fram att personen använder en smarttelefon. Säkerhetspolisen får information om abonnemanget som mannen har men inga uppgifter om hans kommunikation. Säkerhetspolisen misstänker att mannen utnyttjar trådlösa nät (WiFi) för att kommunicera anonymt.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning (smartphone), som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas.

Typfall 3

Vid en förundersökning framkommer information om att man från två kända grovt kriminella grupperingar ”mobiliserar” inför en större händelse som är av intresse för båda sidor. Stämningen är så hatisk att det finns farhågor om att synnerligen grovt våld kommer att användas. Vid den förundersökning som inleds försöker polisen kartlägga de individer som kan vara inblandade. Det visar sig att man från båda sidor undviker att ha fysiska möten. I stället sker all kontakt via krypterade sociala medietjänster eller andra egenutvecklade slutna forum.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som de misstänkta kommunicerar med skulle kunna fastställas.

Typfall 4

Efter ett fullbordat terroristattentat utomlands får Säkerhetspolisen information från sin motsvarighet i det aktuella landet att någon av gärningsmännen har haft kontakt med flera IP-adresser som sannolikt är kopplade till en mobiltelefon i Sverige. Efter att information inhämtats från den aktuella operatören kan IP-adresserna knytas till en viss mobiltelefon, som har ett anonymt abonnemang. Genom uppgifter från hemlig övervakning av elektronisk kommunikation kan innehavaren av mobiltelefonen identifieras som en person med koppling till terroraktörer i Sverige. Vid avlyssning av telefonen visar

det sig att den används endast för krypterad IP-baserad kommunikation.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas. Det gäller även i vilken miljö den misstänkte finns när han kommunicerar.

Typfall 5

Efter att ett terroristbrott fullbordats i Sverige står det klart att gärningsmannen måste ha haft hjälp av andra för att utföra dådet. Vid kartläggning av gärningsmannens kommunikationer framkommer att han haft ett flertal kontakter via internet med personer både i Sverige och utomlands. Säkerhetspolisen ser en uppenbar risk för att ytterligare attentat kan komma att genomföras inom en snar framtid och behöver få kontroll på vilka de övriga personerna är. Gärningsmannens datorer och telefoner tas i beslag. Undersökningen av föremålen visar att gärningsmannen strax före attentatet har haft kontakt med en IP-adress. När hemlig övervakning av elektronisk kommunikation verkställs avseende den IP-adressen framkommer att kommunikation sker med andra IP-adresser såväl i Sverige som utomlands. En av IP-adresserna kan knytas till en sedan tidigare känd anhängare av våldsbejakande islamistisk extremism. När hemlig avlyssning av elektronisk kommunikation verkställs visar det sig att den personens kommunikation är krypterad.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han kommunicerar.

Typfall 6

Tullverket får information om att en gruppering som sedan tidigare är välkänd i narkotikakretsar planerar att föra in ett mycket stort parti heroin till Sverige. En förundersökning om förberedelse till synnerligen grov narkotikasmuggling och synnerligen grovt narkotikabrott inleds. Vid verkställighet av hemlig avlyssning av elektronisk kommunikation kommer det fram att de misstänkta använder sig av Facebook men också motsvarande typ av tjänst i Ryssland. Man har också skapat egna slutna forum där endast särskilt betrodda medlemmar har fått inloggningsuppgifter. Samtliga kommunikationstjänster är krypterade.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som de misstänkta kommunicerar med skulle kunna fastställas liksom i vilken miljö de misstänkta finns när de kommunicerar.

Typfall 7

Flera personer lämnar information om att det inom ett slutet forum pågår en ”hatkampanj” mot de politiker som står bakom Sveriges flyktingpolitik. Flera av de inblandade har uttryckt en vilja att spränga lokaler där centrala statsledningen finns, och man har också efterfrågat vapen och sprängämnen. Hemlig avlyssning av elektronisk kommunikation har inte kunnat ge någon ytterligare information till utredningen eftersom all kommunikation är krypterad.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som de misstänkta kommunicerar med skulle kunna fastställas liksom i vilken miljö de misstänkta finns när de kommunicerar.

Typfall 8

Flera personer har lämnat information till Säkerhetspolisen om att två bröder, 17 och 19 år gamla, har radikaliserats snabbt. Deras närstående är mycket oroliga för att de kan agera okontrollerat. En av bröderna har haft kontakt med personer som kommer från samma bostadsområde och som befinner sig i Syrien för att slåss för Daesh. Bröderna har själva uttalat att de vill kriga för Daesh oavsett var i världen det sker. Vid verkställighet av hemlig avlyssning av elektronisk kommunikation framkommer att en stor del av brödernas kommunikation, både med varandra och med andra, går via krypterade sociala medietjänster. Dessutom har bröderna kontakt med IP-adresser som vid kontroll visar sig innehas av mindre resebyråer utomlands. En av Säkerhetspolisens hypoteser är att bröderna försöker få stridstränade personer från Syrien att komma hem för att begå terroristbrott i Sverige. Eftersom kommunikationen med resebyråerna är krypterad går det inte att få klarlagt vad bröderna har för avsikt med kontakterna.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras.

Typfall 9

Säkerhetspolisen har konstaterat att en lägenhet används av flera personer som är kända i terrorkretsar. En förundersökning om stämpling till terroristbrott pågår och domstolen har beslutat om hemlig avlyssning av elektronisk kommunikation avseende de misstänktas telefoner. Vid ett tillfälle under avlyssningen uttalar en av de misstänkta att han har information i sin dator men att den är krypterad och säker. Säkerhetspolisen bedömer att den informationen skulle kunna vara av mycket stort värde i förundersökningen och överväger att göra husrannsakan i lägenheten där datorn finns. En sådan kan dock inte ske öppet, eftersom det skulle riskera att spoliera utredningsresultatet. I lägenheten bor en familj där någon av familjemedlemmarna alltid är hemma, dvs. lägenheten är aldrig tom.

Det finns med andra ord ingen möjlighet att i detta läge av utredningen komma åt informationen i datorn.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter och om aktiviteter som inte kommuniceras eller lagras.

Typfall 10

Ekobrottsmyndigheten har via finanspolisen fått information om att en person, som sedan tidigare är känd av myndigheten i grova ekobrottssammanhang, har blivit rapporterad av en bank för misstänkt penningtvätt. Uppgifterna gör att misstankarna mot personen stärks och en förundersökning rörande grovt penningtvättsbrott inleds. Uppgifter inkommer från banken, som visar att den misstänkte har överfört pengar till bankkonton utomlands. Vem som är innehavare av de utländska kontona framgår däremot inte. Den misstänktes kontakter med banken har uteslutande skett via internet och en specifik IP-adress har använts. Den misstänkte har avslutat kontot. Banken har ingen uppgift om att den misstänkte har bytt bank. Vid verkställighet av hemlig avlyssning av elektronisk kommunikation framgår att den misstänkte kommunicerar med en IP-adress som innehas av en bank utomlands. Det är omöjligt att få uppgifter från banken. Eftersom kommunikationen med banken är krypterad går det inte att få fram vad kommunikationen rör.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras och om lagrade uppgifter.

Typfall 11

Vid övervakning av en känd underrättelseofficer upptäcker Säkerhetspolisen att hon har svårförklarliga kontakter med en man som vid kontroll visar sig vara anställd vid ett stort teknikföretag som levererar materiel till en myndighet inom det svenska försvaret. Efter

kontakt med den aktuella myndigheten står det klart att mannen arbetar med teknik som direkt kan kopplas till verksamhet som rör rikets säkerhet. En förundersökning om grovt spionerи inleds. Vid verkställighet av hemlig avlyssning av elektronisk kommunikation går det att dra slutsatsen att hårddisken i mannens dator är krypterad. Det framkommer dessutom att en del av hans kommunikation sker via en app som inte är känd sedan tidigare och som är krypterad.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han kommunicerar.

Typfall 12

Vid verkställighet av hemlig avlyssning av elektronisk kommunikation mot ledande personer i ett känt motorcykelgäng framkommer att de undviker att prata om i sammanhanget känsliga saker i klartext över telefon. Det enda man säger efter att ha ringt upp varandra är ”WhatsApp”. Av sammanhanget är det lätt att dra slutsatsen att all kommunikation som avser kriminell verksamhet sker via den tjänsten, där överföring av både tal och bild är krypterad.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om den miljö där de misstänkta finns när de använder utrustningen.

Typfall 13

Säkerhetspolisen misstänker att en viss person med tillgång till kvalificerat hemlig information har värvats som agent av en utländsk underrättelseofficer. Personen har bl.a. vid ett flertal tillfällen besökt det aktuella landet utan att berätta om det för sin arbetsgivare.

Arbetsgivaren misstänker, efter att ha granskat säkerhetsloggar, att mannen sannolikt har kopierat hemliga uppgifter. Vid verkställighet av hemlig avlyssning av elektronisk kommunikation framgår att kommunikationen till och från hans mobiltelefon och dator är krypterad.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustningar, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 14

En serie grova dataintrång sker mot flera myndigheter. Det är oklart vem eller vilka som står bakom brottsligheten när en förundersökning om grova dataintrång inleds. Intrången kan spåras till en server som finns i Sverige. Vid undersökning av servern framgår att den ofta kontaktas från en specifik IP-adress och att kommunikationen är krypterad. Vid kontroll med operatören fastställs att IP-adressen är hemmahörande hos ett mindre bolag inom it-branschen. Det går däremot inte att fastställa vem som är användare eller vilket innehåll kommunikationen har. Polisen bedömer att bolaget inte kan kontaktas för upplysningar utan att utredningen röjs.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i bolagets utrustning, som kan ge information bl.a. om vilka som kommunicerar, innehållet i kommunikationen innan det krypteras och om lagrade uppgifter.

Typfall 15

Säkerhetspolisen har fått information om att en viss namngiven person har sagt till flera bekanta att hans högsta önskan är att dö och att han vill resa till Syrien, kriga för Daesh och bli martyr. Säkerhetspolisen vet sedan tidigare att han har försökt att resa till Syrien

men stoppats av utländska gränskontrollmyndigheter. Om han inte kommer iväg så vill han göra något i Sverige och har börjat söka efter vapen och sprängämnen på internet, både i Sverige och utomlands. Säkerhetspolisen kan genom spaning konstatera att han har tillgång till mobiltelefoner, och han har setts använda en bärbar dator, typ Ipad. En förundersökning om förberedelse till terroristbrott har inletts. När tillståndet till hemlig avlyssning av elektronisk kommunikation ska verkställas går det att se att han kommunicerar i stor omfattning men det går inte att få fram med vem eller vilka och inte heller vilka websidor han besöker. Kommunikationen är krypterad. Kontroll av de IP-adresser som den misstänkte kommunicerar med leder inte utredningen vidare eftersom det rör sig om Tor-kommunikation.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på de personer och den utrustning den misstänkte kommunicerar med (exempelvis användar-ID i en viss app, e-postadress, ljud, bild m.m.) skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 16

Efter information från en uppgiftslämnare driver Säkerhetspolisen en förundersökning om spionerі. En person misstänks för att ha kommit över uppgifter som omfattas av sekretess med hänsyn till rikets säkerhet. Det går dock inte att säga från vilken myndighet uppgifterna kommer. Det sannolika är att personen agerat från sin dator för att komma över uppgifterna. Vid verkställighet av hemlig avlyssning av elektronisk kommunikation framgår att uppgifterna är krypterade och att gärningsmannen använder Tor, vilket gör att det inte går att fastställa vilken myndighet som blivit föremål för intrånget.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras och om identi-

teten på den utrustning den misstänkte kommunicerar med (exempelvis IP-adress, e-postadress m.m.), dvs. vilken eller vilka myndigheter det är fråga om.

Typfall 17

Säkerhetspolisen får information från en säkerhetstjänst i ett annat land om att en person med diplomatisk immunitet misstänks ägna sig åt flyktingspionage och att han har kontakter med en kvinna i Sverige. En förundersökning om olovlig underrättelseverksamhet inleds. Det visar sig vid hemlig avlyssning av elektronisk kommunikation att kvinnan ofta kommunicerar med en utländsk IP-adress och att kommunikationen är krypterad. Säkerhetspolisen misstänker att hon har kontakt med sina svenska uppgiftslämnare via den adressen.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position och om vilka den misstänkta kommunicerar med (exempelvis användar-ID i en viss app, e-postadress, ljud, bild m.m.). Även identiteten på personer som den misstänkta kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkta finns när hon använder utrustningen.

Typfall 18

Personer inom vit makt-miljön planerar att mörda en tongivande vänsteraktivist. Säkerhetspolisen får information om att det i gruppen finns personer med mycket hög teknisk kompetens. All kommunikation inom gruppen är krypterad. Bl.a. lämnar medlemmarna information till varandra i en krypterad molntjänst. Alla datorer som medlemmarna har är krypterade. Det visar sig under förundersökningen att molntjänsten finns i Sverige men det går inte att fastställa vilka datorer som har kontakt med tjänsten.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras och om lagrade

uppgifter. Om det tekniska hjälpmedlet installeras i molntjänsten kan det ge information om det finns fler personer i gruppen än vad som är känt och om identiteten på annan utrustning som kommunicerar med tjänsten.

Typfall 19

Säkerhetspolisen har information om att en grupp män brukar hålla möten med muslimska ungdomar i en föreningslokal i ett utsatt område. Informationen säger att gruppen försöker rekrytera ungdomarna att åka till Syrien och ansluta sig till Daesh. Det finns indikationer på att en för Säkerhetspolisen känd anhängare av islamistisk extremism är gruppens ledare. Vid verkställighet av hemlig avlyssning av elektronisk kommunikation visar det sig att operatören inte längre lagrar historiska uppgifter om inkommande samtal till den misstänktes mobiltelefon i enlighet med EU-domstolens förhandsbesked i december 2016 om s.k. datalagring. Dessutom är kommunikationen krypterad.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter (t.ex. kontaktlista och samtalslogg), om utrustningens position, om identiteten på de utrustningar den misstänkte kommunicerar med (exempelvis IP-adress, e-postadress m.m.) och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 20

En yngre man med kopplingar till vit makt-miljön blir misstänkt för grov allmänfarlig ödeläggelse genom att ha utlöst en sprängladdning vid en flyktingförläggning. Säkerhetspolisen misstänker att han har medhjälpare. Vid spaning kan det konstateras att den misstänkte använder både mobiltelefon och Ipad. Efter kontakt med operatörerna visar det sig att information om hans IP-adress och positions-

uppgifter rörande Ipad:en inte har lagrats i enlighet med EU-domstolens förhandsbesked i december 2016 om s.k. datalagring.

Hemlig dataavläsning skulle ge möjlighet att fysiskt installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, om utrustningens position samt om identiteten på de utrustningar den misstänkte använder själv och dem han kommunicerar med (exempelvis IP-adress, e-postadress m.m.). Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 21

Genom bl.a. spaning mot en känd underrättelseofficer drar Säkerhetspolisen slutsatsen att hon har lyckats värva en agent i Sverige. Agenten är dock hittills okänd. Misstanken är att när underrättelseofficeren kommunicerar med agenten sker det genom att hon utnyttjar trådlösa nät (WiFi), främst på olika restauranger och ibland på hotell.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i underrättelseofficerens utrustning, vilket ger möjlighet att klarlägga identiteten på dem hon kommunicerar med, utrustningens position, vilka trådlösa nät hon använder och i vilken miljö den misstänkta finns när hon använder utrustningen.

Typfall 22

Vid förundersökning rörande grov mordbrand riktad mot en restaurang är misstanken att brottet utförts av personer inom ett lokalt kriminellt nätverk vars inkomstkälla består bland annat av att erbjuda lokala företagare beskydd. En misstänkt gärningsman är identifierad. Polisen har information om att ett e-postkonto har använts för kommunikation inom gruppen före, under och efter brottet. Det har skett på så sätt att personerna har skrivit meddelanden till varandra. För att undvika att avslöja kontakten mellan personerna och vilken information de ger till varandra, har med-

delandena aldrig skickats iväg från kontot. I stället har de sparats som utkast och därigenom funnits tillgängliga för alla som haft lösenord till kontot.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i den personens kommunikation med e-postkontot innan det krypteras och om inloggningsuppgifter. Med hjälp av de uppgifterna kan ett tekniskt hjälpmedel installeras i e-postservern för att ge information om vilka utrustningar som har kommunikation med det aktuella e-postkontot.

Typfall 23

Vid Säkerhetspolisen bedrivs en förundersökning om förberedelse till terroristbrott där en man misstänks för att på internet samla in information om bombtillverkning och försöka köpa komponenter. Det finns uppgifter om att han håller på att sammanställa en ”terrorinstruktion” som ska spridas och att han inte är ensam i planeringen. Han kan ha medhjälpare som hittills är okända för Säkerhetspolisen. Vid verkställighet av hemlig avlyssning av elektronisk kommunikation har det framkommit att hans kommunikation med andra liksom hans tekniska utrustning (dator och smarttelefon) är krypterade.

Hemlig dataavläsning skulle ge möjlighet att installera tekniskt hjälpmedel, som bl.a. registrerar tryckningar på tangentbordet, vilket ger tillgång till lösenord och den text den misstänkte skriver i realtid samt andra aktiviteter som inte kommuniceras eller lagras. Säkerhetspolisen skulle samtidigt kunna få information om innehållet i kommunikationen innan det krypteras, om lagrade uppgifter, t.ex. kontaktlista, samtalslogg och innehållet i dokument som skrivs eller har skrivits, och om utrustningens position. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 24

En man, som tidigare misstänkts för sexualbrott mot barn över internet i annat land, har på nytt misstänkts för likartad brottslighet. Polisen har fått upp ögonen för hans aktiviteter i ett ärende som rör livesända sexuella övergrepp mot flera barn i Sydostasien. Den misstänkte har i de tidigare ärendena haft som modus att radera information i telefon och datorer med hjälp av särskilda program, vilket inneburit att uppgifterna inte kunnat återskapas och ärendena har därför fått läggas ned. Polisen anar därför att efter ett eventuellt beslag kommer information sannolikt inte finnas kvar och inte heller kunna återskapas.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustningar som kan ge information bl.a. om innehållet i kommunikationen, om lagrade uppgifter innan de raderas och om aktiviteter som inte kommuniceras eller lagras.

Typfall 25

Efter ett fullbordat terroristattentat i ett av våra grannländer får Säkerhetspolisen information om att en av de misstänkta gärningsmännen dagarna före dådet har haft kontakt med ett svenskt mobiltelefonnummer. Det rör sig om ett anonymt kontantkort. Misstanken i Sverige rör medhjälp till terroristbrott. Vid verkställighet av hemlig övervakning av elektronisk kommunikation visar det sig att utrustningen inte används för vanliga telefonsamtal utan att den har varit uppkopplad mot internet vid ett flertal tillfällen.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel så att utrustningens position blir klarlagd. Samtidigt kan åtgärden ge möjlighet att med hjälp av telefonens kamera och mikrofon identifiera personen som använder utrustningen.

Typfall 26

En teleoperatör lämnar information till Säkerhetspolisen om att en av dess anställda kan misstänkas för att lämna ut väldigt känslig teknisk information till främmande makt. Informationen har inte direkt bäring på rikets säkerhet men är av mycket stort värde för det aktuella bolaget i konkurrenshänseende. En förundersökning om grovt företagsspionerі inleds. Domstolen beslutar bl.a. om hemlig rumsavlyssning och hemlig kameraövervakning. Det visar sig att någon i mannens familj i stort sett alltid finns hemma i villan. Dessutom är det omöjligt att sätta upp en kamera riktad mot bostaden. Domstolens beslut bedöms inte kunna verkställas.

De beslutade tvångsmedlen skulle kunna verkställas genom att ett tekniskt hjälpmedel för hemlig dataavläsning installeras i den misstänktes dator. På det sättet kan datorns inbyggda mikrofon och kamera användas.

Typfall 27

Efter ett brandattentat mot en moskébyggnad bedrivs en förundersökning om terroristbrott mot en skäligen misstänkt person. Mannen förekommer sedan tidigare i terrorsammanhang och mycket talar för att han inte är ensam gärningsman. Säkerhetspolisen bedriver fysisk spaning mot honom och kan konstatera att han har många kontakter som han träffar på caféer på bostadsorten. Spanarna ser att mannen använder en smartphone och bedömer att det inte är möjligt att komma så nära samtalsparterna att det går att uppfatta vad som sägs. Ibland är det inte ens möjligt att se vilka personer han träffar. Domstolen beslutar om hemlig rumsavlyssning och hemlig kameraövervakning och anger som platser i tillståndet vissa caféer som han tidigare besökt. Tyvärr visar det sig när tvångsmedlen ska verkställas att han hela tiden väljer nya platser för sina möten. Domstolens beslut bedöms inte kunna verkställas.

De beslutade tvångsmedlen skulle kunna verkställas genom att ett tekniskt hjälpmedel för hemlig dataavläsning installeras i den misstänktes smartphone. På det sättet kan mobiltelefonens inbyggda mikrofon och kamera användas.

8.4 Andra uppgifter från de brottsbekämpande myndigheterna

8.4.1 Hur kan hemlig dataavläsning verkställas?

I direktiven framgår att vi ska kartlägga och beskriva bl.a. hur en metod för hemlig dataavläsning kan förväntas verkställas. Det framgår också av direktiven att vi ska utgå från de tekniska möjligheter som finns i dag. Vi ska i det följande beskriva de fem faser som varje verkställighet av hemlig dataavläsning kommer behöva passera genom om åtgärden tillåts.[12] Uppgifter har lämnats av tekniska experter vid brottsbekämpande myndigheter och dessa har fått tillfälle att gå igenom framställningen.

Det bör framhållas att det inte vore ändamålsenligt att göra allt för detaljerade beskrivningar av de tekniker som kan användas för hemlig dataavläsning. Dels för att det inte är fråga om statiska tekniker utan i stället om dynamiska sådana som kommer behöva skräddarsys med olika detaljer och egenskaper utifrån förutsättningarna i varje enskilt fall, dels för att utvecklingen på området är snabb och detaljer i teknikerna därför snabbt kan bli utdaterade. Av denna anledning görs framställningen av tekniken i det följande på en övergripande nivå. Trots detta tenderar framställningen att bli tämligen teknisk i vissa delar. För att göra den mer lättbegriplig för den som saknar tekniska förkunskaper inleder vi därför här med ett enkelt och konkret exempel avseende verkställighet av hemlig rumsavlyssning som sedan löper som en röd tråd genom framställningen av faserna. Exemplet löper sedan som jämförelsematerial i beskrivningen av respektive fas.

Exempel: Verkställighet av hemlig rumsavlyssning

Polisen har information om att en misstänkt (målpersonen) ska träffa en brottskumpan vid ett möte i målpersonens hem (1). Polisen vet genom spaning att hemmet är försett med dörrar som är svårforcerade (åtminstone utan att lämna märken efter sig) men har noterat att målpersonen, när denne vid samma tid varje dag lämnar hemmet under en timma, placerar nyckeln till altandörren på ett visst gömställe (1).

[12] Informationen i detta avsnitt är främst inhämtad från utredningens studiebesök och andra möten med tekniska experter vid brottsbekämpande myndigheter i såväl Sverige som utomlands. Enligt dessa kommer de åtgärder/faser som nedan anförs vara nödvändiga vid verkställighet av hemlig dataavläsning oavsett hur lagstiftning om åtgärden slutligt utformas (t.ex. avseende vilken teknik som får användas eller vilka uppgifter som får samlas in).

> Polisen skaffar sig tillstånd till hemlig rumsavlyssning i målpersonens hem med tillstånd att ta sig in där (1). När det blir dags att verkställa åtgärden använder sig polisen av den gömda nyckeln för att ta sig in i bostaden (2). Väl på plats där inne placerar polismännen mikrofoner och sändare på de platser där mötet förväntas äga rum (3). Mötet äger rum och den tekniska utrustningen som placerats i bostaden skickar det ljud som tas upp till polisens avlyssningsenhet som kan lyssna på det som sägs (4). När mötet har ägt rum beger sig polisen åter till bostaden för att på nytt ta sig in där och hämta tillbaka utrustningen (5).

I all sin enkelhet innehåller exemplet samtliga fem faser som kommer genomgås även vid verkställighet av hemlig dataavläsning. Faserna, som framgår av de siffror som är satta inom parentes, är:

1. Kartläggning/planering
2. Intrång
3. Installation
4. Avläsning
5. Avslut (avinstallation)

Kartläggnings-/planeringsfas

För att hemlig dataavläsning alls ska kunna lyckas, i meningen få in uppgifter som eftersöks, är det av avgörande betydelse att den verkställande brottsbekämpande myndigheten har skaffat sig kunskaper om målpersonen. I första hand tar kartläggningen sikte på att identifiera vilken typ av teknisk utrustning (målobjekt) som målpersonen använder eftersom det är mot målobjektet som åtgärden ska riktas. Målobjektet kan vara både fysiskt (t.ex. en dator eller mobiltelefon) och immateriellt (t.ex. ett e-postkonto, en app eller ett program).

Även uppgifter om målpersonen kan vara av stor betydelse för en lyckad verkställighet, såsom dennes säkerhetsmedvetande och var hen och målobjektet befinner sig vid olika tidpunkter. Också beträffande målobjektet kommer den brottsbekämpande myndigheten som ska verkställa åtgärden behöva göra en tämligen omfattande kartläggning, t.ex. avseende vilken version som används (såväl hård- som programvara) och vilka tekniska sårbarheter (se följande avsnitt) som är kända om målobjektet.

Utifrån resultatet av kartläggningen kommer den brottsbekämpande myndigheten som har att verkställa åtgärden sedan behöva planera hur det ska ske. Det kan tänkas en rad olika tekniker för detta. Först när en lyckad kartläggning skett och planeringen är genomförd kommer det emellertid vara rimligt att ansöka om tillstånd att genomföra åtgärden.

Om kartläggnings- och planeringsfasen kan sägas att de uppgifter som nämnts här endast är exempel på sådan information som kan vara nödvändig för en lyckad verkställighet. Det är inte möjligt att uttömmande redogöra för vilka uppgifter som kommer att behövas eftersom det kan och kommer att skilja sig åt i varje enskilt fall och beroende på vad som är syftet med åtgärden (t.ex. vilka uppgifter som eftersöks eller om åtgärden vidtas i brottsförhindrande eller brottsutredande verksamhet). Vad som däremot är säkert är att hemlig dataavläsning inte kommer att kunna genomföras utan att en kartläggning har skett. Kartläggningen uppvisar i alla delar stora likheter med traditionellt inre och yttre polisiärt spaningsarbete varför de brottsbekämpande myndigheterna är väl förberedda för sådana åtgärder som ingår här.

I exemplet avseende hemlig rumsavlyssning tog kartläggningen av målpersonen (den misstänkte) sikte på att det skulle ske ett möte som bedömdes som intressant. Målobjektet (i det fallet låter vi detta representeras av den misstänktes bostad) kartlades på så vis att spaning utvisade att detta vid en viss tid lämnas obevakat och att det fanns ett sätt att då ta sig in i det (den gömda nyckeln). När tillräcklig kartläggning genomförts ansöktes om tillstånd. Motsvarande uppgifter, men då i stället avseende egenskaper hos den tekniska utrustningen och möjligheter att ta sig in i den utan att det märks, kommer alltså behöva samlas in även vid hemlig dataavläsning.

Intrångsfasen

När en lyckad kartläggning och planering genomförts och tillstånd meddelats kan den praktiska verkställigheten inledas. Den brottsbekämpande myndigheten som ska verkställa åtgärden går då in i det som vi kallar intrångsfasen. För att beskriva denna fas krävs först en kort förklaring av två centrala begrepp. Det första begreppet är *sårbarhet* (eng. vulnerability). Med begreppet avses i detta samman-

hang något som gör ett it-system känsligt för angrepp. På webbsidan IT-ord[13] förklaras begreppet sårbarhet enligt följande.

> Sårbarheter kan vara tekniska brister eller förbiseenden, mänskliga svagheter eller en kombination. Oftast menar man brister i datornätverkens system för identifiering, inloggning och rättigheter. Kontrollen av in- och utgående datatrafik kan ha sårbarheter, liksom granskningen av den utrustning som ansluts till nätverket, och de program som körs. I en bredare bemärkelse kan sårbarheter också vara mänskliga svagheter som slarv, tanklöshet och naivitet […] i kombination med teknik som inte har utformats för att kompensera för sådana svagheter.[14]

När vi i detta betänkande talar om sårbarheter gör vi det i den bredare bemärkelse som nämns i citatet. Det innebär att en sårbarhet kan vara både av teknisk natur, såsom en bugg[15] i ett it-system eller en felaktig inställning däri, eller av personlig natur, såsom brister i säkerhetstänkande hos en användare.

Det kanske kan förefalla enklare att förstå att mänskliga tillkortakommanden förekommer (t.ex. att en person använder samma lösenord på flera olika konton, använder ett lösenord som är lätt att lista ut eller har dålig kontroll på sin telefons säkerhetsinställningar) än att det finns inbyggda sårbarheter i de it-system som vi alla dagligen använder. Naturligtvis arbetar de allra flesta företag och organisationer som tillhandahåller elektroniska tjänster eller utvecklar produkter för elektronisk kommunikation kontinuerligt med att försöka hålla en hög säkerhet. Det tycks dock vara omöjligt att utforma systemlösningar helt utan buggar, och i förlängningen därmed helt utan potentiella sårbarheter.

Mycket förenklat kan detta förklaras med att datorer är dumma, i meningen att de gör vad den som programmerar sagt åt dem att göra. Det innebär att programmeringen måsta vara helt exakt och korrekt. Minsta lilla, om än obetydliga, fel i programmeringen (som ju som utgångspunkt genomförs av människor) kan leda till buggar som i sin tur kan innebära sårbarheter som kan utnyttjas för att bereda sig tillträde till utrustningen.[16]

---

[13] IT-ord är en sajt med ord och termer från it-branschen som tillhandahålls av Computer Sweden och IDG. IT-ord redigeras och uppdateras av Anders Lotsson, skribent på IDG och representant för IDG i Svenska Datatermgruppen. (it-ord.idg.se/om-it-ord/)
[14] it-ord.idg.se/ord/sarbarhet/
[15] Buggar är fel i programkod eller i andra tekniska konstruktioner, se it-ord.idg.se/ord/bugg/
[16] För en mer utförlig beskrivning av olika typer av buggar och sårbarheter och varför det troligen alltid kommer att finnas sådana i it-system se Bellovin et. al. *Lawful Hacking: Using*

Själva utnyttjandet av en sårbarhet för oss in på det andra begreppet som behöver förklaras för att intrångsfasen ska bli förståelig, nämligen *exploit*. Vi har valt att använda det engelska uttrycket eftersom det saknas en vedertagen svensk motsvarighet i förevarande sammanhang, även om attackmetod, attack mot sårbarhet och utnyttjande av sårbarhet ibland används. På webbsidan IT-ord förklaras exploit på följande vis.

> Metod som utnyttjar en sårbarhet i ett datorsystem för att komma åt skyddad information eller för sabotage. Kallas ofta för exploit script, men en exploit behöver inte vara ett skript utan kan vara ett komplett program eller en annan metod. Ordet exploit används om:
>
> – själva attacken (även kallad exploitation);
>
> – metoden eller programmet som används;
>
> – sårbarheten som angriparen drar fördel av.[17]

För att undvika begreppsförvirring använder vi här inte exploit för att beskriva sårbarheten i sig, den benämner vi helt enkelt sårbarhet. Givetvis avses inte heller med exploit att utnyttja en sårbarhet för sabotage, utan målet för en exploit i förevarande sammanhang är endast att komma åt skyddade uppgifter. Det bör redan här nämnas att en exploit sällan avser endast intrångsfasen utan också kan sägas vara en del av installationsfasen. Till detta återkommer vi i nästa avsnitt. I förevarande avsnitt är därför endast själva intrångsdelen av intresse när vi talar om exploit.

En exploit ser olika ut beroende bland annat på vilken sorts sårbarhet som ska utnyttjas och om den kräver fysisk tillgång till it-systemet mot vilket den ska adresseras eller om det är möjligt att genomföra den på distans (t.ex. via en webbsida eller ett e-postmeddelande). En enkel form av exploit kan vara att logga in på målpersonens e-postkonto genom att använda dennes inloggningsuppgifter. En mer avancerad form kan vara att styra om ett anrop från en dator till en webbsida så att datorn i stället dirigeras till en webbsida som kontrolleras av angriparen. Användaren förmås sedan

existing vulnerabilities for wiretapping on the internet s. 22 ff. Det bör också förtydligas att buggar i programvara ofta existerar utan att innebära en sårbarhet som kan utnyttjas för intrång i systemet.

[17] it-ord.idg.se/ord/exploit/

t.ex. att ladda ner programkod som utnyttjar en sårbarhet på användarens dator. Som nämndes inledningsvis är det dock inte ändamålsenligt att i detalj redovisa tekniker. De två exempel som här lämnats får därför anses visa på den bredd som finns när det gäller olika tekniker för att utnyttja en sårbarhet.

Som torde ha framgått är en förutsättning för en lyckad intrångsfas vid verkställighet av hemlig dataavläsning dels att det finns en sårbarhet som kan utnyttjas för intrång, dels att sårbarheten faktiskt utnyttjas för åtkomst. Detta kan jämföras med exemplet avseende hemlig rumsavlyssning. Den sårbarhet som identifierades där var att målpersonen vid en viss tid varje dag lämnade sin bostad (obevakad) och att denne då gömde nyckeln på ett särskilt ställe, dvs. att det i och för sig finns möjlighet att ta sig in utan upptäckt och utan att lämna spår. Det som kan jämföras med exploit är själva intrånget (dvs. polismännens användande av nyckeln för att komma in i huset obemärkt). Också placeringen av avlyssningsutrustning och polismännen i sig själva kan emellertid sägas vara en del av den exploit som genomförs (se installationsfasen).

Det som sagts ovan har tagit sikte på intrång i kommunikationsutrustning. Hemlig dataavläsning skulle emellertid också kunna verkställas utan intrång i sådana system, t.ex. med särskild hårdvara. Exempel på sådan hårdvara är s.k. tangentloggare (eng. keylogger) som fysiskt har fästs på eller vid teknisk utrustning för att registrera knapptryckningar som sedan skickas till eller samlas in av den brottsbekämpande myndigheten.[18] När det är fråga om sådan verkställighet är intrångsfasen i det närmaste helt identisk med vad som gäller vid exempelvis hemlig rumsavlyssning, dvs. det handlar då om att hitta sätt att obemärkt få fysisk tillgång till den utrustning som åtgärden ska riktas mot (sårbarhet) och sedan utnyttja detta sätt (exploit), t.ex. genom att fästa en tangentloggare på utrustningen.

[18] Tangentloggare finns också som programvara, dvs. program som registrerar knapptryckningar eller motsvarande.

Installationsfasen

Intrånget i teknisk utrustning har inte något självändamål. Om det efter ett sådant intrång inte är eller kan göras möjligt för den brottsbekämpande myndigheten att samla in den eftersökta informationen är intrånget meningslöst. Av den anledningen är installationsfasen av betydelse. Vi ska strax återkomma till den. Först ska dock sägas att när en sårbarhet utgörs av att den brottsbekämpande myndigheten har tillgång till exempelvis målpersonens inloggningsuppgifter till ett e-postkonto kan det förekomma att någon installation inte är nödvändig. Så är t.ex. fallet om det enda som eftersöks är en misstänkt persons e-postmeddelanden. Vid sådana tillfällen kan således installationsfasen snabbt lämnas till förmån för avläsningsfasen (se nedan) eftersom sådana meddelanden då kan vara möjliga att läsa utan någon installation av t.ex. program som ska möjliggöra avläsning.

Installationsfasen torde dock inte sällan vara av stor betydelse, oavsett om verkställighet sker med hårdvara eller programvara. I föregående avsnitt redogjorde vi för begreppet exploit. Vad vi dock inte utvecklade särskilt där är att en exploit typiskt sett innefattar inte bara själva intrånget utan också en installation av det tekniska hjälpmedel som ska möjliggöra avläsningen. Eftersom ett intrång inte är av något värde för den brottsbekämpande myndigheten om det inte möjliggör insamling av den information som eftersöks krävs att nödvändig utrustning (tekniska hjälpmedel) installeras.

För att en sådan installation ska kunna genomföras när programvara ska användas för avläsningen krävs i typfallet två saker, dels ett installationsprogram, dels den programvara som läser av de uppgifter som avses, dvs. det tekniska hjälpmedlet. Installationsprogrammet har, som namnet antyder, till uppgift att installera det tekniska hjälpmedlet medan alltså den andra programvaran utgör det tekniska hjälpmedlet. För att på nytt återknyta till rumsavlyssningsexemplet i inledningen skulle installationsprogrammet kunna jämföras med polismännen (som ju installerar) och det tekniska hjälpmedlet med mikrofonerna och sändarna.

Både installationsprogrammet och det tekniska hjälpmedlet kommer att behöva skräddarsys och kommer därmed att se olika ut beroende på förutsättningarna i det enskilda fallet, t.ex. systemarkitekturen i det system där intrånget ska ske och vilka typer av uppgifter som ska läsas av, t.ex. kommunikationsuppgifter eller

lagrade uppgifter. Det är därför inte ändamålsenligt att på detaljnivå beskriva konstruktionen av dessa olika programvaror.

Det bör nämnas att när hemlig dataavläsning sker med hjälp av hårdvara som fästs på, i eller vid målobjektet, t.ex. en tangentloggare, är svårigheterna i installationsfasen desamma som vid exempelvis hemlig rumsavlyssning, nämligen att undvika att utrustningen eller den som installerar den upptäcks.

Avläsningsfasen

När en lyckad installation har skett sker själva informationsinsamlingen (avläsningen). Den kan gå till på olika sätt beroende på vilken metod som valts för verkställighet. När avläsning sker efter att den brottsbekämpande myndigheten använt inloggningsuppgifter till t.ex. ett e-postkonto kan avläsningen ske genom att den som verkställer åtgärden, på plats i den brottsbekämpande myndighetens lokaler, direkt från en datorskärm tar del av innehållet i de e-postmeddelanden som avläsningen avser. När det är fråga om avläsning med programvara som installerats i den misstänktes utrustning kommer den installerade programvaran, liksom är fallet vid verkställighet av befintliga hemliga tvångsmedel, möjliggöra för den brottsbekämpande myndigheten att i sina lokaler ta del av uppgifterna som läses av eftersom dessa skickas elektroniskt dit. Det kommer i båda fallen att krävas program hos den brottsbekämpande myndigheten som tar omhand de uppgifter som hämtas in och omvandlar dessa till läsbar information. I vissa fall, främst när det gäller verkställighet genom hårdvara, kommer det inte att vara möjligt att hämta in uppgifterna löpande på distans. I de fallen kommer avläsning vara möjlig först sedan den utrustning som använts har samlats in.

När det gäller avläsningsfasen uppvisar den tydliga likheter med informationsinsamlingen vid verkställande av befintliga hemliga tvångsmedel. Jämförelsen med det inledningsvis nämnda rumsavlyssningsexemplet kan därför te sig tämligen överflödig. För formens skull ska ändå nämnas att avläsningen av information kan jämföras med att ljudet som tas upp skickas till (och avlyssnas på) den brottsbekämpande myndighetens avlyssningsenhet.

Avslutningsfasen (avinstallationen)

När verkställigheten avslutas sker avinstallation eller motsvarande. Det innebär att den teknik som använts tas bort eller görs obrukbar. Även i denna fas är det i hög grad beroende på vilken teknik som valts för hur så ska ske och vilka resurser det förutsätter. Antingen kommer det ske på samma sätt som i det inledande rumsavlyssningsexemplet, dvs. att den brottsbekämpande myndigheten hämtar tillbaka utrustningen, eller genom att man avaktiverar, avinstallerar, tidsbegränsar eller på annat sätt utesluter möjligheten att fortsätta nyttja det tekniska hjälpmedlet. Utredningen har av tekniska experter vid de brottsbekämpande myndigheterna försäkrats om att det, om verkställighet sker med programvara, alltid kommer att vara möjligt att antingen avinstallera denna eller på annat sätt göra den obrukbar efter en viss tidpunkt.

8.4.2 Vilka resurser kräver hemlig dataavläsning?

I situationer där de brottsbekämpande myndigheterna har eller får tillgång till inloggningsuppgifter skulle det vara möjligt redan i dag – utan att det krävdes några särskilda resurser – att använda dessa för inloggning på en tjänst eller liknande för att därefter läsa innehållet där. Några särskilda resursbehov när det gäller hemlig dataavläsning efter sådan inloggning kan således inte sägas föreligga.

Såvitt avser resursåtgång för att installera hårdvara som teknik för att genomföra hemlig dataavläsning torde den vara att jämföra med resursåtgången för att installera utrustning för hemlig rumsavlyssning. Även vid en sådan åtgärd är det ju fråga om installation av hårdvara i visst utrymme. De hårdvaror det skulle bli fråga om vid hemlig dataavläsning, exempelvis s.k. keyloggers (som registrerar vilka knappar som trycks ned på ett tangentbord), finns på marknaden och är inte förenade med sådana kostnader som gör att anskaffningen av dessa kan sägas vara av betydelse. Det som fortsättningsvis behandlas i detta avsnitt gäller därför enbart verkställighet av hemlig dataavläsning med programvara.

Redan i dag finns det tekniker för att verkställa hemlig dataavläsning. Om så inte vore fallet skulle ju åtgärden i de länder åtgärden används (se t.ex. kapitel 5) vara tämligen ineffektiv. Grovt indelat kan man säga att de brottsbekämpande myndigheterna skulle kunna

införskaffa sådana tekniker på två sätt. Båda dessa sätt har sina förrespektive nackdelar.

För det första skulle myndigheterna kunna köpa in programvara från kommersiella aktörer. En fördel som ett sådant förfarande skulle innebära är att det borde möjliggöra ett relativt snabbt igångsättande av tekniken för hemlig dataavläsning eftersom de produkter eller tjänster som tillhandahålls via kommersiella aktörer torde vara utvecklade redan. De kommersiella aktörerna på marknaden kan också förväntas ha ett intresse av att var behjälpliga med iordningställande och implementering av ett nytt systemstöd för att komma över uppgifter och ta omhand dessa. Det finns emellertid också nackdelar med att införskaffa dylika systemlösningar från kommersiella aktörer. En uppenbar sådan är att det finns risk för att de brottsbekämpande myndigheterna blir utlämnade till andras tekniska kunnande. I sig självt är detta tämligen oproblematiskt men med hänsyn till den typ av uppgifter som metoden är avsedd att samla in, särskilt med avseende på sekretess- och integritetsfrågor, och vikten av att inga obehöriga har möjlighet att ta del av dessa uppgifter är det ett problem att behöva förlita sig på utomstående (utan sådan behörighet). Dessutom finns risk för att de brottsbekämpande myndigheterna inte har möjlighet att själva vidareutveckla teknikerna om de förvärvas från kommersiella aktörer. Till de nu anförda nackdelarna kommer även ett ekonomiskt perspektiv. Som kommer att framgå i det följande är också andra sätt som finns för att komma över systemlösningar som kan verkställa hemlig dataavläsning kostsamma. När det gäller förvärvande från en privat kommersiell aktör kan det förväntas att inköpspriset bara för att komma över små eller begränsade systemlösningar eller tekniker blir väldigt högt.

Det andra sättet att komma över en teknik för att verkställa hemlig dataavläsning är egen utveckling. De uppenbara fördelarna med ett sådant tillvägagångssätt skulle vara att de brottsbekämpande myndigheterna då själva förfogar över sina tekniska metoder och utan hinder kan vidareutveckla dessa. De skulle också kunna skräddarsys för verksamheten och de åtgärder som de ska användas för. Det skulle därtill vara möjligt för de brottsbekämpande myndigheterna att upprätthålla ett starkt metodskydd eftersom det alltid kan vara klarlagt vilka personer som har tillgång till upplysningar om tekniken. Även vid egen utveckling av tekniska metoder skulle emellertid anskaffningskostnaderna bli betydande. En organisation

av tekniker skulle behöva arbeta för att få fram fungerande och lämplig teknik vilket skulle innebära väsentliga personalkostnader. Dessutom kommer det att vara fråga om ett löpande utvecklingsarbete även sedan teknik och systemlösningar tagits fram, dels för att effektivisera, dels för att ta fram ny teknik.

Som synes finns olika för- och nackdelar med båda sätten att införskaffa system för verkställighet. En kombination av de två anskaffningssätten kan inte uteslutas. Oavsett vilket sätt som väljs för att införskaffa en teknisk metod för hemlig dataavläsning kommer de brottsbekämpande myndigheterna att behöva avsätta resurser för utveckling och underhåll av både system och kompetens. Detta för att kunna verkställa åtgärden och ta till vara på den information som hämtas in. I kapitel 12 redovisas de kostnader som de brottsbekämpande myndigheterna bedömt kommer uppstå för att införskaffa tekniken som behövs.

Det sagda har tagit sikte på resurser för teknikanskaffning. Hemlig dataavläsning kommer också kräva tämligen omfattande resurser vid verkställighet av ett enskilt ärende. I den delen torde emellertid åtgärden närmast vara att jämföra med resursåtgången vid hemlig rumsavlyssning, se avsnitt 8.4.1.

8.4.3 Hur kan data som inhämtats med metoden bearbetas?

Mycket av den information som kan hämtas in med en metod för hemlig dataavläsning är redan i dag sådan att de brottsbekämpande myndigheterna har rättslig men inte faktisk tillgång till den.[19] Samtliga fyra brottsbekämpande myndigheter som verkställer hemliga tvångsmedel (Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket) har, utifrån den egna organisationens respektive behov, därför redan i dag en struktur för bearbetning av den information som hämtas in. Det finns en för dessa myndigheter gemensam systemlösning inom ramen för Samordnad Teknisk Inhämtning (STI) där data från den hemliga tvångsmedelsanvändningen tas omhand. Från den gemensamma systemlösningen fördelas insamlad data till den verksamhetsgren som har att ta hand om den. Inom Polismyndigheten finns exempelvis olika verksamhets-

[19] Se beträffande betydelsen av detta förklaringen i avsnitt 4.3.3.

grenar för ”internetavlyssning” (dvs. avlyssning av datakommunikation efter tillstånd till hemlig avlyssning av elektronisk kommunikation) och ”telefonsamtalsavlyssning”, vilka båda får de uppgifter som ska bearbetas och analyseras från den nämnda systemlösningen.

De uppgifter som skulle kunna bli tillkommande med hemlig dataavläsning (beroende på hur metoden utformas) jämfört med de uppgifter som samlas in genom befintliga hemliga tvångsmedel är sådana som innebär att den brottsbekämpande myndigheten tar del av t.ex. innehåll på den tekniska utrustningen som avläses eller inloggningsuppgifter som knappas in. Liksom övriga data som kommer in genom hemlig tvångsmedelanvändning är även dessa data digitala. Omvandlingen till läsbar information av dessa data är varken svårare eller enklare än den omvandling som redan sker. Med hänsyn till att de brottsbekämpande myndigheterna redan i dag omhändertar data i digital form vid hemlig tvångsmedelsanvändning finns förutsättningar att bearbeta även tillkommande data som kan förväntas av hemlig dataavläsning. Detta gäller oavsett om den myndighetsgemensamma systemlösningen kan användas även för hemlig dataavläsning eller om nya systemlösningar behövs.

Mot bakgrund av de kostnader som det kommer att vara förenat med att ta fram teknik för hemlig dataavläsning kan det förutses att verkställighet och insamling på något sätt kommer att behöva ske samordnat mellan de brottsbekämpande myndigheterna. Så har skett tidigare vid införande av vissa hemliga tvångsmedel och myndigheterna har, som redan nämnts, ett fungerande samarbete inom ramen för STI.

9 Bör hemlig dataavläsning införas som ett nytt hemligt tvångsmedel?

9.1 Inledning

Vid införande av nya tvångsmedel krävs att noggranna avvägningar har gjorts beträffande vilket behov av åtgärden som finns, åtgärdens förväntade effektivitet och nytta samt vilka integritetsintrång åtgärden kan förväntas medföra. Det är först efter en analys av dessa perspektiv som det är möjligt att göra avvägningar avseende om åtgärderna bör införas. Sådana analyser och avvägningar måste också göras när ändringar föreslås som utökar användningsområdet för befintliga tvångsmedel. Integritetsskyddskommittén anförde bland annat följande beträffande dessa analyser och avvägningar.[1]

> Europakonventionens och regeringsformens krav på att en inskränkning i envars rätt till respekt för sitt privatliv etc. skall vara nödvändig torde som ett minimikrav innebära att man kan påvisa och beskriva ett faktiskt behov av en sådan inskränkning. Det är således inte tillräckligt att i allmänna ordalag resonera kring att det kan finnas ett behov av utvidgade möjligheter att använda ett tvångsmedel. När ett faktiskt behov väl är påvisat gäller det för lagstiftare att väga detta behov mot vikten av att värna rättssäkerhet och personlig integritet, dvs. att göra en proportionalitetsbedömning. Det är därvid inte tillfyllest att lagstiftaren lakoniskt ”finner” att nyttan av ett på visst sätt utformat tvångsmedel är större än behovet av att bevara skyddet för den personliga integriteten på en intakt nivå, utan vad som krävs är en resonerande framställning där omständigheter som talar för tvångsmedlets supremati omsorgsfullt prövas och bryts mot de argument som talar i motsatt riktning. Utan en sådan noggrann genomgång saknas möjlighet till verklig insikt i vilka motiv som varit avgörande för lagstiftaren. Om nödvändigheten av att införa ny integritetskränkande tvångsmedelslagstiftning inte förklaras på ett övertygande sätt finns risk att lagstiftningen möts med misstro och

[1] SOU 2007:22 Del 1 s. 176 f.

> att medborgarnas förtroende för lagstiftningen och intentionerna bakom densamma minskar till skada för rättssamhället i stort. Det ligger också i lagstiftarens eget intresse att ge en fyllig analys och beskrivning av motivbilden beträffande i princip all integritetsinskränkande lagstiftning. Om behovsanalysen är alltför knapphändig och ingen egentlig proportionalitetsavvägning görs löper lagstiftaren nämligen i värsta fall risken att de dömande instanserna med rätt eller fel underkänner lagstiftningen såsom stridande mot Europakonventionens och/eller regeringsformens krav i fråga om skyddet för den personliga integriteten.

Det finns skäl att ansluta sig till Integritetsskyddskommitténs uppfattning om de analyser och avvägningar som ska göras, vilken också ligger väl i linje med vad som anges i våra direktiv. Frågan är emellertid hur de olika analyserna ska ske.

I direktiven anges avseende frågan om *behov* att det, för att det ska vara möjligt att göra proportionalitetsavvägningen, inledningsvis måste fastställas om det finns ett *reellt behov* av hemlig dataavläsning som metod i brottsbekämpningen eller om den brottsbekämpande förmågan kan upprätthållas med mindre integritetskänsliga metoder. Att det ska vara fråga om ett reellt behov förtydligas senare i direktiven med att det endast är under förutsättning att behovet är *tungt vägande* och *grundligt redovisat* som det kan ligga till grund för fortsatta överväganden om att införa metoden. Frågor som rör behovet av hemlig dataavläsning behandlas i avsnitt 9.2.

När det gäller frågan om den förväntade effektiviteten anges i direktiven att vi ska ta reda på om hemlig dataavläsning kan förväntas vara en effektiv metod för brottsbekämpning i förhållande till behovet. I direktiven ges också några exempel som kan vara av betydelse för effektivitetsbedömningen, såsom hur metoden tekniskt kan utformas samt vilka tekniska möjligheter och problem som kan förutses vid verkställighet. I avsnitt 9.3 redovisas våra bedömningar beträffande effektivitet.

Vad sedan avser vilka följder hemlig dataavläsning kan få för den personliga integriteten anges bl.a. följande i direktiven. Varje befogenhet för staten att bereda sig tillgång till information om medborgarna leder till ingrepp i den personliga integriteten. Ramarna för intrånget bestäms av hur befogenheten avgränsas och utformas i lag. En behörighet för brottsbekämpande myndigheter att i realtid hemligt läsa information i och från datorer och andra tekniska utrustningar, t.ex. mobiltelefoner, skulle potentiellt kunna innebära ett omfattande intrång i enskildas privatliv. Vid överväganden om hemlig

dataavläsning måste därför integritetseffekterna beskrivas noga. Det måste så långt det är möjligt redogöras för hur skyddet för den personliga integritetens kärnområden, dvs. sådant som rör individen och dennes personlighet, skulle påverkas av hemlig dataavläsning, bl.a. risken för att andra personer än den som är föremål för tvångsåtgärden påverkas. Våra bedömningar beträffande integritetsrisker presenteras i avsnitt 9.4.

När analyserna av behov, effektivitet och integritetsrisker är redovisade övergår vi i avsnitt 9.5 till några inledande proportionalitetsavvägningar. Kapitlet avslutas sedan med ett avsnitt om reglerna om egendomsskydd, och dessas betydelse vid avvägningarna om hemlig dataavläsning (avsnitt 9.6).

9.2 Behov

Utredningens bedömning: Det föreligger tungt vägande behov av nya och bättre metoder för att i hemlighet komma åt uppgifter som redan i dag får hämtas in i de brottsbekämpande myndigheternas verksamhet men som på grund av bl.a. den tekniska utvecklingen och brotts- och samhällsutvecklingen i övrigt inte kan kommas åt.

9.2.1 Utgångspunkter

Att döma av utredningsdirektiven och det tidigare förslaget om hemlig dataavläsning (SOU 2005:38) är den primära anledningen till att hemlig dataavläsning alls diskuteras problem vid hemlig avlyssning av elektronisk kommunikation. Stort utrymme har där ägnats åt denna fråga i jämförelse med utrymmet som ägnats åt andra åtgärder som kan vidtas och uppgifter som kan samlas in med metoden. Det kan också noteras att när Utredningen om vissa hemliga tvångsmedel i sitt betänkande (SOU 2012:44) uttalade något om hemlig dataavläsning (vilket, trots att betänkandet egentligen inte handlade om den åtgärden, gjordes på grund av att de brottsbekämpande myndigheterna ”med viss emfas” framhållit att det fanns ett behov) så nämn-

des inte något annat behovsområde än det som sades finnas på kommunikationsavlyssningsfältet.[2]

Hemlig dataavläsning är dock en speciell metod eftersom den möjliggör insamling av olika typer av uppgifter, alltså inte bara kommunikationsuppgifter. I detta avseende skiljer sig metoden från befintliga hemliga tvångsmedel, som ju huvudsakligen är avgränsade utifrån vilken typ av uppgifter som kan samlas in med dem. Som framgått i avsnitt 4.3.3 skulle det med hemlig dataavläsning vara möjligt att, utöver innehåll i och uppgifter om elektronisk kommunikation, samla in också andra typer av uppgifter. Som exempel nämndes bl.a. lagrade uppgifter (innefattande t.ex. dokument, fotografier och program), detaljerade positioneringsuppgifter (innefattande t.ex. GPS-positioner för viss teknisk utrustning) och andra avlyssnings- eller övervakningsuppgifter (innefattande t.ex. ljud- eller bildupptagning sedan ett program på en mobiltelefon startas upp för att använda telefonens mikrofon eller kamera).

Det går att tala om behov utifrån olika perspektiv, t.ex. behovet av att kunna samla in vissa uppgifter (informationsbehov) eller behovet av nya metoder för informationsinsamling (metodbehov). När Utredningen om vissa hemliga tvångsmedel undersökte behovet av bl.a. hemlig rumsavlyssning och några hemliga tvångsmedel som användes i preventivt syfte var analysen primärt inriktad på styrkan av informationsbehovet (dvs. hur starkt behovet är av den information man förväntar sig av det hemliga tvångsmedlet samt vad informationen kunde förväntas leda till). Det är en naturlig utgångspunkt för behovsprövningen när det är tydligt avgränsat vilka typer av uppgifter som är möjliga att samla in med en viss metod. Eftersom hemlig dataavläsning skulle kunna användas för att samla in olika typer av uppgifter behöver vi dock först avgränsa vilka typer av uppgifter vår analys omfattar. Först därefter kan vi fråga oss om det finns behov av informationen som de olika uppgiftstyperna kan ge i den brottsbekämpande verksamheten. En tredje fråga som behöver besvaras i behovsanalysen är om det finns behov av en ny metod för att samla in uppgifterna.

Bedömningarna av om det finns tungt vägande informationsbehov och, om så är fallet, tungt vägande behov av att få använda

[2] Se avsnitt 4.2.2.

hemlig dataavläsning för att samla in uppgifterna kommer att göras utifrån följande ”uppgiftstyper”.

1. *Innehåll i och uppgifter om meddelanden som överförs eller överförts i elektroniskt kommunikationsnät*

   Uppgiftstypen motsvarar uppgifter som enligt 27 kap. 18 § rättegångsbalken i dag får samlas in efter tillstånd till hemlig avlyssning av elektronisk kommunikation och uppgifter som enligt 27 kap. 19 § första stycket 1 rättegångsbalken i dag får samlas in efter tillstånd till hemlig övervakning av elektronisk kommunikation. Uppgifterna får i dag hämtas in både under förundersökning under de förutsättningar som anges i rättegångsbalken och i underrättelseverksamhet enligt bestämmelserna i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och lagen (1991:572) om särskild utlänningskontroll (LSU). Delar av uppgifterna (historiska uppgifter om meddelanden som överförts) får också hämtas in i underrättelseverksamhet enligt bestämmelserna i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen).

2. *Lokaliseringsuppgifter*

   Uppgiftstypen motsvarar uppgifter som enligt 27 kap. 19 § första stycket 2 och 3 rättegångsbalken i dag får samlas in efter tillstånd till hemlig övervakning av elektronisk kommunikation.[3] Uppgifterna får i dag hämtas in både under förundersökning under de förutsättningar som anges i rättegångsbalken och i underrättelseverksamhet enligt bestämmelserna i preventivlagen, LSU och inhämtningslagen.

[3] Enligt 27 kap. 18 § tredje stycket rättegångsbalken gäller att tillstånd till hemlig avlyssning av elektronisk kommunikation också ger rätt att vidta åtgärder som kan vidtas efter tillstånd till hemlig övervakning av elektronisk kommunikation. Lokaliseringsuppgifter kan således hämtas in även vid hemlig avlyssning av elektronisk kommunikation.

3. *Optisk personövervakning*

   Uppgiftstypen motsvarar uppgifter som enligt 27 kap. 20 a § rättegångsbalken i dag får samlas in efter tillstånd till hemlig kameraövervakning. Uppgifterna får i dag hämtas in både under förundersökning under de förutsättningar som anges i rättegångsbalken och i underrättelseverksamhet enligt bestämmelserna i preventivlagen.

4. *Avlyssning av samtal m.m.*

   Uppgiftstypen motsvarar uppgifter som enligt 27 kap. 20 d § rättegångsbalken i dag får samlas in efter tillstånd till hemlig rumsavlyssning. Uppgifterna får i dag endast hämtas in under förundersökning under de förutsättningar som anges i rättegångsbalken.

5. *Uppgifter som finns elektroniskt lagrade och uppgifter som visar hur viss teknisk utrustning används*

   Uppgifter som finns elektroniskt lagrade får samlas in av brottsbekämpande myndigheter i samband med undersökning av teknisk utrustning vid husrannsakan, enligt bestämmelserna i 28 kap. rättegångsbalken eller vid undersökning av teknisk utrustning som tagits i beslag enligt 27 kap. rättegångsbalken. Motsvarande möjlighet att ta del av uppgifterna saknas i dag i underrättelseverksamhet.

   Möjligheten att samla in uppgifter som visar hur teknisk utrustning används saknar motsvarighet i befintlig tvångsmedelslagstiftning men kan vara möjlig att samla in genom t.ex. spaning. Uppgiftstypen avser t.ex. tangenttryckningar, skrivande i dokument som inte sparas och uppgifter om vilka program som används.

Ett alternativ för behovsanalysen hade varit att kort och gott presentera analysen för respektive ”uppgiftstyp” som nu presenterats, var för sig. Så kommer att ske men eftersom det enligt vår mening är av stor betydelse för analysen att flertalet av de presenterade uppgifterna redan i dag får samlas in efter tillstånd till befintliga hemliga tvångsmedel har vi funnit skäl att också försöka strukturera behovs-

analysen på ett mer funktionellt sätt. Vi har i denna strävan delat in analysen i två delar, nämligen:

1. Behovet av hemlig dataavläsning för att samla in uppgifter som får samlas in med redan befintliga hemliga tvångsmedel (avsnitt 9.2.3).
2. Behovet av att kunna samla in andra uppgifter från teknisk utrustning än vad som är möjligt med hemliga tvångsmedel i dag (avsnitt 9.2.4).

I den första gruppen hamnar uppgifter som är möjliga att hämta in med hemlig dataavläsning som de brottsbekämpande myndigheterna redan i dag kan få tillstånd att i hemlighet samla in (dvs. uppgifter i kategorierna 1–4 ovan). I den andra gruppen hamnar uppgifter som kan hämtas in med hemlig dataavläsning som i dag inte är möjliga för brottsbekämpande myndigheter att få tillgång till genom användning av hemliga tvångsmedel (uppgifter i kategori 5 ovan).

Det finns en skillnad i behovsanalysen avseende dessa två delar eftersom det i den första redan är klarlagt att det finns ett reellt behov för de brottsbekämpande myndigheterna att kunna samla in uppgifterna. Det ingår inte i vårt uppdrag att pröva om de behovsanalyser som gjorts tidigare beträffande informationsbehovet fortfarande har skäl för sig. Vår behovsanalys i den delen tar därför primärt sikte på i vilken utsträckning det finns ett reellt behov av nya metoder eller tekniker för att kunna komma åt uppgifterna. I den andra delen får frågan om informationsbehovet en mer framträdande plats.

Innan vi kommer in på den egentliga behovsanalysen gör vi en kort summering av vad som kan sägas ha framkommit beträffande förändrade förhållanden som skäl för att nya metoder behövs i den brottsbekämpande verksamheten.

9.2.2 Allmänt om behovet av hemlig dataavläsning

Av redovisningen i kapitel 6 framgår att teknikutvecklingen som skett under de senaste 20 åren har varit mycket snabb. I allt högre utsträckning förlitar sig myndigheter, företag och privatpersoner på ny teknik och internet. Som framgår av den där redovisade statistiken avseende teknik- och internetanvändning synes Sverige bestå av personer som gärna tar till sig den nya tekniken. För att bara nämna några områden kan vi konstatera att landet i dag består av en befolk-

ning där större delen av invånarna dagligen använder smarttelefoner, där e-post och direktmeddelanden via telefoner och datorer är vardagligheter för de allra flesta och där medborgarna har ett flertal olika användarkonton på en rad internetsidor och sociala nätverk.

I de allra flesta avseenden har teknikutvecklingen och internetanvändningen inneburit något positivt. Samtidigt finns åtminstone en baksida av teknikutvecklingen. Lika tillgänglig som tekniken är för var och en är den för kriminella. Det innebär i många fall att kriminella, liksom befolkningen i övrigt, kan ta del av t.ex. kommunikationstjänster, konton på internet och smarttelefoner men använda dessa i sin kriminalitet. Tydliga exempel på sådant ont uppsåt finns i Europols rapport IOCTA 2016. Bland annat framgår där att det blir allt vanligare att personer, via internet, beställer och regisserar livesända sexuella övergrepp mot barn i fattiga länder som sedan visas och spelas in för att spridas. Vidare framgår där att internet, särskilt sociala medier, fungerar som propagandaspridare bland terroristgrupperingar. Även på flera andra områden rapporteras i IOCTA 2016 om hur kriminella utnyttjar internet och ny teknik för sin verksamhet. Också svenska undersökningar och uppgifter från representanter för de brottsbekämpande myndigheterna vittnar om ett ökat användande av internet och ny teknik i organiserad kriminell verksamhet både för att begå brott och för att dölja brottslighet, se t.ex. avsnitt 7.5.

I det moderna informationssamhället har frågan om informationssäkerhet aktualiserats på många plan. Det kan konstateras att medvetenheten ökat bland människor, företag, myndigheter och stater om att det finns risker med internet och att det därför uppstått mycket goda och helt legitima skäl för dem att skydda sina förehavanden från insyn. Det framstår som tydligt för utredningen att även kriminella vill göra så. Detta är givetvis ingen ny företeelse. ”Katt- och råttalekar” mellan brottsbekämpning och kriminella har pågått under alla tider. Kriminella har i denna jakt ofta utnyttjat fördelar som ny teknik kan ge dem. Frågan är dock om ny teknik någonsin tidigare, på ett så enkelt sätt, gett kriminella ett sådant försteg framför brottsbekämpningen som den nya tidens teknik gett, t.ex. när det kommer till möjligheterna att dölja sin brottslighet. Med ganska enkla medel kan kriminella exempelvis utnyttja verktyg, som tagits fram och utvecklats för helt legitima syften, som ett skydd mot insyn från brottsbekämpningsmyndigheterna. Dessutom

möjliggör internet i sig för vissa kriminella att begå brott utan att befinna sig på ”brottsplatsen”.

Det är svårt att kvantifiera hur mycket ny brottslighet som tillkommit i takt med den tekniska utvecklingen, främst internettillgången. På en rad områden har traditionell kriminalitet tagit steget in i it-miljö. De nämnda sexuella övergreppen på distans är ett sådant exempel. Det finns också områden där ny brottslighet kan sägas ha uppstått genom den tekniska utvecklingen. Ett exempel är utvecklingen och användningen av sabotageprogram i illegala syften, t.ex. att ta kontrollen över samhällsviktiga funktioner eller slå ut företagsnätverk.

Något som kan slås fast, oavsett om det är fråga om helt nya typer av brottslighet eller traditionell brottslighet i ny skepnad, är att en stor del av alla brott som i dag begås och planläggs lämnar digitala spår. I synnerhet torde detta gälla allvarlig brottslighet som kräver viss planering, där en fungerande kommunikation ofta är av stor betydelse. Av denna anledning är definitionen som Brå använt i sin rapport om it-relaterad brottslighet (se avsnitt 7.2) användbar även i detta sammanhang. För ju mer digitala spår som lämnas innan, vid och efter allvarlig brottslighet desto större anledning finns det att fundera på vilka utredningsmetoder som kan anses lämpliga för att hitta, ta till vara på och analysera dessa spår. Detta synsätt gör sig i allra högsta grad gällande både i brottsförebyggande och brottsutredande verksamhet.

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

Innehåll i och uppgifter om meddelanden som överförs eller överförts i elektroniskt kommunikationsnät

Inledning

Metoden för hemlig dataavläsning skulle kunna användas för att samla in sådant innehåll i meddelanden som de brottsbekämpande myndigheterna i dag kan få tillstånd att hämta in genom användning av hemlig avlyssning av elektronisk kommunikation. Metoden skulle också kunna användas för att samla in uppgifter om meddelanden som får hämtas in efter tillstånd till hemlig övervakning av elek-

tronisk kommunikation eller genom inhämtning enligt inhämtningslagen.

Hemlig telefonavlyssning fanns i rättegångsbalken redan när balken infördes. Innan år 1989 avsåg avlyssningen dock endast det som kanske kan beskrivas som ”klassisk” telefonavlyssning, vilken ofta verkställdes genom att polisen fysiskt kopplade in sig på de koppartrådar som telefonsamtal, i vilka brottsmisstänkta personer deltog, färdades genom. Först i samband med införande av bestämmelserna om hemlig teleavlyssning och teleövervakning i 27 kap. 18 och 19 §§ rättegångsbalken år 1989 gavs de brottsbekämpande myndigheterna möjlighet att få tillstånd att avlyssna och övervaka även annan kommunikation än telefonsamtal. Det som är särskilt viktigt för denna utredning vidkommande är att lagstiftaren i samband med den lagändringen införde möjligheter för de brottsbekämpande myndigheterna att ”lyssna av” datakommunikation. Anledningen till att lyssna av satts inom citationsmarkering är att avlyssningen i dessa sammanhang i realiteten innebär avläsning av data (i vart fall som en förutsättning för att avlyssning, t.ex. när det är fråga om röst- eller videosamtal via internet, sedan ska kunna ske).

Till grund för bedömningen att ändra på regelverket om telefonavlyssning låg bl.a. Tvångsmedelskommitténs betänkande *Tvångsmedel – Anonymitet – Integritet* (SOU 1984:54). Kommittén föreslog dock inte att dataöverföring skulle omfattas av avlyssningsbestämmelserna eftersom det ”enligt RPS ännu inte uppstått något behov av att tillgripa motsvarande åtgärder”. Kommittén konstaterade emellertid att det visserligen kunde antas ”att även dataöverföring i en framtid kan komma att användas som ett sätt att befordra meddelanden i t.ex. brottslig verksamhet” (SOU 1984:54 s. 220). När regeringen cirka fem år efter Tvångsmedelslagskommitténs slutbetänkande lade fram propositionen som låg till grund för de då nya reglerna om hemlig teleavlyssning och hemlig teleövervakning gjordes således en annan bedömning än den som kommittén redovisat beträffande datakommunikation. I propositionen konstaterades först, helt i enlighet med Tvångsmedelskommitténs förslag, att om polisen har rätt att avlyssna telefonsamtal under vissa betingelser, bör motsvarande möjlighet finnas när det gäller t.ex. text- eller bildöverföring. Däremot ansåg departementschefen att lagstiftningsförslaget också skulle omfatta all kommunikation som befordras via det allmänna telenätet, vilket innebar att sådan datakommunikation som sker över ett telenät

skulle komma att omfattas. Detta ansågs vara befogat ”med hänsyn till den snabba tekniska utveckling som skett sedan Tvångsmedelskommittén lade sitt betänkande” (prop. 1988/89:124 s. 39).

Det har inte framkommit någonting som talar för att avlyssning och övervakning av traditionell telefoni, dvs. telefoni som inte är IP-telefoni, via koppartråd (fast telefoni) och i etern (mobiltelefoni) fungerar sämre än den gjort tidigare. Enligt uppgift till utredningen fungerar denna avlyssning och övervakning tvärtom fortfarande som den ska. Det bör dock framhållas att den tekniska utvecklingen har inneburit att allt mindre kommunikation (i såväl tal som skrift) sker via traditionell telefoni. Det beror både på de nya internetbaserade kommunikationstjänster som utvecklats och i allt högre utsträckning används och på att det finns en generell utveckling som innebär att traditionell telefoni övergår till att vara IP-baserad. Det innebär att de metoder som finns för att fånga upp sådan kommunikation efter tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation kan förutsättas fortsätta tappa i värde. När det gäller avlyssning och övervakning av datakommunikation, dvs. huvudsakligen kommunikation som sker via internet, är nämligen befintliga metoder för att samla in uppgifter sällan eller aldrig tillräckliga.

Konsensus råder bland brottsbekämpande myndigheter (vilket framkommit både i behovsbeskrivningarna och vid utredningens olika studiebesök) om att ny teknik och kriminellas kunskaper om polisens metoder har gjort att hemlig avlyssning och övervakning av elektronisk kommunikation i dag är långt ifrån lika effektiva metoder för avlyssning och övervakning av datakommunikation (dvs. främst avlyssning och övervakning av kommunikation som sker via internet) som de varit tidigare. Den mest framträdande orsaken till detta är den ökande krypteringsgraden som märks i kommunikation mellan kriminella.

Problem relaterade till kryptering

Kryptering av kommunikation innebär att de brottsbekämpande myndigheterna inte får del av innehållet i kommunikationen (avlyssning), och i många fall inte heller uppgifter om kommunikationen (övervakning), i klartext utan i stället endast av oläsbar rappakalja. Enligt uppgifter till utredningen i både behovsbeskriv-

ningar och vid studiebesök hos de enheter vid brottsbekämpande myndigheter som ansvarar för avlyssning och övervakning har framkommit att mer än 90 procent av den avlyssnade internettrafiken i dag är krypterad. Denna datakommunikation kan bestå av exempelvis samtal via appar, direktmeddelanden, e-post och internetsurf, vilka därmed alltså inte är möjliga att ta del av i klartext. Det anförda innebär således att mindre än tio procent av den datakommunikation som i dag får avlyssnas eller övervakas faktiskt kan läsas i klartext av de brottsbekämpande myndigheterna, och således ge information i ärendet. Av dessa knappa tio procent utgör, enligt uppgift, merparten surfande hos nyhetsbyråer (vanligen via tidningstjänsters appar) och på pornografiska webbsidor och är därmed sällan av värde för de utredningar där avlyssning sker.

Att andelen kommunikation som krypteras av all kommunikation, dvs. inte bara kommunikation som avlyssnas eller övervakas av de brottsbekämpande myndigheterna, under senare tid har ökat markant finns starkt stöd för inte bara i behovsbeskrivningarna. Ett tydligt exempel är Googles statistik avseende kryptering av inkommande och utgående e-posttrafik från och till andra e-postleverantörer som redovisats i avsnitt 6.3.2. Av denna statistik framgår att cirka 30 procent av såväl inkommande som utgående trafik till och från Gmail[4] i slutet av 2013 var skyddad med krypterad överföring. Motsvarande andel i början av oktober 2017 var cirka 89 procent.

Att en allt större andel av befolkningen använder sig av internetbaserade kommunikationstjänster torde vara allmänt känt och tydliggörs också i de rapporter som redovisats i avsnitt 6.2. Där framgår också att de som använder sådana tjänster gör så allt mer. Det finns ingenting som tyder på att kriminella skulle avvika från befolkningen i övrigt när det gäller den ökade användningen av internetbaserade kommunikationstjänster. Rapporterna om it-relaterad brottslighet och kriminellas användning av internet i och för sin brottslighet (avsnitt 7.2 och 7.3) och uppgifterna i behovsbeskrivningarna talar snarare i motsatt riktning, dvs. att kriminella i än högre utsträckning använder sig av sådana kommunikationsmöjligheter. Därtill kommer att de allmänna beskrivningar om viss

[4] Gmail är en gratis webbaserad e-posttjänst från Google som i dag torde vara en av världens största s.k. webbmejltjänster. Det bör sägas att all e-post som skickas mellan Gmails användare är krypterad och exkluderad i statistiken.

allvarlig brottslighet (främst terroristbrottslighet och organiserad brottslighet) som redovisats i avsnitt 7.4 och 7.5, liksom behovsbeskrivningarna, vittnar om att det i dessa typer av kriminalitet är av särskild betydelse med välfungerande och säkra kommunikationer.

Några utgångspunkter för de fortsatta bedömningarna bör därför vara att kriminella använder internetbaserade kommunikationstjänster i stor utsträckning i sin kriminalitet[5] och att en stor, och alltjämt ökande, andel av internettrafiken (inklusive kommunikation via internetbaserade kommunikationstjänster) i dag krypteras. Det ska påpekas att kryptering i många fall inte kräver en aktiv åtgärd av den som använder internet och internetbaserade kommunikationstjänster. I stället har i stort sett samtliga appar och program som används för kommunikation i dag inbyggda funktioner för skydd och säkerhet (kryptering) som standard för alla användare.

Det saknas underlag och säkra kvantitativa uppgifter om hur vanligt det är att kriminella använder ytterligare kryptering utöver den som erbjuds som standard. Av de uppgifter som framkommit i behovsbeskrivningarna och vid utredningens studiebesök hos de brottsbekämpande myndigheterna vågar vi i vart fall dra slutsatsen att det förekommer, i synnerhet bland vissa grupper av organiserat kriminella och i nätverk som Säkerhetspolisen i sin verksamhet har i uppdrag att kontrollera. Frågan är emellertid av underordnad betydelse eftersom även standardmetoderna för kryptering uppenbarligen är så svårgenomträngbara för den som försöker forcera dem att de brottsbekämpande myndigheterna i regel inte kan komma åt sådana uppgifter i klartext.

Problem relaterade till anonymisering

Det är emellertid inte bara kryptering som i behovsbeskrivningarna framhållits som problem för de brottsbekämpande myndigheterna med att komma åt innehåll i och uppgifter om meddelanden. Också

[5] Här bör återigen påminnas om definitionen av it-relaterad brottslighet i avsnitt 7.2 enligt vilken som it-relaterad brottslighet räknas inte bara att it är målet eller medlet för brottsligheten utan också att it har beröring med brottet, exempelvis genom att digitala spår lämnas som kan användas som bevisning. Även om internetbaserade kommunikationstjänster används som mål eller medel för brott torde det i de flesta fall, när det gäller hemlig avlyssning och övervakning av elektronisk kommunikation, vara beröringen med brottsligheten som är av störst intresse för de brottsbekämpande myndigheterna.

anonymisering, dvs. åtgärder som av annan anledning än kryptering begränsar effekten som verkställighet av åtgärderna medför, har anförts som skäl för nya metoder.

Avlyssning och övervakning av elektronisk kommunikation riktad mot en mobiltelefon utförs i dag i normalfallet genom att teleoperatörer förser de brottsbekämpande myndigheterna med innehållet i den kommunikation (och uppgifter om kommunikationen) som belastar abonnemanget. Det kan vara samtal, sms och internettrafik (vilken alltså i sig kan bestå av t.ex. samtal och direktmeddelanden motsvarande sms men också av annat internetsurfande och e-posttrafik). När en avlyssnad person övergår från att använda abonnemangets (eller kontantkortets) surf till att använda WiFi-nätverk belastar surfandet inte längre abonnemanget (eller kontantkortet). Att så sker innebär inte alltid att användaren agerar för att undgå avlyssning. I stället är det ett rimligt, vanligt och helt legitimt sätt att utnyttja kanske både snabbare surfhastighet och lägre kostnad eller minskad förbrukning för det egna abonnemanget. Att abonnemanget eller kontantkortet inte belastas innebär dock i dessa fall att de brottsbekämpande myndigheterna inte kan ta del av den internetbaserade kommunikation som sker. Annorlunda uttryckt kan man säga att kommunikationen anonymiseras för de brottsbekämpande myndigheterna. Det blir således – även i situationer där den avlyssnade inte vidtagit medvetna åtgärder för att undvika avlyssning – i viss mån slumpmässigt vilka uppgifter brottsbekämpande myndigheter kan komma över med hjälp av hemlig avlyssning eller övervakning av elektronisk kommunikation. En sådan ordning framstår inte som godtagbar. Dessutom ger behovsbeskrivningarna vid handen att åtgärden bland kriminella används för att undvika avlyssning och övervakning. Det är naturligtvis än mer otillfredsställande att beslutade åtgärder inte fungerar som de är tänkta i dessa situationer.

Också andra typer av anonymisering, då mer medveten sådan, vållar enligt behovsbeskrivningarna problem. Det handlar främst om anonymiseringstjänster som gör enskilda individer ”osynliga” i sin internetkommunikation i så måtto att de använder anonymiserade (och avindividualiserade) IP-nummer för kommunikationen, se t.ex. avsnitt 6.3.3. Problematiken med anonymiserad kommunikation är att de brottsbekämpande myndigheterna i många fall inte får del av den alls, till skillnad från i krypteringsfallen där man alltså får del av

uppgifterna i krypterad form. I övrigt är problematiken och de bedömningar som behöver göras desamma som vid problemen med kryptering. Det saknas därför skäl att upprepa det vi sagt tidigare.

Konsekvenser av kryptering och anonymisering

Flera av de brottsbekämpande myndigheterna har anfört att problemen får stora konsekvenser. Exempel på sådana konsekvenser som förts fram i behovsbeskrivningarna är i tidigt skede nedlagda eller bortvalda utredningar. Så sker när andra utredningsåtgärder än hemlig avlyssning (eller övervakning) av elektronisk kommunikation inte bedömts vara till nytta för utredningen och avlyssning eller övervakning inte förväntas fungera på grund av kryptering eller anonymisering. Andra exempel är att man inte kommer åt de personer som är av kanske allra störst intresse för utredningarna; de i toppen av hierarkin i kriminella organisationer. Dessa personer uppvisar nämligen enligt behovsbeskrivningarna inte sällan ett mycket högt säkerhetsmedvetande (som i nu aktuellt avseende yttrar sig genom t.ex. hög grad av kryptering) och gör dessutom typiskt sett inte sådana misstag som krävs för att utredningar ska lyckas (t.ex. slarvar med inloggningsuppgifter eller underlåter att använda kryptering). Dagens ordning kan därför ofta innebära att de brottsbekämpande myndigheterna, trots kännedom om vilka dessa individer är, saknar möjlighet att komma åt dem och därigenom störa ut den kriminalitet de styr över. Detta framstår som synnerligen otillfredsställande.

Ytterligare konsekvenser som förts fram är att en hög grad av krypterad kommunikation i ärenden där hemlig avlyssning av elektronisk kommunikation används (dvs. ärenden som trots detta inte lagts ned eller valts bort) får till följd att utredningarna tar väsentligt längre tid och mer sällan leder till att brottsmisstänkta åtalas och döms. Längre utredningstid torde dessutom i allmänhet leda till högre utredningskostnader.

Det bör i sammanhanget som avser konsekvenser av problemen med kryptering sägas något om regeringens årliga redovisning till riksdagen avseende användningen av hemliga tvångsmedel. En läsning av dessa redovisningar ger nämligen knappast vid handen att kryptering utgör ett särskilt stort problem vid verkställighet av

hemlig avlyssning och övervakning av elektronisk kommunikation. Den nyttobedömning som där görs, dvs. vilken nytta de brottsbekämpande myndigheterna anser sig ha av tvångsmedlen, har varit tämligen konstant över tid.[6] Dessutom har antalet tillstånd till hemlig avlyssning och övervakning ökat över tid.

För det första bör den omständigheten att det förekommer i tidiga stadier bortvalda och nedlagda utredningar påverka den totala nyttan av tvångsmedelsanvändningen eftersom dessa fall inte ens tillståndsprövas, än mindre leder till tvångsmedelsanvändning (och således inte finns med i statistiken). Om nedlagda och bortvalda utredningar inte finns representerade i den årliga statistiken dras resultatet inte ned eftersom det endast är situationer där tvångsmedel använts som redovisas.

För det andra är, som redan nämnts, hemlig avlyssning och övervakning av elektronisk kommunikation fortfarande effektiva och fungerande tvångsmedel när det gäller vanlig telefoni (fast och mobil) som inte är IP-telefoni. Det innebär att när nytta uppkommer i ett ärende, t.ex. på grund av att en misstänkt slarvat i sin kommunikation och använt okrypterad överföring och då nämner något som bedöms vara till nytta för utredningen, anses tvångsmedlet ha varit till nytta även om resten av kommunikationen är krypterad. Vanlig mobiltelefoni (samtal och sms) torde dessutom fortfarande förekomma som kommunikationsmedel bland en del kriminella som utsätts för avlyssning eller övervakning. Det innebär att det fortfarande förekommer ärenden med hemlig avlyssning eller övervakning av elektronisk kommunikation som kan verkställas utan de problem som beskrivits.

För det tredje är nyttobedömningen som görs och även andra statistiska uppgifter i de årliga redovisningarna svårbedömda och svårjämförda eftersom kriterier har ändrats över tid. Nyttobedömningen har utsatts för kritik, se t.ex. hänvisningar i den senaste redovisningen.[7] Därtill har i olika sammanhang framhållits svårigheten att leda i bevis att en viss åtgärd har lett till en viss effekt. Allra tydligast i detta avseende har nog Utredningen om vissa hemliga tvångsmedel

[6] Som anfördes i avsnitt 8.2 har Åklagarmyndigheten i sin skrivelse till regeringen avseende tvångsmedelsanvändningen för 2016 dock noterat minskad nytta med hemlig avlyssning av elektronisk kommunikation i vissa avseenden jämfört med tidigare år, bl.a. till följd av kryptering.
[7] Skr. 2016/17:69 s. 34.

varit. Det finns därför skäl att citera ett avsnitt ur den utredningens betänkande.[8]

> Att en viss nyttoeffekt – t.ex. att åtal eller lagföring skett – är knuten till informationen från ett visst hemlig tvångsmedel är ofta problematiskt att belägga. Detta beror bl.a. på att information blir relevant som en bit i ett större pussel (betydelsen av den enskilda pusselbiten är svår att avgöra) och att det blir fråga om orsakssamband i flera led (t.ex. tvångsmedel – förhör – annat tvångsmedel – åtal). Är effekten att ett visst brott förhindrats, blir svårigheten att belägga ett orsakssamband ännu större.

Till detta ska läggas att nyttoredovisningen är tämligen binär, dvs. antingen uppstår nytta eller så uppstår inte nytta. Det är alltså inte fråga om större eller mindre nytta alternativt en gradering av nytta i varje ärende som redovisas. Det innebär att oavsett hur stor nytta (eller hur många av de nyttoeffekter ”som räknas”) man skulle kunna få ut av ett tvångsmedel så är det tillräckligt, för att tvångsmedelsanvändning i ett visst ärende ska anses ha varit nyttig, att någon nytta har uppkommit.

Dessutom kan man nog inte heller bortse från att syftet med redovisningen, som ju i förlängningen är att upprätthålla legitimiteten för de hemliga tvångsmedlen, kan påverka om man i gränsfallen läser in nytta eller inte. Det är i vart fall inte en orimlig tanke att de brottsbekämpande myndigheterna, som ju rimligen är intresserade av att behålla möjligheterna till tvångsmedelsanvändningen, kan tänkas tolka tveksamma resultat på ett för den egna verksamheten positivt sätt. En sådan tolkning kan leda till att fler ärenden än vad som borde vara fallet räknas till de nyttiga.

Till det anförda kommer också att antalsjämförelser är vanskliga att göra utifrån de årliga redovisningarna. Som exempel kan nämnas att antalet tillstånd fram till och med år 2009 redovisades på ett sätt som gjorde att flera teleadresser kunde innefattas i ett tillstånd medan det från år 2010 redovisades en teleadress per tillstånd. Det har från representanter från de brottsbekämpande myndigheterna också framhållits att antalet tillstånd inte är en särskilt relevant uppgift för att få reda på hur utvecklingen sett ut eftersom uppgiften inte säger något om hur många personer som utsatts för tvångsmedelsanvändning. Detta då det är ett vanligt agerande bland kriminella att t.ex. använda flera telefoner. Tyvärr är inte heller uppgifter

[8] SOU 2012:44 s. 33.

om antalet misstänkta som utsatts för tvångsmedel direkt möjlig att jämföra under någon längre tid. Första gången sådana uppgifter redovisades var år 2009. Då, och fram till och med redovisningen för 2012, redovisades det sammanlagda antalet misstänkta som utsatts för *något* hemligt tvångsmedel. Från och med redovisningen för år 2013 lades i stället fram uppgifter om antalet misstänkta som utsatts för *respektive* tvångsmedel.

Vår bedömning är, mot bakgrund av det som nu anförts, att det inte behöver finnas en motsättning mellan att nyttan med hemlig avlyssning och övervakning av elektronisk kommunikation synes vara tämligen konstant över tid och ökade problem med vissa typer av hemlig avlyssning och övervakning av elektronisk kommunikation (avlyssning och övervakning av internetkommunikation). Inte heller behöver det finnas en motsättning mellan att antalet tillstånd ökat över tid och dessa problem. Det bör dessutom påpekas att Åklagarmyndigheten i sin redovisning för tvångsmedelsanvändningen 2016 rapporterar om minskad nytta i vissa avseenden, vilket enligt myndigheten ”skulle kunna tas till intäkt för att värdet av hemlig avlyssning av elektronisk kommunikation generellt sätt har minskat från 2015 till 2016”.

Sammanfattande slutsatser

Sammanfattningsvis kan beträffande behovet av nya åtgärder sägas följande. Det har på senare år skett en kraftig minskning avseende i vilken utsträckning brottsbekämpande myndigheter genom hemlig avlyssning och övervakning av elektronisk kommunikation kan ta del av internetbaserad kommunikation och uppgifter om sådan kommunikation. Minskningen beror på såväl medveten som omedveten användning av krypterings- och anonymiseringstjänster i kombination med att internetbaserad kommunikation kommit att stå för en allt större andel av den totala elektroniska kommunikationen, vilken kan förväntas fortsätta. Sammantaget leder detta till att de brottsbekämpande myndigheterna med dagens verkställighetstekniker kan ta del av endast en liten del av den internetbaserade kommunikationen som domstolens tillstånd avser i dag jämfört med för några få år sedan och en synnerligen liten del jämfört med för exempelvis tio år sedan. Eftersom andelen internetbaserad kommuni-

kation kan förväntas fortsätta att öka lär utvecklingen fortsätta i samma riktning. Mot bakgrund av att så mycket som 90 procent av den avlyssnade kommunikationen (av internetbaserad kommunikation) i dag kan vara dold för de brottsbekämpande myndigheterna framstår behovet i denna del som tungt vägande.

Den nu gjorda analysen leder till slutsatsen att en metod som ger tillgång till de uppgifter som här diskuterats i klartext skulle vara mycket värdefull för de brottsbekämpande myndigheterna. Det får därför anses föreligga tungt vägande behov för de brottsbekämpande myndigheterna att med nya metoder kunna bereda sig tillgång till sådana uppgifter.

Hemlig avlyssning och övervakning av elektronisk kommunikation är möjliga åtgärder både i brottsförebyggande och brottsutredande verksamhet efter beslut av domstol, se kapitel 3. De problem som här konstaterats beträffande detta tvångsmedel skiljer sig inte åt beroende på vilken laglig grund som avlyssningen vilar på; de anledningar som redovisats som skäl till problemen gör sig helt enkelt gällande både i de brottsförebyggande och brottsutredande fallen. Det finns också stöd för denna slutsats i det underlag vi redovisat i kapitel 7 om att såväl terrorister som organiserat kriminella är beroende av kommunikation i sin verksamhet och att de använder sig av olika krypterings- och anonymiseringslösningar för att undvika upptäckt från brottsbekämpande myndigheter. Det kan därför inte anses föreligga olika behov beroende på om syftet med åtgärden är brottsförhindrande eller brottsutredande (dvs. om den sker i underrättelseverksamhet eller i förundersökningsverksamhet).

Lokaliseringsuppgifter

Genom hemlig övervakning av elektronisk kommunikation och inhämtning enligt inhämtningslagen har de brottsbekämpande myndigheterna möjlighet att få tillgång till lokaliseringsuppgifter avseende bl.a. mobiltelefoner. Det kan gälla uppgifter om vilken basstation en telefon eller annan elektronisk kommunikationsutrustning varit uppkopplad mot i samband med kommunikation. Tidigare gällde att lokaliseringsuppgifter, för att kunna lämnas ut, hade genererats i samband med att mobiltelefonen varit uppkopplad för kommunikation. Lokaliseringsuppgifter som fanns hos operatören och som

genererades av utrustningens kontakt med en basstation utan att det var fråga om kommunikation omfattades alltså inte. Dessa regler ändrades år 2012. Sedan dess finns inte något krav på att lokaliseringsuppgifterna ska ha genererats i samband med att den tekniska utrustningen har varit uppkopplad för kommunikation och lokaliseringsuppgifter som finns hos operatören som genereras av utrustningens kontakt med en basstation utan att det varit fråga om kommunikation kan därför numera hämtas in. Detta gäller enligt både reglerna om hemlig övervakning av elektronisk kommunikation och inhämtningslagens bestämmelser.

Uppgifter om var elektronisk kommunikationsutrustning befinner eller befunnit sig finns inte bara hos teleoperatören utan också många gånger i utrustningen. Hemlig dataavläsning skulle därför kunna användas för att ta del av sådana uppgifter. Så skulle kunna ske både genom att ta del av de uppgifter som finns sparade i en telefon med platsinformation och genom aktivering av inbyggd positioneringsutrustning, t.ex. GPS.

Dessa uppgifter torde vara väsentligt mer exakta än de som kan hämtas in från operatören om vilken mast telefonen kopplat upp sig mot.[9] Det säger sig självt att det vore en stor fördel för brottsbekämpningen med exakta lokaliseringsuppgifter jämfört med de uppgifter som kan hämtas in i dag. Som Åklagarmyndighetens experter framhållit i sin behovsbeskrivning är det en enorm skillnad mellan att påstå att en person befunnit sig på brottsplatsen X vid tidpunkten Y med hjälp av en lokaliseringsuppgift som täcker ett område av flera kvarter en kvart före brottstidpunkten och att påstå detsamma med en exakt GPS-positionering vid den exakta brottstidpunkten.

Det har i behovsbeskrivningarna framhållits att EU-domstolens dom[10] den 21 december 2016 om bl.a. de svenska bestämmelserna om lagringsskyldighet för leverantörer av elektroniska kommuni-

[9] Det kan visserligen framhållas att det i stadsmiljö inte sällan är möjligt att med tämligen god precision genom s.k. mastpositionering mot bakgrund av att det i stadsmiljö finns många basstationer. Sådan positionering torde emellertid aldrig kunna nå samma exakthet som lokalisering med GPS, vilken i många fall kan lämna uppgift om var den tekniska utrustningen befinner sig med en felmarginal på endast några meter.

[10] I domen (mål C 203/15) slog EU-domstolen fast bl.a. att de svenska reglerna om lagringsskyldighet inte stod i överensstämmelse med EU-rätten på grund av att de föreskrev en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.

kationstjänster medfört att de brottsbekämpande myndigheterna får tillgång till färre och mindre detaljerade lokaliseringsuppgifter än vad som var fallet innan domen. Enligt uppgift från Tullverket innehåller exempelvis uppgifterna från vissa operatörer efter domen inte någon detaljerad information alls om var den person som är misstänkt för brott finns eller har funnits vid en viss intressant tidpunkt. Åklagarmyndigheten har förklarat att det sedan domen inte längre, från vissa operatörer, kan inhämtas uppgifter om telefonens position vid ett telefonsamtals slut.

Ytterligare en aspekt som framhållits av åklagarexperterna är att lokaliseringsuppgifter enligt nu gällande ordning förutsätter att telefonen är påslagen. Så är sällan fallet i direkt samband med utförandet av ett planerat brott.

När den ovan nämnda lagändringen genomfördes år 2012 framhöll regeringen i propositionen beträffande inhämtning av lokaliseringsuppgifter i realtid att myndigheterna på det sättet t.ex. kan följa en viss mobiltelefon längs en flyktväg eller lokalisera ett gömställe eller den plats där en eventuell gärningsman kan befinna sig. För att uppnå sådana syften framstår det som självklart att än mer detaljerade uppgifter än de som är möjliga att samla in i dag skulle vara synnerligen värdefulla. Säkerhetspolisen har exempelvis anfört att i flera utredningar som myndigheten har och har haft har positionsuppgifterna från operatörerna varit allt för oprecisa för att vara avgörande när det gäller att knyta en person till en viss plats.

Det som nu framhållits talar enligt vår mening med styrka för att det föreligger tungt vägande behov av nya och bättre metoder för att samla in lokaliseringsuppgifter, som ju enligt befintlig lagstiftning redan får samlas in. Ingenting har framkommit som talar för att behovet skiljer sig åt beroende på om syftet med åtgärden är brottsförhindrande (dvs. åtgärd enligt inhämtningslagen eller preventivlagen) eller brottsutredande (dvs. åtgärd enligt rättegångsbalken).

Optisk personövervakning och avlyssning av ljud

I de fall teknisk utrustning har en kamerafunktion eller mikrofonfunktion skulle tekniska metoder kunna användas för att aktivera dessa funktioner eller någon av dem. Inhämtning av sådana uppgifter

skulle kunna motsvara vad som får hämtas in efter tillstånd till hemlig kameraövervakning och hemlig rumsavlyssning.

Det ska först nämnas att ingenting har framkommit i behovsbeskrivningarna som talar för att hemlig kameraövervakning eller hemlig rumsavlyssning i teknisk mening fungerar sämre i dag än de gjort tidigare, såsom beskrivits ovan beträffande hemlig avlyssning och övervakning av elektronisk kommunikation på grund av kryptering m.m. Däremot har det i behovsbeskrivningarna framkommit att det förekommer tillfällen då det 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 eftersom dagens reglering medfört att vissa kriminella t.ex. undviker platser där åtgärderna kan förväntas vidtas. Säkerhetspolisens experter har exempelvis anfört 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 får eller fysiskt kan verkställas. Andra förfaranden som anförts som exempel i behovsbeskrivningarna är att de som vill undvika åtgärderna inte lämnar lokaler obevakade, växlar platser för möten och vistas i geografiska områden som är svåra för de brottsbekämpande myndigheterna att smälta in i.

Till skillnad från vad som gäller vid hemlig avlyssning och övervakning av elektronisk kommunikation – där ju de tekniska metoderna inte längre ger tillgång till de uppgifter som eftersöks – är det alltså inte tekniken i sig utan endast andra förutsättningar för verkställighet som ligger till grund för vad som anförts som behov av nya metoder. När det gäller möjligheten att aktivera kameran har också en särskild fördel med åtgärden påtalats av de brottsbekämpande myndigheternas experter, nämligen möjligheten att kontrollera vem som använder den tekniska utrustningen. I många fall är en vanlig förklaring när misstänkta personer konfronteras med att vissa meddelanden har skickats eller andra åtgärder vidtagits från deras telefon eller dator att de lånat ut eller låtit någon använda utrustningen, alternativt att det inte är deras telefon eller dator. Med en

möjlighet att t.ex. använda den s.k. ”selfiekameran”, dvs. kameran på en mobiltelefon som är riktad mot användaren kan snabbt avgöras om det är den som åtgärden avser eller annan person som skickat meddelandet. Också möjligheten att på detta sätt identifiera den person som använder utrustning som kan kopplas till viss brottslighet har framhållits som argument för behovet av att kunna aktivera mikrofon (för röstigenkänning) eller kamera (för bildigenkänning) genom hemlig dataavläsning

Även om det i behovsbeskrivningarna inte närmare angetts hur vanligt förekommande sådana omständigheter som de som nu nämnts är framstår det som tydligt att behov uppstår i de brottsbekämpande myndigheternas verksamheter tämligen frekvent. Det kan inte anses tillfredsställande att personer i kriminella miljöer i någon mening förfogar över möjligheterna för de brottsbekämpande myndigheterna att lyckas i sina utredningar. Redan risken för att så blir fallet måste därför enligt vår mening anses utgöra tungt vägande behov av åtgärder som kompletterar de befintliga möjligheterna.

Som nämnts ovan skulle hemlig dataavläsning kunna möjliggöra en löpande insamling av sådana uppgifter som här diskuteras, 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 vilken plats åtgärden får vidtas på (se 27 kap. 20 b, 20 e och 21 §§ rättegångsbalken). Det är emellertid inte bara på sådana platser som uppgifter av intresse för de brottsbekämpande myndigheternas utredningar kan diskuteras mellan kriminella. Det finns inte skäl att ifrågasätta uppgifterna om att kriminella personer, åtminstone personer inom den organiserade brottsligheten, är väl införstådda med vilka platser det är störst risk för att utsättas för åtgärderna på och att dessa personer anpassar sitt beteende efter sådan kunskap i syfte att undgå avlyssning eller övervakning. Det behov som konstaterats vara tungt vägande måste därför anses gälla 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 ske. En annan sak är givetvis att detta behov måste vägas mot både de skäl som föranledde begränsningarna som i dag föreligger och, liksom övriga behov, mot integritetsintresset.

Sammanfattningsvis föreligger enligt utredningens mening tungt vägande behov av att låta hemlig dataavläsning omfatta möjligheten att aktivera en teknisk utrustnings mikrofon eller kamera i syfte att fånga upp och samla in sådana ljud- eller bilduppgifter som i dag får samlas in genom hemlig rumsavlyssning eller hemlig kameraövervakning.

Det bör nämnas att hemlig rumsavlyssning i dag inte är en tillåten åtgärd i brottsförhindrande verksamhet. 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 utom ramen för en förundersökning mer sällan synes finnas konkreta uppgifter om t.ex. att möten ska ske på en viss plats för att avhandla viktiga frågor. Regeringen bedömde därför att behovet i detta skede i högre utsträckning tycktes avse sådan information som typiskt sett erhålls från de andra tvångsmedlen, t.ex. avseende kontaktnät eller rörelsemönster.[11] Vad som framkommit under utredningsarbetet har enligt vår bedömning inte givit skäl att dra några andra slutsatser beträffande behovet än de som regeringen redovisade. Vår bedömning som redovisats ovan tar därför, beträffande uppgifter som får samlas in vid hemlig rumsavlyssning, endast sikte på förundersökningsfallen.

När det däremot gäller hemlig kameraövervakning är åtgärden tillåten i underrättelseverksamhet under de förutsättningar som framgår av preventivlagen (men inte enligt LSU eller inhämtningslagen). Ingenting har framkommit som ger anledning att anta att behovet som vi ovan konstaterat skiljer sig åt mellan förundersöknings- och preventivlagsfallen.

9.2.4 Behovet av att kunna samla in andra uppgifter

Insamling av elektroniskt lagrade uppgifter under förundersökning

Beslags- och husrannsakansinstituten har funnits i rättegångsbalken sedan balken infördes. Det finns dock inga särskilda regler om husrannsakan i eller undersökningar av datorer eller andra informations-

[11] Prop. 2013/14:237 s. 101.

bärare. Inte heller finns några regler i balken som särskilt tar sikte på beslag av elektroniskt lagrade uppgifter.[12]

Enligt svensk rätt anses det tillåtet att besluta om husrannsakan på en viss plats i syfte att söka efter uppgifter som finns lagrade i en elektronisk informationsbärare på platsen. Det krävs då inte något särskilt beslut om husrannsakan för informationsbäraren (se SOU 1995:47 s. 184 och SOU 2011:45 s. 295 och 296). Ofta finns datorer och andra informationsbärare i sådana miljöer, hus, rum eller slutna förvaringsställen som inte får genomsökas utan ett beslut om husrannsakan. I praktiken blir det därför ofta en sekundär fråga hur man ska se på undersökningen av själva informationsbäraren.

Beslag av informationsbärare syftar många gånger till att den utredande myndigheten ska få tillgång till de uppgifter som finns lagrade i föremålet och inte till själva föremålet i sig. Det kan därför tyckas märkligt att det inte finns några lagregler som särskilt behandlar hur uppgifterna i utrustningen får tas om hand eller hur utrustningen får undersökas. Klart är emellertid att i praktiken anses föremål som tas i beslag få undersökas. Denna praxis har ansetts innebära en rätt att gå igenom t.ex. en dators eller mobiltelefons innehåll. Genom husrannsakan och beslag av elektroniska informationsbärare får de brottsutredande myndigheterna således tillgång till elektroniskt lagrade uppgifter.[13]

Av det som nu nämnts står det således klart att redan befintlig lagstiftning ger möjlighet för de brottsbekämpande myndigheterna att samla in uppgifter som lagrats elektroniskt. Detta gäller dock endast i brottsutredande verksamhet eftersom de angivna tvångsmedlen regleras i rättegångsbalken. Vår bedömning är därför att det redan finns ett konstaterat behov av att kunna samla in uppgifter i den brottsutredande verksamheten. När det gäller sådan verksamhet blir därför frågan om det finns tungt vägande behov av en metod som i hemlighet och löpande kan förse brottsbekämpande myndigheter med sådana uppgifter, vilket i praktiken inte är möjligt i dag.

[12] I Beslagsutredningens (Ju 2016:08) uppdrag ingår bl.a. att överväga om ändringar behövs i detta avseende.

[13] I doktrinen har dock anförts att ett beslag ger rätt till en extern undersökning av föremålet, men inte rätt att genomsöka dess innehåll. Företrädarna för denna uppfattning gör gällande att informationsbärarens minne bör betraktas som ett slutet förvaringsställe enligt 28 kap. 1 § RB och att det därför krävs ett beslut om husrannsakan för att dess innehåll ska få undersökas. Se t.ex. Bring och Diesen, Förundersökning, 4 uppl. s. 415.

Insamling av elektroniskt lagrade uppgifter utanför förundersökning

Bakgrund

Som just nämndes gäller rättegångsbalkens regler endast när förundersökning pågår. Det finns inga motsvarande regler som gäller utanför förundersökning, dvs. i den brottsförhindrande verksamheten. Såvitt avser underrättelseverksamheten behöver därför informationsbehovet i sig konstateras. Först om det finns ett sådant behov ska samma fråga som för den brottsutredande verksamheten ställas, dvs. om det finns tungt vägande behov av en metod som i hemlighet och löpande kan förse brottsbekämpande myndigheter med uppgifterna, vilket alltså i praktiken inte är möjligt i dag.

Vad anbelangar informationsbehovet i brottsförhindrande verksamhet bör något först sägas om de brottsbekämpande myndigheternas underrättelseverksamhet. I huvudsak är sådan verksamhet inriktad på att avslöja om en viss, inte närmare specificerad brottslighet har ägt rum, pågår eller kan antas komma att begås. Ett övergripande mål med underrättelseverksamheten är att förse de brottsutredande myndigheterna med kunskap som kan omsättas i operativ verksamhet. I underrättelsearbetet samlar myndigheterna sålunda in, bearbetar och analyserar uppgifter som senare kan ha betydelse för att förebygga och förhindra brott. Det framtagna underrättelsematerialet kan också typiskt sett läggas till grund för ett beslut om att inleda förundersökning.

I propositionen som föregick preventivlagen diskuterades frågan om behovet att tillåta hemliga tvångsmedel innan förundersökning inletts. Regeringen angav i det sammanhanget bl.a. följande beträffande Säkerhetspolisens behov. Den allvarliga brottslighet som Säkerhetspolisen har till uppgift att bekämpa – däribland terrorism, spionage och författningshotande verksamhet – äventyrar stora samhällsvärden och utgör ett hot mot enskilda människors liv och hälsa. Särskilt den under senare åren ökande terrorismen har förstärkt denna hotbild. Brottsligheten är ofta svårbemästrad eftersom Säkerhetspolisen ställs mot motståndare som agerar i det fördolda, med stor förslagenhet och med betydande hänsynslöshet. Det är viktigt att samhället kan värja sig mot detta slag av brottslighet och att åtgärder kan vidtas innan brotten har inträffat. Behovet av ett effektivt underrättelsearbete är därför särskilt tydligt i fråga om

brottslighet av detta slag. Arbetet måste också ibland kunna inledas långt innan man kan tala om misstankar om ett visst brott. Redan uppgifter om att exempelvis ett större attentat kan vara för handen ger naturligtvis anledning att intensifiera spaningsinsatserna, trots att myndigheterna på detta tidiga stadium inte kan veta något närmare om vilket brott som kommer att begås eller vilken eller vilka personer som kommer att genomföra det. [14]

Regeringen konstaterade i propositionen att de dåvarande 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, spionibrott och författningshotande brottslighet. Mot denna bakgrund bedömde regeringen 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.[15]

När det gällde den öppna polisens 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. Såvitt avsåg sådan brottslighet konstaterade regeringen att det förekommer brottslighet i form av allvarliga hot mot befattningshavare inom rättssystemet, mot politiker, och mot personer verksamma inom massmedierna. Sådan brottslighet utgör inte bara ett hot mot de enskilda personer som den primärt är riktad mot. Den kan på sikt också hota vår legala, stabila och demokratiska samhällsordning och förtjänade därför, enligt regeringens mening, att betecknas som systemhotande. Det är av yttersta vikt att systemhotande brottslighet inte ges möjlighet att öka i omfattning. Det förutsätter att det också på detta område kan bedrivas ett effektivt brottsförebyggande arbete och att samhället har möjlighet att ingripa tidigt mot den som planerar brott av detta slag.[16]

[14] Prop. 2005/06:177 s. 38.
[15] Prop. 2005/06:177 s. 39 f.
[16] Prop. 2005/06:177 s. 40 f.

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.[17]

Preventivlagen har varit i kraft sedan år 2007. Utredningen om vissa hemliga tvångsmedel som bl.a. hade till uppgift att utvärdera lagen konstaterade i sitt betänkande år 2012 (SOU 2012:44) beträffande användningen av hemliga tvångsmedel i underrättelseverksamhet att lagen nästan uteslutande hade använts inom Säkerhetspolisens område. De situationer den användes i var när allvarliga brott av visst slag befarats och information för att komma vidare hade ansetts inte kunna erhållas på annat sätt men där tillräckligt med information inte fanns för att inleda förundersökning. Utredningen konstaterade också att det fanns goda grunder att anta att tvångsmedlet bidragit till att viss utpekad brottslighet hade förhindrats i en dryg tiondel av fallen. Utredningen bedömde att det fanns ett påtagligt behov för Säkerhetspolisen att även utom ramen för en förundersökning kunna använda vissa hemliga tvångsmedel för att förhindra brott.[18]

Trots att den öppna polisen inte använde hemliga tvångsmedel i underrättelseverksamhet enligt lagen konstaterade Utredningen om vissa hemliga tvångsmedel, i enlighet med vad regeringen anförde i ovan angiven proposition, att en del brott inom den organiserade brottsligheten är av särskild natur. Vid sådana brott, som i påverkanssyfte riktar sig mot befattningshavare inom rättssystemet, politiker eller företrädare för massmedia, kan slutenheten inom de grupperingar som utför brotten vara särskilt påtaglig. Sammantaget fann utredningen att behovet av att kunna använda hemliga tvångsmedel inom den öppna polisens verksamhet inte var lika starkt som inom Säkerhetspolisens verksamhet. Dock ansågs ett påtagligt behov

[17] Prop. 2005/06:177 s. 41
[18] SOU 2012:44 s. 37 f.

föreligga även för den öppna polisen att utom en förundersökning kunna använda vissa hemliga tvångsmedel för att förhindra systemhotande brott.[19]

Det bör också nämnas att regeringen, i samband med införandet av preventivlagen diskuterade frågan om husrannsakan i underrättelseverksamhet. Anledningen till att frågan togs upp var att de brottsbekämpande myndigheterna hade förklarat sig ha ett stort behov av att kunna göra en husrannsakan t.ex. i en bostad, på en arbetsplats eller i en annan lokal där det finns skäl att anta att det förvaras föremål som efter granskning eller undersökning kan ge kunskap om vilka slags brott som en viss organisation eller vissa personer har för avsikt att begå. Regeringen konstaterade först att ett sådant förslag innebar ett mycket långtgående intrång i den personliga integriteten och att det därför bör finnas ett mycket starkt behov av sådana tvångsåtgärder. Därefter gjorde regeringen bedömningen att det som förekommit i lagstiftningsärendet inte gav tillräckligt belägg för att det finns ett sådant påtagligt behov.[20] Regeringen uttalade dock också att det skulle beaktas att polisens uppgivna behov av att inhämta uppgifter som kan finnas i bostäder ofta torde avse uppgifter som finns lagrade i datorer, att förslag på det området var föremål för överväganden både nationellt och inom EU (bl.a. genom förslagen om hemlig dataavläsning i SOU 2005:38 och om husrannsakan i it-miljö på distans i Ds 2005:6) och att det därför var lämpligt att avvakta resultatet av dessa överväganden innan ytterligare bedömning skulle göras av polisens behov i brottsbekämpningen i det nu aktuella hänseendet.[21] De övervägandena föranledde emellertid inte lagstiftning på området.

Informationsbehovet

Säkerhetspolisen har i sin behovsbeskrivning anfört att det ligger i sakens natur att möjligheten att få lagrade uppgifter löpande i realtid många gånger kan vara helt avgörande för att identifiera brottsplaner, förhindra att brott fullbordas och avvärja överhängande fara. Det saknas skäl att ifrågasätta denna beskrivning. Det framstår

[19] SOU 2012:44 s. 38.
[20] Prop. 2005/06:177 s. 51 f.
[21] Prop. 2005/06:177 s. 52.

därför som närmast självklart att de lagrade uppgifterna som skulle kunna hämtas in genom hemlig dataavläsning skulle ha lika stort värde i den brottsförhindrande verksamheten som i den brottsutredande. De skäl som regeringen anförde i lagstiftningsarbetet med preventivlagen och som redovisats ovan beträffande vikten av att förhindra de brott som Säkerhetspolisen ansvarar för och för annan systemhotande brottslighet gör sig fortfarande gällande. Attentatet i Stockholm där en gärningsman med en lastbil körde ihjäl fem personer och skadade många på Drottninggatan den 7 april 2017 liksom bombdådet där en ensam gärningsman sprängde sig själv i närheten av Drottninggatan den 11 december 2010 visar tydligt hur svårförhindrad sådan brottslighet är. Det är av yttersta vikt att de brottsbekämpande myndigheterna ges rätt förutsättningar i underrättelseverksamheten för att förhindra liknande dåd. Att under vissa förhållanden kunna ta del av elektroniskt lagrade uppgifter kan förväntas vara ett hjälpmedel som kan bidra till detta.

Mot bakgrund av vad som nu redovisats är det vår bedömning att det föreligger tungt vägande informationsbehov såvitt avser elektroniskt lagrade uppgifter i underrättelseverksamheten. Det tungt vägande behovet föreligger enligt vår bedömning beträffande den brottslighet som i dag kan föranleda användning av hemliga tvångsmedel enligt preventivlagen och LSU.

Behovet av nya metoder

I behovsbeskrivningarna anges olika typer av omständigheter som föranlett att uppgifter som tidigare varit möjliga att få ut från teknisk utrustning i många fall inte längre kan samlas in. Eftersom informationen som de brottsbekämpande myndigheterna kan få ut av sådana uppgifter ofta är av stor betydelse i brottsutredningar innebär en minskad uppgiftsinsamling från teknisk utrustning inte sällan problem för utredningen.

En första omständighet är den ökade krypteringsgraden. Som anförts ovan beträffande kommunikation innebär kryptering stora bekymmer för de brottsbekämpande myndigheternas uppgiftsinsamling i samband med undersökningar av teknisk utrustning. I typfallet saknas nämligen möjligheter att ta sig runt krypteringen utan inloggningsuppgifter eller krypteringsnycklar.

Det har varit svårt att få klarhet i hur vanligt förekommande krypteringsproblematiken är och i vilken utsträckning den har ökat. Visst underlag finns dock, t.ex. i Brås rapport It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem vilken vi redogjort närmare för i avsnitt 7.2. Till att börja med kan konstateras att it-beslag ökat markant under senare år. Både för datorer och mobiltelefoner togs år 2014 omkring 60 procent fler sådana enheter i beslag än år 2008, vilket kan jämföras med ökningen för samtliga beslag under samma period som var åtta procent. Därtill kommer att it-inslagen i de polisanmälda brotten, dvs. exempelvis fall där digitala spår har lämnats som kan användas som bevisning vid brott, totalt sett har mer än fördubblats mellan åren 2006 och 2014. Enligt Brårapporten uppgår brott med sådana it-inslag nu till åtminstone 17 procent av den totala andelen brott, vilket enligt Brå sannolikt är en kraftig underskattning av den totala andelen brott med it-inslag (på grund av vissa svårmätbara omständigheter). Till detta ska läggas att Europol år 2016 redovisade att tjugotalet europeiska länder rapporterat problem med att it-brottslingar använder krypteringsprogram för att skydda lagrade uppgifter. Vidare rapporteras av Europol att sådan kryptering inte längre är begränsad till traditionella datorer utan att det sker en ökning av liknande lösningar för mobila enheter.[22]

Tullverket har i sin behovsbeskrivning anfört att andelen beslag av teknisk utrustning som är låst och krypterad i storstadsområdena är så hög som 50–80 procent av alla sådana beslag. Säkerhetspolisen och Åklagarmyndigheten har uppgett att problematiken förekommer i stort sett i varje fall av beslag av hårdvara som utgör teknisk utrustning som kan användas till kommunikation.

En annan omständighet som lyfts fram som problem vid undersökningar av teknisk utrustning är förekomsten av raderingsprogram. Sådan programvara kan, enligt vad som uppgetts för utredningen, 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 sker. Av instruktioner i s.k. antiforensik som florerar på diverse internetforum

[22] IOCTA 2016 s. 46.

rekommenderas den som vill skydda sig mot myndigheternas åtgärder att köra raderingsprogram på sin dator (eller annan tekniska utrustning) flera gånger per dag. Det innebär att de uppgifter som finns lagrade vid en tidpunkt kan vara försvunna, och inte möjliga att återskapa, bara sekunder senare. Av experter som arbetar vid Polismyndigheten med it-forensik har utredningen fått förklarat för sig att raderingsprogram i förening med tung kryptering innebär att tillslag mot it-skickliga kriminella (inom vilken kategori inte sällan personer som sysslar med t.ex. grov barnpornografibrottslighet och grova sexuella utnyttjanden av barn via internet hamnar) ofta måste planeras minutiöst och vara oerhört forcerade för att komma över en dator i påslaget och ”öppet” läge. Om något går fel vid ett sådant tillslag så att den misstänkte får tillfälle att radera eller låsa utrustningen, vilket enligt samma uppgiftslämnare t.ex. kan ske genom en enkel rörelse med muspekaren, så kan hela utredningen gå om intet. Motsvarande beskrivningar har lämnats av Åklagarmyndighetens och Säkerhetspolisens experter.

Vidare har det framkommit att inte bara särskilda raderingsprogram utan också inbyggda funktioner i modern teknisk utrustning utgör problem för de brottsbekämpande myndigheternas it-forensiker i arbetet med att återskapa uppgifter. Ett exempel är de s.k. SSD-diskarna (solid state drive), vilka tillsammans med funktionen ”trim” tar bort raderad information automatiskt. När användaren raderar uppgifter markeras utrymmet på SSD-disken som ledigt. Det som då sker automatiskt i bakgrunden är att markerade data plockas bort med hjälp av trim och att utrymmet på SSD-disken därmed kan användas på nytt. När ny information tillförs på det utrymme där raderade data har plockats bort kan de borttagna uppgifterna i dag inte återskapas av it-forensiker. Detta skiljer sig från vad som gäller för en traditionell hårddisk där raderade uppgifter inte sällan är möjliga att återskapa, förutsatt att ett raderingsverktyg inte har använts. I takt med att ny teknik, som exempelvis den beskrivna SSD-tekniken, blir allt mer utbredd försvåras (och t.o.m. förhindras) således möjligheten till återskapande av raderade uppgifter för de brottsbekämpande myndigheterna.

Även beträffande raderingsprogram och de förbättrade raderingsfunktionerna har det varit svårt att få klara uppgifter om hur vanligt förekommande detta är. Helt klart är dock att problematiken förekommer. Enligt uppgifter som Tullverkets expert samlat in från it-

forensiker har det inom ett av verkets totalt fyra kompetenscenter för brottsbekämpande verksamhet, noterats ett totalt bortfall (dvs. att samtliga uppgifter i ett it-beslag är borta i samband med undersökningen av beslaget) i omkring fem–sex procent av it-beslagen.[23] Åklagarmyndighetens experter har anfört att en erfaren it-forensiker vid Region syd uppskattar företeelsen som ökande i ärenden om grov brottslighet och har erfarit det främst i ärenden med väl teknikmedvetna misstänkta som är måna om att dölja sina förehavanden. Enligt denna uppskattning förekommer problematiken i uppemot vart åttonde ärende.

Ett belysande exempel på de olika omständigheter som nu anförts finns i ett av de typfall som Polismyndighetens experter redovisat i sin behovsbeskrivning. Exemplet rör utredningar om grovt barnpornografibrott och återges här i sin helhet.

> De personer som ägnar sig åt att samla på bilder av barnpornografisk karaktär vill skydda sin samling. Det sker genom att lägga bilderna och filmerna på hårddiskar och på avgränsade ytor som sedan krypteras. Lösenorden är oftast komplicerade och personerna lämnar inte ut dessa. Vissa krypteringsprogram lagrar inte lösenord över huvud taget, utan dessa måste samlas in när de skrivs in av användaren i realtid. I samtliga ärenden på senare tid hos Nationellt it-brottscentrum har det förekommit installerade raderingsprogram på datorn. Ett raderingsprogram suddar ut alla spår av hanteringen av bild- och filmfiler. Det raderar både sökvägar och namn på filer på de lokala lagringsenheterna. Även filernas väg in till datorn raderas. Det går följaktligen inte att se hur eller varifrån filerna har laddats ner till datorn. Det har även förekommit fall där den misstänkte har installerat om hela datorn en gång per månad för att radera alla spår.

Till de anförda omständigheterna kommer att uppgifterna i ökande grad lagras på annan plats än i den tekniska utrustningen. Som framhållits i avsnitt 6.2.6 uppgav redan 2014 nästan en tredjedel av personerna som ingick i Statistiska centralbyråns undersökning att de då hade använt lagringsutrymme på internet. Bland 25–34-åringarna var andelen 55 procent. Uppgifter som lagras i det s.k. molnet, dvs. på annan plats än i den enskildes tekniska utrustning, innebär i dag att uppgifterna inte kan samlas in i samband med undersökningar av teknisk utrustning. De brottsbekämpande myndigheterna har nämligen i dag inte rätt att utan särskilt tillstånd (t.ex. husrannsakans-

[23] Det bör framhållas att utredningen saknar uppgifter från övriga tre kompetenscenter.

beslut riktat mot den plats där uppgifterna lagras) ta del av uppgifter som lagras utanför den tekniska utrustningen.

Liksom beträffande kryptering har molnlagringstjänster ett i allra högsta grad legitimt användningsområde. De besparar den absoluta majoriteten personer utrymme i teknisk utrustning och erbjuder därtill möjlighet att skydda t.ex. fotografier om den tekniska utrustningen de annars skulle lagras på går sönder. Emellertid framgår av behovsbeskrivningarna att också kriminella använder molnlagring i sin kriminalitet. Säkerhetspolisen ger i de typfall man redovisat i sin behovsbeskrivning (se typfall 18 och 22 i avsnitt 8.3.6 och i bilaga 2) exempel på hur kriminella delar uppgifter med varandra i en molntjänst.

De nu anförda omständigheterna talar enligt utredningens mening med styrka för att åtgärder bör vidtas för att ge de brottsbekämpande myndigheterna inte bara rättslig utan också faktisk tillgång till uppgifter som finns elektroniskt lagrade. Vår bedömning är att främst 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. Sammantaget leder detta till bedömningen att det finns tungt vägande behov för de brottsbekämpande myndigheterna av en metod som i hemlighet, löpande och i realtid, kan samla in elektroniskt lagrade uppgifter.

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 hur teknisk utrustning i olika avseenden används. Det är svårt att upprätthålla en klar gräns mot uppgifter som lagras eftersom det kan skilja sig åt från utrustning till utrustning och program till program vad som lagras respektive inte lagras. Exempel på uppgifter som avses kan dock vara författande i ett elektroniskt dokument som inte sparas av användaren och angivande av vissa inloggningsuppgifter. I somliga fall förekommer att dessa uppgifter lagras till-

fälligt 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.

Metoden för hemlig dataavläsning skulle kunna användas för att hemligt i realtid ta del av vad som sker på den tekniska utrustning som åtgärden avser och således kunna fånga upp både uppgifter som lagras och som inte lagras.

Eftersom det synes slumpmässigt vilka uppgifter som lagras, jfr t.ex. det nyss citerade exemplet från Polismyndighetens experter, ligger det nära till hands att bedöma uppgifter som inte kan återfinnas i efterhand på samma vis som vi nyss bedömt sådana som lagras. Säkerhetspolisen har i sin behovsbeskrivning 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 att identifiera brottsplaner, förhindra att brott fullbordas, avvärja överhängande fara, verkställa tvångsmedel och säkra bevis. Det som enligt Säkerhetspolisen bl.a. kan vara av mycket stort värde är realtidsuppgifter om att utrustningen faktiskt används, om att tangentbord används, om innehållet i dokument eller meddelanden som skrivs (men inte sparas eller skickas), om inloggningsuppgifter, om att lagring sker på extern media t.ex. USB-minne, om att filer öppnas och om att program startas.

De uppgifter som varken kommuniceras eller lagras kan enligt Säkerhetspolisens behovsbeskrivning behövas före, under och efter verkställighet av tvångsmedel, som gripande, husrannsakan och beslag. De kan ge information om att en person finns på en viss plats vid en viss tidpunkt, om inloggningsuppgifter och 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 redigerar kontaktlistor eller bilder, samt för att se om någon förändrar en säkerhetslogg eller öppnar ett dokument eller ett program vid givet tillfälle. Att öppna program kan innebära att personen sätter utrustningen i ”flygläge” och förbereder meddelanden för att senare snabbt kunna kommunicera.

Säkerhetspolisens uppgifter i denna del visar enligt vår uppfattning att behovet är lika starkt av att ta del av uppgifter som inte

lagras som det behov som ovan konstaterats beträffande elektroniskt lagrade uppgifter.

9.2.5 Är behovet olika stort för olika brott?

Vi har i det föregående konstaterat att det föreligger tungt vägande behov av nya metoder både som ett sätt att komma åt uppgifter som befintliga hemliga tvångsmedel kan ge rättslig men inte faktisk tillgång till och för att i hemlighet, löpande och i realtid, kunna ta del av uppgifter som finns tillgängliga i teknisk utrustning. När det gäller behovet för olika brott kan först konstateras att direktiven är tydliga avseende när hemlig dataavläsning kan komma i fråga, nämligen för de brott som i dag kan föranleda hemlig avlyssning av elektronisk kommunikation. Vi har därför inte låtit andra brott än dessa vara föremål för vår analys. För en redogörelse av vilken typ av brott det rör sig om hänvisas här till avsnitt 3.4.1.

Det kan hävdas att viss brottslighet – t.ex. terrorist- eller narkotikabrottslighet – i allmänhet torde fordra mer kommunikation än annan allvarlig brottslighet, t.ex. en synnerligen grov misshandel utan föregående planering. Utifrån sådana omständigheter kan rimligen behovet av åtgärder för att komma åt krypterad information i meddelanden anses vara 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 ta del av den misstänktes kommunikation eller annan information för att exempelvis knyta denne till brottet. Vikten av att kunna följa sådana spår i kölvattnet av ett begånget brott kan inte anses mindre därför att det kan förväntas finnas färre uppgifter att hämta in. Av denna anledning har vi inte funnit att behovet, avseende något av de konstaterade behovsområdena, i något avgörande avseende kan anses mindre för vissa brottskategorier än andra. När det gäller brottsförhindrande verksamhet gör sig samma resonemang gällande som det nyss redovisade. Vår slutsats är därför att behovet är tungt vägande för samtliga de brott som kan föranleda hemlig avlyssning av elektronisk kommunikation.

9.3 Effektivitet

Utredningens bedömning: Hemlig dataavläsning kan användas som metod för att komma åt sådana uppgifter som de brottsbekämpande myndigheterna har tungt vägande behov av. Åtgärden kommer dock kunna genomföras i färre ärenden än där det finns behov av den. När hemlig dataavläsning kan genomföras förväntas åtgärden leda till betydligt bättre information än vad dagens metoder ger tillgång till. Metoden kommer att medföra kostnadsökningar. Den bör därför i första hand användas i kampen mot den allra allvarligaste brottsligheten där det saknas reella alternativ. I de fallen förväntas hemlig dataavläsning vara en effektiv åtgärd.

9.3.1 Utgångspunkter

En paradox med effektivitetsanalyser av nya åtgärder på tvångsmedelsområdet är att flera faktorer som kan antas påverka effektiviteten inte blir kända förrän en åtgärd har införts och prövats i skarpt läge samtidigt som ju åtgärden inte ska införas om den inte kan anses tillräckligt effektiv.[24] Denna paradox och svårigheter att bedöma hur värdefulla uppgifter som kan samlas in med en ny metod utgör osäkerhetsmoment i vår effektivitetsanalys. Därtill finns det en rad omständigheter som kan förutses och som kan förväntas påverka effektiviteten av hemlig dataavläsning men där det är svårt att uttala sig om i vilken grad så kommer att ske, exempelvis att den tänkta tekniken fungerar i skarpt läge. Icke desto mindre ska enligt direktiven en effektivitetsanalys göras.

En utgångspunkt för analysen bör vara att resultatet av den inte bör och knappast kan värderas i siffror eller andelstal. I betänkandet *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44) gjorde Utredningen om vissa hemliga tvångsmedel en omfattande kartläggning av bland annat nyttan med vissa dittillsvarande tidsbegränsade tvångsmedelslagar. En av de slutsatser som utredningen ansåg sig kunna dra av kartläggningen, vilken vi inte funnit skäl att ifrågasätta, var att nytta och effektivitet på grund av frågornas komplexitet i all-

[24] Se t.ex. Annika Brickman, *Vad får man tåla?*, SvJT 2007 s. 179.

mänhet inte lämpar sig särskilt bra för att mätas i siffror och andelstal relaterade till vissa följder. En på förhand bestämd procentandel av samtliga fall där hemliga tvångsmedel ska leda till ett visst resultat var enligt den utredningen inte lämpligt att slå fast, bland annat på grund av att det vid jämförelser med andra hemliga tvångsmedel är svårt att helt undvika förenklade andelsresonemang. Sådana resonemang kan enligt Utredningen om vissa hemliga tvångsmedel endast tillåtas utgöra en utgångspunkt för en fortsatt och mer resonerande analys.[25]

En annan utgångspunkt för vår effektivitetsanalys är att den bör vara så bred som möjligt. Inte så sällan talas i anslutning till behovet av hemliga tvångsmedel om effektivitet. Det finns emellertid inget entydigt svar på vad som avses med effektivitet i detta sammanhang. Tvärtom synes effektivitetsbegreppet skapa viss förvirring i den juridiska diskussionen.[26] Också i våra direktiv används effektivitetsbegreppet i delvis olika betydelser. Klart är emellertid att vi ska utreda i vilken utsträckning hemlig dataavläsning kan förväntas vara en effektiv metod för brottsbekämpning i förhållande till behovet. Svaret på den frågan är enligt direktiven i stor utsträckning beroende av hur metoden tekniskt kan utformas. Vår undersökning ska enligt direktiven utgå från de tekniska möjligheter som finns och beakta de svårigheter vid verkställighet som kan förutses. Frågor som är av betydelse för effektiviteten och som enligt direktiven bör belysas är hur bearbetning av information som inhämtas genom metoden kan förväntas gå till, hur myndigheterna ska skaffa den tekniska förmåga som krävs för att använda metoden, risken för att kriminella anpassar sitt beteende för att komma runt nya övervakningsverktyg och vilka resurser metoden förutsätter.

Mot bakgrund av det anförda använder vi i effektivitetsanalysen begreppet effektivitet i vid mening. Vi bedömer inledningsvis effektiviteten i såväl kvantitativ som kvalitativ mening och diskuterar sedan andra effektivitetspåverkande faktorer.

Det bör framållas att de uppgifter som redovisas i det följande huvudsakligen baseras på uppgifter som utredningen mottagit från

[25] SOU 2012:44 s. 481.

[26] Se t.ex. Magnus Ulvängs artikel *Brottsbekämpning, rättssäkerhet och integritet – vad är det som har hänt och vad skall vi göra?*, SvJT 2007 s. 8. Det kan nämnas att effektivitetsbedömningen i SOU 2012:44 utgjorde en del av behovsanalysen. Vi har, främst mot bakgrund av direktivens utformning, funnit skäl att dela upp frågorna om behov och effektivitet.

experter vid brottsbekämpande myndigheter i Sverige. Vid de studiebesök utredningen gjort och övriga kontakter som förevarit med brottsbekämpande myndigheter i länder som tillämpar hemlig dataavläsning eller en motsvarighet till åtgärden har efterfrågats kvantitativ information om åtgärdens effektivitet och nytta, t.ex. avseende hur ofta metoden används och vilken nytta den medför. Det har emellertid, till följd av sekretess, inte varit möjligt att i något fall få detaljerade uppgifter på detta område, se vidare avsnitt 5.6.

Avslutningsvis ska också sägas att en utgångspunkt för våra bedömningar av effektiviteten är att teknik för hemlig dataavläsning kan användas för att komma åt alla de olika typer av uppgifter som vi i föregående avsnitt konstaterat att det finns behov av i den brottsbekämpande verksamheten.

9.3.2 Kvantitativ effektivitet

Innehåll i och uppgifter om meddelanden som överförs eller överförts i elektroniskt kommunikationsnät

Enligt uppgifter som utredningen har fått från experter vid de brottsbekämpande myndigheterna som utrett de tekniska förutsättningarna för verkställighet av hemlig dataavläsning kommer åtgärden vara möjlig att använda i ett begränsat antal fall. I antalet verkställigheter räknat skulle åtgärden, åtminstone till en början, enligt dessa uppgiftslämnare vara mer jämförbar med hemlig rumsavlyssning än med hemlig avlyssning eller övervakning av elektronisk kommunikation. Det beror på olika faktorer, t.ex. omfattande förberedelsearbete och tekniska svårigheter vid verkställighet.

Det kan konstateras att det meddelades tillstånd till hemlig rumsavlyssning mot 51 personer år 2015 och mot 55 personer år 2016 medan antalen som det riktades hemlig avlyssning av elektronisk kommunikation mot var 1 158 personer år 2015 och 1 253 personer år 2016.[27] Av behovsanalysen framgår att det finns behov av att komma åt uppgifter som man i dag inte kan hämta in i klartext på grund av kryptering och anonymisering i de flesta fall där hemlig avlyssning eller övervakning av elektronisk kommunikation genom-

[27] Anförda antal avser Ekobrottsmyndighetens, Polismyndighetens och Tullverkets verksamheter och är hämtade från Åklagarmyndighetens rapport den 31 maj 2017, dnr ÅM 2016-308.

förs. Hemlig dataavläsning framstår mot bakgrund av det anförda i kvantitativ mening framstår som en begränsat effektiv åtgärd i förhållande till föreliggande behov.

Det bör dock framhållas att Säkerhetspolisens tvångsmedelsärenden inte ingår i den statistik som redovisats ovan. Den myndighetens tvångsmedelsanvändning redovisas sammantagen, dvs. för samtliga hemliga tvångsmedel. År 2016 meddelades 307 beslut om hemliga tvångsmedel avseende Säkerhetspolisens verksamhet. Det kan därför sägas att hemlig dataavläsning torde vara mer kvantitativt effektiv i den verksamheten än i övriga brottsbekämpande myndigheters verksamhet.

Hemlig dataavläsning för lokaliseringsuppgifter

Det är svårt att fastställa precis hur stort behovet av att samla in lokaliseringsuppgifter med hemlig dataavläsning, t.ex. genom att aktivera GPS-utrustningen på en mobiltelefon, är. Det är självklart så att när en brottsbekämpande myndighet behöver lokaliseringsuppgifter i en utredning så är det från effektivitetssynpunkt bra om uppgifterna är så exakta som möjligt. Samtidigt torde befintlig teknik för inhämtning av lokaliseringsuppgifter många gånger ge tillräckligt bra uppgifter, se t.ex. de redovisade exemplen beträffande hemlig övervakning av elektronisk kommunikation i Åklagamyndighetens rapport *Redovisning av användningen av vissa hemliga tvångsmedel under 2016* (ÅM 2016-308). Det finns heller inte särredovisat hur ofta tillstånd till hemlig övervakning av elektronisk kommunikation (och inhämtning enligt inhämtningslagen) innebär rätt att hämta ut lokaliseringsuppgifter.

Mot den angivna bakgrunden är det svårt att bedöma hur effektiv hemlig dataavläsning kan vara i förhållande till behovet i kvantitativ mening. Det kan emellertid konstateras att det meddelades tillstånd till hemlig övervakning av elektronisk kommunikation mot 2 104 personer år 2015 och mot 2 290 personer år 2016.[28] Det kan förutsättas att det hade varit till fördel för utredningarna i många fall om mer exakta lokaliseringsuppgifter hade kunnat hämtas in. Mot bakgrund av vad som ovan anförts om antalet verkställighetstillfällen då

[28] Se ÅM2016-308 s. 11.

hemlig dataavläsning kan användas framstår åtgärden även beträffande lokaliseringsuppgifter som en i kvantitativ mening begränsat effektiv åtgärd i förhållande till föreliggande behov.

Hemlig dataavläsning för optisk personövervakning och avlyssning av ljud

När det gäller hemlig kameraövervakning och hemlig rumsavlyssning är det betydligt färre personer som blir föremål för dessa åtgärder än antalet personer som blir föremål för hemlig avlyssning och övervakning av elektronisk kommunikation. År 2015 var antalet kameraövervakade personer 122 och år 2016 var antalet 117.[29] Motsvarande antal för hemlig rumsavlyssning var 51 personer år 2015 och 55 personer år 2016.[30]

Som framhållits i behovsbeskrivningarna och i avsnitt 9.2.3 är inte skälet till att nya metoder behövs för att kunna verkställa de nu nämnda åtgärderna att tekniken har förändrats, såsom är fallet för hemlig avlyssning och övervakning av elektronisk kommunikation. I stället är det främst praktiska svårigheter i enskilda fall, t.ex. att den brottsbekämpande 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 som föranlett behovet. Det torde innebära att det endast är i vissa fall som det finns ett behov att använda teknik för hemlig dataavläsning för att samla in kameraövervaknings- eller rumsavlyssningsuppgifter. Eftersom antalet personer som utsätts för hemlig kameraövervakning och hemlig rumsavlyssning är få, i förhållande till vad som gäller för andra tvångsmedel, och eftersom teknik för hemlig dataavläsning endast torde aktualiseras i vissa av dessa fall framstår hemlig dataavläsning i nu aktuellt avseende, i kvantitativ mening i förhållande till behovet, som en tämligen effektiv åtgärd.

[29] Se ÅM2016-308 s. 17.
[30] Se ÅM2016-308 s. 23.

Hemlig dataavläsning för att samla in elektroniskt lagrade uppgifter och uppgifter som visar hur viss teknisk utrustning används

När det gäller behovet av att samla in elektroniskt lagrade uppgifter med hemlig dataavläsning är det svårt att kvantifiera behovet. Den statistik som redovisats i avsnitt 9.2.4 vittnar emellertid om att det förefaller vara tämligen ofta som elektronisk utrustning tas i beslag som uppgifter i utrustningen inte är möjliga att samla in. Mot bakgrund av hur många beslag av sådan utrustning som görs torde antalet tillfällen då det föreligger behov av att komma åt lagrade uppgifter vida överstiga det antal verkställighetstillfällen som hemlig dataavläsning kommer att kunna genomföras vid. I kvantitativ mening framstår hemlig dataavläsning i nu aktuellt avseende som en begränsat effektiv åtgärd.

Såvitt avser behovet av att samla in uppgifter som visar hur viss teknisk utrustning används är det än svårare att kvantifiera behovet. Vad det handlar om är uppgifter som varken lagras eller kommuniceras, dvs. uppgifter som inte kan samlas in med andra tvångsmedel. Även om behovet av att samla in sådana uppgifter, i kvantitativ mening, torde vara väsentligt lägre än avseende behovet av att samla in elektroniskt lagrade uppgifter så synes det vara större än det uppskattade antalet verkställighetstillfällen avseende hemlig dataavläsning. I kvantitativ mening framstår hemlig dataavläsning även i detta avseende som en begränsat effektiv åtgärd.

9.3.3 Kvalitativ effektivitet

I detta avsnitt diskuteras i vad mån hemlig dataavläsning kan förväntas vara en kvalitativt effektiv metod, med vilket vi avser att åtgärden när den används i ett enskilt fall kan förväntas ge de uppgifter den används för att hämta in. En utgångspunkt för oss har varit att teknik för hemlig dataavläsning kan användas för att komma åt alla de olika typer av uppgifter som vi konstaterat att det finns behov av i den brottsbekämpande verksamheten. Det finns emellertid faktorer i de enskilda fallen som kan påverka den kvalitativa effektiviteten. Främst är sådana faktorer hänförliga till vilken teknik som finns tillgänglig just när åtgärden aktualiseras. I detta avsnitt görs därför inte motsvarande indelning som i föregående avsnitt

beträffande de olika uppgiftstyperna som det finns behov av att kunna samla in. I stället diskuteras effektiviteten utifrån olika tekniker.

När hemlig dataavläsning ska genomföras utan att den brottsbekämpande myndigheten har fysisk tillgång till den tekniska utrustningen åtgärden ska avse handlar det främst om att utnyttja sårbarheter för att komma åt uppgifterna, se avsnitt 8.4.1. Sådana sårbarheter kan vara av olika slag och därför i förlängningen ge tillgång till olika ”delar” av viss teknisk utrustning. För att ge ett exempel kan det handla om att en app i en mobiltelefon har en för den brottsbekämpande myndigheten känd säkerhetsbrist. På grund av säkerhetsbristen kan det vara möjligt att genom appen, på distans ta sig in i och skicka programvara till en viss teknisk utrustning (dvs. utrustning tillhörig den som ska bli föremål för hemlig dataavläsning). Beroende på förutsättningarna i det enskilda fallet kan det dock finnas begränsningar i vad som är möjligt att åstadkomma utifrån att just den angivna sårbarheten används som ”väg in” i utrustningen. Också andra tekniska faktorer, exempelvis hur säkerheten (brandväggar, virusprogram etc.) är beskaffad kan påverka vad som är möjligt att åstadkomma. Ibland kan det därför vara praktiskt möjligt att ta del av alla eller väldigt många uppgifter som finns i utrustningen medan det i andra situationer inte kommer att vara möjligt att ta del av mer uppgifter än de som finns tillgängliga i en viss app (eller kanske endast vissa uppgifter som finns där). Om många uppgifter kan hämtas in torde förutsättningarna att samla in den eftersökta informationen typiskt sett öka medan det omvända typiskt sätt torde gälla när få uppgifter kan hämtas in. Samtidigt kan det i ett enskilt fall vara så att mycket värdefull information kan erhållas även om endast få uppgifter kan samlas in medan lite information av intresse kan mottas när en stor mängd uppgifter kan kommas över. Det nu anförda får tjäna som exempel för att illustrera vilken bredd av möjligheter och svårigheter som föreligger på det tekniska planet och, kanske framför allt, också vilka svårigheter som finns med att uttala sig om åtgärdens kvalitativa effektivitet på ett generellt plan.

Till effektivitetsanalysen måste dock läggas att företag som utvecklar hårdvara, programvara eller appar kontinuerligt arbetar för att upptäcka och täppa igen sådana säkerhetsbrister som kan utnyttjas för att komma in i teknisk utrustning. De företag som utvecklar säkerhetssystem (exempelvis virusprogram eller brandväggar) för t.ex. datorer och telefoner arbetar därtill löpande med att

upptäcka sådan programvara som kan behöva användas av brottsbekämpande myndigheter vid verkställighet av hemlig dataavläsning. Det innebär att även om det vid en given tidpunkt finns både en väg in i teknisk utrustning och programvara utvecklad som kan förse de brottsbekämpande myndigheterna med uppgifter så kan möjligheten till hemlig dataavläsning komma att förändras eller upphöra genom t.ex. en uppdatering som täpper igen säkerhetshålet (s.k. patch) eller att ett virusprogram upptäcker den programvara som installerats.

När hårdvara används vid verkställighet torde det främst vara fråga om s.k. keyloggers, en sorts utrustning som registrerar tangentnedslag på tangentbord.[31] Sådan utrustning torde primärt vara möjlig att använda riktad mot traditionella datorer. De uppgifter som kan hämtas in med denna teknik är därmed begränsad till vilka tangenter som trycks ned. Tekniken kan exempelvis ge uppgifter om vad som skrivs i kommunikation men torde främst vara användbar för att komma över inloggningsuppgifter (som t.ex. skulle kunna användas vid ett senare beslag eller vid verkställighet av hemlig dataavläsning med annan teknisk metod). Det finns program som är utvecklade för att upptäcka dylika hårdvaror och dessutom kan det finnas risk för att den som utsätts för åtgärden upptäcker utrustningen fysiskt just eftersom det är fråga om hårdvara. Om den som åtgärden avser upptäcker utrustningen kan det innebära att inhämtningen går om intet, även om installation och inhämtning fram till upptäckandet varit lyckosam.

Vad sedan avser användande av inloggningsuppgifter i genomförandet av hemlig dataavläsning kan konstateras att de uppgifter som den brottsbekämpande myndigheten därigenom skulle kunna få del av är begränsad till den tjänst eller det konto som inloggning sker på. Det innebär att en mindre mängd uppgifter än vad som är fallet vid exempelvis lyckad användning av programvara som installerats i teknisk utrustning kan hämtas in. Dock förekommer det vid inloggning på användarkonton till många tjänster via annan utrustning än den som vanligtvis används att kontoinnehavaren får ett meddelande om inloggningen. När så sker finns risk för att framtida meddelanden (eller lagrade uppgifter) inte kan hämtas in, såväl på grund av att

[31] Det bör nämnas att keyloggers också finns som mjukvara och därmed kan tänkas användas även med andra tekniker för verkställighet av hemlig dataavläsning.

inloggningsuppgifterna ändras som att den som åtgärden avser slutar att använda kontot.

Det synes mot bakgrund av det anförda finnas faktorer som kan påverka den kvalitativa effektiviteten av hemlig dataavläsning oavsett vilken teknik för att verkställa åtgärden som används. Eftersom hemlig dataavläsning emellertid, i vart fall inledningsvis, endast kommer att kunna användas vid ett begränsat antal tillfällen, se avsnitt 9.3.2, kan det förutsättas att den brottsbekämpande myndigheten 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. Det är därför vår bedömning att åtgärden, när den kan användas, kommer att vara mycket verkningsfull och att de svårigheter som redovisats ovan bör vara beaktade innan verkställighet sker. I kvalitativ mening, såvitt avser hur mycket av de eftersökta uppgifterna som kan hämtas in genom hemlig dataavläsning när åtgärden används, kan därför effektiviteten förväntas bli hög.

Frågan är också vilka nyttoeffekter som kan förväntas av att det blir möjligt att samla in de eftersökta uppgifterna. Det säger sig självt att det här blir fråga om rena uppskattningar, huvudsakligen baserade på uppgifter från utredningens experter vid de brottsbekämpande myndigheterna. Det bör dock nämnas att Utredningen om vissa hemliga tvångsmedel gjorde jämförelser mellan vilken information representanter för brottsbekämpande myndigheter hoppades erhålla när de ansökt om ett visst tvångsmedel och vilken information som faktiskt erhölls. Slutsatsen av jämförelsen var att informationen som erhölls – med undantag för vid hemlig rumsavlyssning – i stort sett motsvarade den förväntade. Att utfallet vid hemlig rumsavlyssning var något sämre än förväntat berodde främst på att tekniken inte alltid fungerade som planerat. Mängden och användbarheten av de uppgifter som samlades in i de olika ärendena var varierande. Utredningen konstaterade att det i ett inte obetydligt antal fall var fråga om konkreta uppgifter om exempelvis brottsplaner. Ofta handlade det dock om mer allmänna uppgifter, såsom personers kontaktnät eller vilja och förmåga att utföra en viss typ av brott, som bedömdes relevanta för utredningen.[32] Vi anser oss av det anförda kunna dra slutsatsen att de brottsbekämpande myndigheternas uppfattning av

[32] SOU 2012:44 s. 496

vad man kan förvänta sig av hemlig dataavläsning måste tillåtas väga tungt.

En genomgående synpunkt i alla behovsbeskrivningar är att hemlig dataavläsning skulle kunna avhjälpa de problem som föreligger på de områden där behov finns. En lyckad verkställighet av hemlig dataavläsning kan innebära att den brottsbekämpande myndigheten kan ta del av de eftersökta uppgifterna i klartext. Redan i dag uppstår, trots de problem som föreligger vid verkställighet, nytta vid användning av de hemliga tvångsmedlen.[33] Det finns ingenting som talar för att nyttoeffekterna av de uppgifter som kan hämtas in genom hemlig dataavläsning skulle vara mindre än de nyttoeffekter som uppstår vid användningen av dagens hemliga tvångsmedel. Det som representanter för de brottsbekämpande myndigheterna anfört talar i stället i väsentlig mån för att uppgifterna som kan hämtas in med hemlig dataavläsning skulle ge både fler och bättre, mer kvalitativa, nyttoeffekter. Det finns därför skäl att utgå från att hemlig dataavläsning skulle innebära större nytta i de brottsbekämpande myndigheternas ärenden än vad dagens hemliga tvångsmedel medför. I kvalitativ mening får mot bakgrund av det anförda hemlig dataavläsning anses vara en effektiv åtgärd.

9.3.4 Effektivitet i relation till resursåtgång

Vad sedan gäller vilka resurser som kommer krävas för att hemlig dataavläsning ska kunna bli verklighet kan först konstateras att resursåtgången vid verkställighet, eller kanske snarare inför verkställighet, i många fall kommer att vara att jämföra med den resursåtgång som kartläggning och andra förberedelser som hemlig rumsavlyssning kräver. Kartläggningar av den misstänkte och dennes tekniska utrustning behöver typiskt sett ske innan verkställighet kan ske för att åtgärden ska vara kvalitativt effektiv när den används, se föregående avsnitt. Det innebär att åtgärden kommer att kräva en hel del personalresurser från den brottsbekämpande myndigheten vars ärende det är fråga om.

Det sagda har handlat om åtgärder *inför* verkställighet i ett enskilt ärende. Något ska också sägas om arbetet *under* verkställighet.

[33] Se t.ex. regeringens skrivelse 2016/17 s. 33 f.

Ingenting av det som framkommit talar för att arbetet med själva insamlingen av uppgifter från hemlig dataavläsning kommer att kräva varken mer eller mindre arbetsinsatser från de brottsbekämpande myndigheterna än vad som krävs vid verkställighet av befintliga hemliga tvångsmedel.

Däremot föreligger stor sannolikhet för att det i lyckade verkställighetsärenden, dvs. då de eftersökta uppgifterna kan samlas in, kommer att finnas mer uppgifter att ta om hand och analysera än vad som är fallet med befintliga hemliga tvångsmedel. Det anförda gäller särskilt när hemlig dataavläsning ska användas för att samla in uppgifter som får samlas in efter tillstånd till hemlig avlyssning av elektronisk kommunikation, där ju mycket av uppgifterna som samlas in i dag är krypterade, och för att samla in elektroniskt lagrade uppgifter, vilket inte är möjligt med något av de hemliga tvångsmedel som är tillåtna i dag. Det innebär att arbetet för de arbetsgrupper som ska analysera de inhämtade uppgifterna blir mer omfattande än vad som krävs i dag. En ökad uppgiftsmängd att bearbeta och analysera ställer också högre krav på ändamålsenliga verktyg och arbetsmetoder för analysen.

Det finns ytterligare en aspekt som bör beaktas avseende resursåtgång, nämligen kostnaderna för utveckling och implementering av den teknik som behövs för hemlig dataavläsning. I det sammanhanget kan konstateras att oavsett om de brottsbekämpande myndigheterna själva ska utveckla tekniken eller om de ska köpa in den kommer kostnaderna bli betydande, se kapitel 12.

Om hemlig dataavläsning är ett effektivt tvångsmedel utifrån de resurser åtgärden kräver är primärt en fråga om politiska prioriteringar. När hemlig rumsavlyssning skulle införas anförde regeringen bl.a. följande.

> Hemlig rumsavlyssning är otvivelaktigt ett mycket resurskrävande tvångsmedel som kräver omfattande förberedande spaningsinsatser. Men detta är enligt vår mening inte 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.[34]

[34] Prop. 2005/06:178 s. 41.

Motsvarande resonemang som regeringen redovisade gör sig enligt utredningens mening gällande också för hemlig dataavläsning. Hemlig dataavläsning är, enligt vad representanter för brottsbekämpande myndigheter framhållit, många gånger enda möjligheten för de brottsbekämpande myndigheterna att få tillgång till den kritiska informationen. Det kan dessutom enligt tekniska experter förutsättas att de tekniska metoderna för hemlig dataavläsning kommer att både effektiviseras och förfinas med tiden vilket talar för att metoden kan användas oftare, med såväl bättre utfall som minskad resursåtgång som följd. Icke desto mindre kommer hemlig dataavläsning vara en metod som medför kostnadsökningar för de brottsbekämpande myndigheterna, i synnerhet relaterade till anskaffning och underhåll av verkställighetsteknik.

Mot bakgrund av kostnadsökningarna som kan förväntas och av att hemlig dataavläsning endast, åtminstone till en början, kommer att aktualiseras i ett begränsat antal ärenden per år kan åtgärden framstå som en ineffektiv arbetsmetod. Vi anser emellertid inte att så behöver vara fallet. Åtgärden bör dock, även om den kan förväntas vara verkningsfull i arbetet mot flera olika typer av brottslighet, för att anses effektiv i första hand riktas mot den allra allvarligaste och mest svårutredda eller svårförhindrade brottsligheten. Av behovsbeskrivningarna framstår det som uppenbart att den typ av brottslighet som Säkerhetspolisen ansvarar för att förebygga, förhindra och upptäcka (brott mot rikets säkerhet och terrorbrott) och brottslighet i organiserat kriminella miljöer utgör sådan brottslighet som hemlig dataavläsning i första hand bör användas mot.

Det finns hos såväl Säkerhetspolisen som hos övriga brottsbekämpande myndigheter en god kännedom om organisationsstrukturer och om personerna inom kriminella organisationer som är av intresse i de brottsbekämpande myndigheternas olika verksamhetsområden. Denna kännedom innebär emellertid inte att personerna i ”toppen” av kriminella nätverk kan lagföras särskilt ofta (eller, i Säkerhetspolisens fall, att önskvärd kontroll av kända riskpersoner kan uppnås i alla skeden). Desto oftare är det i stället personer längre ned i hierarkin som kan lagföras. Det beror på att personerna i toppen av strukturerna, liksom flertalet av de individer Säkerhetspolisen har i uppdrag att ha kontroll över, inte sällan är skickliga på att på olika sätt gå under de brottsbekämpande myndigheternas radar. Deras kommunikationer är t.ex., enligt representanter för de

brottsbekämpande myndigheterna, så gott som alltid krypterade och således inte avlyssningsbara. Samtidigt är det en förutsättning för såväl den organiserade brottsligheten som för många av Säkerhetspolisens målpersoner att ha fungerande kommunikationer.

Mot bakgrund av att de brottsbekämpande myndigheterna redan i dag har kännedom om vilka dessa personer är och av intresset att komma åt dem framstår det som uppenbart att befintliga metoder inte når hela vägen fram. Om så vore fallet kan det ju, mot bakgrund av det samhälleliga intresset av att bekämpa sådan brottslighet, förväntas att tillräckliga insatser redan skulle ha satts in. Även om det inte på något vis är självklart att hemlig dataavläsning skulle leda till att alla, eller ens flera, av personerna i toppen av de kriminella nätverken, eller i Säkerhetspolisens fall t.ex. fler potentiella attentatsmän, skulle kunna åtkommas av de brottsbekämpande myndigheterna, skulle metoden ge bättre förutsättningar än vad de metoder som finns i dag gör för att så skulle kunna ske.

Det är en ren bedömnings- och prioriteringsfråga om man anser att hemlig dataavläsning är en effektiv åtgärd i relation till de resurser den kommer att kräva. Klart torde i vart fall vara att stora kostnadsökningar för åtgärden är försvarbara från effektivitetssynpunkt om åtgärden används och är lyckosam för att avvärja eller utreda ett enda terroristattentat eller för att komma åt ledande personer inom organiserad brottslighet som annars inte skulle kunna åtkommas. Som redovisats tidigare i betänkandet bedöms motsvarigheten till hemlig dataavläsning i Danmark vara ett ”særdeles nyttigt efterforskningsmiddel” och har där använts i förhållande till personer som senare dömts för terroristbrottslighet.

9.3.5 Betydelsen av kriminellas agerande

Inte så sällan framhålls förmågan hos kriminella att anpassa sig till de metoder som de brottsbekämpande myndigheterna använder. Särskilt anses detta gälla personer inom organiserad brottslighet. Våra utredningsdirektiv anger att risken för att de personer som begår brott anpassar sitt beteende för att komma runt de nya övervakningsverktygen och hur det skulle påverka effektiviteten behöver beaktas vid effektivitetsanalysen.

I SOU 2012:44 anfördes att strategier för att dölja den kriminella verksamheten, skydda huvudmän, varor och pengar, skaffa information och till och med påverka myndighetspersoner är centrala frågor för organiserad brottslighet. I den kriminella miljön finns därför ett stort intresse av att följa myndigheternas arbete, bygga upp kunskap om deras rutiner och på lämpligt sätt anpassa verksamheten och utveckla motstrategier.[35]

I samma betänkande angav Polisen bl.a. följande i sin behovsbeskrivning angående hemlig rumsavlyssning. Den grova organiserade brottsligheten blir allt mera medveten om vilka åtgärder de brottsbekämpande myndigheterna har möjlighet att använda. De kriminella känner väl till de lagliga gränserna för tvångsmedlen och följer utvecklingen av lagstiftningsarbete och praxis. Man anpassar sitt beteende efter förutsättningarna. T.ex. undviker man att tala om brottslighet i avlyssningsbara telefoner och att hålla möten på platser som kan tänkas vara avlyssnade. För att ytterligare förstärka säkerheten kring sin verksamhet använder de kriminella ibland även olika former av motmedel, som exempelvis störningsutrustningar, detekteringsutrustningar, kameror, dolda larm och visuell motspaning.[36]

I betänkandet anfördes också att personer med koppling till organiserad brottslighet inte enbart lägger ned mycket möda på att hemlighålla kommunikation, utan de skyddar sig även på annat sätt. Deras logistik är anpassad till att verksamheten är kriminell. En vanlig metod är att huvudmännen anlitar personer för riskfyllda uppgifter och använder mellanhänder för att inte exponera sig för myndigheterna.[37]

Det kan mot bakgrund av vad som nu anförts på goda grunder antas att kriminella involverade i allvarlig brottslighet följer utvecklingen avseende vilka metoder de brottsbekämpande myndigheterna får använda.

Om hemlig dataavläsning införs och de brottsbekämpande myndigheterna får tillstånd att genomföra åtgärden finns det risk för att åtgärden misslyckas, i meningen inte kan verkställas eller blir avbruten, om det sker en uppdatering av den tekniska utrustningen. Sådana uppdateringar kan initieras av den som skapat den tekniska

[35] Se SOU 2012:44 s. 217.
[36] Se SOU 2012:44 s. 248.
[37] Se SOU 2012:44 s. 344.

utrustningen (hård- eller mjukvarutillverkare) t.ex. för att en säkerhetsbrist har uppmärksammats. Om säkerhetsbristen är den som de brottsbekämpande myndigheterna tänkt använda vid verkställigheten kan således ett lyckosamt resultat omintetgöras genom en uppdatering. I någon mening är därför den omständigheten att kriminella håller teknisk utrustning uppdaterad en risk som kan påverka åtgärdens effektivitet.

En annan sådan risk, vilken i hög utsträckning förekommer redan i dag, är att kriminella använder flera olika tekniska utrustningar, typiskt sett flera telefoner. Ett sådant agerande – som inte sällan innebär att telefoner används endast kortare tid för att sedan slängas – medför att kartläggningsarbetet för de brottsbekämpande myndigheterna blir mer omfattande och dessutom snabbt kan bli omintetgjort. Emellertid torde ett sådant agerande också innebära en begränsning i möjligheterna för de kriminella att kommunicera på ett enkelt sätt.

Risken för att misstänkta ska uppmärksamma den teknik som de brottsbekämpande myndigheterna använder har av experterna på området bedömts som mycket begränsad. Denna bedömning gäller när verkställigheten genomförs med programvara. Dels krävs nämligen ett mycket tränat och tekniskt kunnigt öga, dels behöver den som söker veta vad den letar efter. När det gäller verkställighet med hårdvara torde risken för upptäckt motsvara den som gäller vid hemlig rumsavlyssning. Såvitt avser verkställighet efter inloggning på en misstänkts användarkonto kan det finnas en risk för att den misstänkte får meddelande om att sådan inloggning skett. Här bör dock återigen framhållas att det ligger i den brottsbekämpande myndighetens intresse att inte röja verkställigheten. Riskerna bör därför inte överskattas.

Det vore emellertid naivt att tänka sig att kriminella personer som är noga med att inte fysiskt eller på annat sätt direkt befatta sig med kriminaliteten och dessutom är noggranna att med alla till buds stående medel skydda sig och sin kommunikation (eller lagrade uppgifter) skulle ”gå i fällan” för att de brottsbekämpande myndigheterna ges möjlighet att vidta nya åtgärder. Det kan i stället förutsättas att sådana personer kommer att fortsätta söka efter motåtgärder för att undvika kontroll från de brottsbekämpande myndigheterna. Ett agerande som kan tänkas är en minskad användning av teknisk utrustning för kommunikation. En sådan utveckling är om-

vittnad redan i dag i vissa kriminella kretsar, som i viss utsträckning synes ha övergått från elektronisk kommunikation till andra sätt att kommunicera, t.ex. vid personliga möten. Ett dylikt agerande hämmar naturligtvis effektiviteten av hemlig dataavläsning men innebär samtidigt att andra, traditionella, spaningsmetoder eller tvångsmedel kan sättas in. Dessutom hämmas inte bara effektiviteten av tvångsmedelsanvändningen utan en övergång till annan kommunikation än elektronisk sådan torde också hämma effektiviteten av den brottsliga verksamheten.

Sammanfattningsvis kan konstateras att personer i den kriminella världen, i synnerhet organiserat kriminella, alltid kommer att söka begränsa effektiviteten av de åtgärder som de brottsbekämpande myndigheterna får vidta. Det ligger i sakens natur att så sker eftersom det kan få ödesdigra konsekvenser för kriminella att inte göra så. Det kan samtidigt konstateras att de motåtgärder som är möjliga att vidta för att undvika hemlig dataavläsning sannolikt kommer att påverka den kriminella verksamheten i, för de kriminella, negativ riktning.

9.4 Integritet

Utredningens bedömning: Hemlig dataavläsning innebär, vid en jämförelse med nuvarande ordning, i flera avseenden att riskerna för enskildas personliga integritet ökar.

9.4.1 Utgångspunkter

Skyddet för den personliga integriteten i lagstiftningen

Som en allmän målsättning för den offentliga verksamheten finns i 1 kap. 2 § fjärde stycket regeringsformen stadgandet att det allmänna ska verka för att demokratins idéer blir vägledande inom samhällets alla områden samt värna den enskildes privatliv och familjeliv. Bestämmelsen kompletteras och utvecklas i samma grundlag av det skydd som framgår av 2 kap. 6 § regeringsformen. I dess första stycke anges bl.a. att var och en är skyddad mot kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse och mot hemlig avlyssning eller upp-

tagning av telefonsamtal eller annat förtroligt meddelande. Enligt andra stycket gäller att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Även i Europakonventionen finns regler som skyddar den personliga integriteten för konventionsstaternas invånare. I dess artikel 8.1 anges att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Personlig integritet nämns inte särskilt i artikeln men respekten för de intressen som där anges torde i allt väsentligt innebära skydd för motsvarande intressen som de svenska grundlagsreglerna ger den personliga integriteten.

En bestämmelse om rätt till respekt för bl.a. privatlivet 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). Där framgår att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Av artikel 52.3 i rättighetsstadgan 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.

Begreppet personlig integritet

Många försök har gjorts att definiera begreppet personlig integritet. Integritetsskyddskommittén, Utredningen om ett modernt och starkt straffrättsligt skydd för den personliga integriteten och Integritetskommittén har i betänkanden redogjort för sådana försök. I förevarande sammanhang är det tillräckligt med en hänvisning till dessa redogörelser (se t.ex. s. 53–62 i SOU 2007:22 Del 1, s. 63–75 i SOU 2016:7 och s. 136–147 i SOU 2016:41).

Det står av de nämnda redogörelserna klart hur svårt det är 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. Det synes dessutom sällan ändamålsenligt att försöka ge en sådan bestämning eller

definition.[38] Integritetskommittén konstaterade att skälet till att begreppet inte låter sig fångas i en tydlig sentens är att rätten till en privat sfär inte är absolut, utan relaterad till en rad olika omständigheter, som dessutom kan variera över tid. Därför fann kommittén skäl att ansluta sig till följande slutsats som drogs i departementspromemorian Skyddet för enskilda personers privatliv (Ds 1994:51).[39]

> Det är svårt att ge ett sådant begrepp en tydligare avgränsning än att det innefattar vad som normalt framstår som angeläget att värna om för att den enskilde skall vara tillförsäkrad en rimlig, fredad, privat zon.

Även om det således är svårt, och troligen inte ändamålsenligt, att positivt bestämma vad begreppet personlig integritet innefattar 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”.[40]

När det gäller hemliga tvångsmedel har integritetseffekter diskuterats i vart fall i två av de nämnda betänkandena, vilka båda behandlade integritetsaspekter av lagstiftning som spände över en rad olika områden. Frågan har också varit uppe i utredningar och propositioner som föreslagit nya eller ändrade regler om hemlig tvångsmedelsanvändning liksom vid andra utredningar som utvärderat de hemliga tvångsmedlen. Därtill har integritetsfrågan angående hemliga tvångsmedel diskuterats i såväl juridisk doktrin som i kriminologiska sammanhang.[41] Det är svårt att tala om en samlad bild avseende vilka aspekter som bör hamna särskilt i fokus när risker för den personliga integriteten i samband med hemliga tvångsmedel ska analyseras.

Integritetsskyddskommittén fann att de straffprocessuella tvångsmedlen, särskilt de hemliga sådana, intar en särställning på integritetsskyddsområdet eftersom de ger staten laglig rätt till en långtgående och ofta djupt integritetskränkande övervakning och kontroll över medborgarna. Anledningen till att dessa tvångsmedel alls kan accepteras i ett demokratiskt samhälle är enligt kommittén att mot-

[38] SOU 2007:22 Del 1 s. 63 och SOU 2016:41 s. 147.
[39] SOU 2016:41 s. 147.
[40] SOU 2016:41 s. 148.
[41] Se t.ex. hela första häftet i SvJT 2007, Markus Naarttijärvis doktorsavhandling *För din och andras säkerhet, konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel* (2013) samt Janne Flyghed m.fl. *Brottsbekämpning – mellan effektivitet och integritet* (2000).

stående intressen, i synnerhet intresset av att effektivt kunna bekämpa grov brottslighet, under vissa omständigheter ter sig viktigare än skyddet för den personliga integriteten.[42]

Utredningen om vissa hemliga tvångsmedel ansåg i sitt betänkande *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44), främst utifrån sina direktivs utformning och Integritetsskyddskommitténs uttalanden om personlig integritet, 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, enligt Utredningen om vissa hemliga tvångsmedel, med befogenhetens (tvångsmedlets) utformning och tillämpning.[43] Våra direktiv beträffande integritetsfrågorna ansluter i hög utsträckning till det som Utredningen om vissa hemliga tvångsmedel anförde.

Hemlig dataavläsning och integritetsaspekter

I direktiven sägs bland annat att vi ska undersöka vilket integritetsintrång hemlig dataavläsning skulle medföra för enskilda och beskriva vilka avgränsningar som behövs. Där anges också att vi så långt det är möjligt ska redogöra för hur skyddet för den personliga integritetens kärnområden, dvs. sådant som rör individen och dennes personlighet, skulle påverkas av hemlig dataavläsning.

Omfattningen av de integritetskränkningar som kan bli följden av att hemlig dataavläsning får användas är av olika anledningar svår att uppskatta. Dels är det beroende på hur åtgärden utformas, dels medför varje tvångsmedelsanvändning oundvikligen ingrepp i den enskildes integritet. Hur allvarligt ingreppet är kan dock skifta från ett fall till ett annat. Det är därför vanskligt att i generella termer uttala

[42] Se SOU 2007:22 Del 1 s. 170.
[43] Se SOU 2012:44 s. 480.

något om vilka intrång hemlig dataavläsning skulle medföra för enskilda. Ett sätt att ändå angripa frågan är att i stället utgå från vilka risker för den personliga integriteten det går att se framför sig om åtgärden införs, både generellt och i de enskilda fallen. Eftersom vi anser att det är mer ändamålsenligt att tala om risker för den personliga integriteten kan den redogörelse som följer sägas utgöra integritetsriskbedömning.

En traditionell riskbedömning syftar till att identifiera risker och att därefter så långt som möjligt förhindra att riskerna leder till oönskade konsekvenser. I detta avsnitt kommer vi emellertid att stanna vid att identifiera de risker för den personliga integriteten som vi ser framför oss om hemlig dataavläsning införs och dessutom försöka värdera dessa risker. Frågan om att förhindra att riskerna leder till oönskade konsekvenser behandlas i stället i proportionalitetsavvägningen nedan och, framför allt, i våra överväganden och förslag i nästa kapitel.

Vi har gjort ett försök att värdera de olika riskerna utifrån vilken inverkan ett integritetsintrång har på den enskilde och på samhället i stort. För att dessa bedömningar inte ska bli allt för subjektiva har vi i möjligaste mån försökt att utgå från nuläget, dvs. göra bedömningen utifrån en jämförelse med vad som gäller i dag (t.ex. beträffande vilka andra möjligheter som finns att komma över motsvarande uppgifter). I värderingen av riskerna har vi försökt att bedöma riskökningarna utifrån en fyragradig skala där den första nivån är *ingen ökad risk*. I övrigt sträcker sig skalan från den lägre risknivån *viss ökad risk*, via medelnivån *påtagligt ökad risk* till den risknivå som innebär de största riskerna, nämligen *allvarligt ökad risk*.

Eftersom hemlig dataavläsning i flera avseenden i praktiken innebär en ny metod för att samla in uppgifter som får samlas in med redan befintliga hemliga tvångsmedel bör det återigen understrykas att vårt uppdrag inte omfattar en översyn av dessa.[44] Utrymme för en sådan analys finns inte heller inom ramen för denna utredning. Dessutom finns det skäl att utgå från att befintliga tvångsmedel alltjämt är nödvändiga och godtagbara från integritetssynpunkt.[45] I de delar

[44] Ett sådant uppdrag har dock Utredningen om datalagring och EU-rätten, se Dir. 2017:16.
[45] Jfr argument mot denna hållning i Markus Naarttijärvis avhandling *För din och andras säkerhet, Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel* s. 474 f. Vår uppfattning är emellertid att de utvärderingar som gjorts på senare tid, t.ex. i

hemlig dataavläsning i praktiken skulle vara ett sätt att verkställa befintliga hemliga tvångsmedel (i meningen samla in motsvarande information som får samlas in med dessa) finns därför skäl att endast bedöma om åtgärden innebär några ytterligare integritetsrisker i jämförelse med de åtgärder som ska verkställas, vilka ju innebär integritetsrisker som redan är balanserade i lagstiftningen.

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

Genom hemlig avlyssning och övervakning av elektronisk kommunikation samt inhämtning enligt inhämtningslagen får brottsbekämpande myndigheter rätt att i hemlighet ta del av innehåll i meddelanden (avlyssning) och uppgifter om meddelanden (övervakning och inhämtning) som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress. Motsvarande uppgifter skulle kunna samlas in med hemlig dataavläsning. Med den åtgärden skulle uppgifter som med nuvarande åtgärder inte är faktiskt möjliga att ta del av i klartext (pga. exempelvis kryptering) eller inte alls är möjliga att ta del av (pga. exempelvis anonymisering) kunna bli möjliga att ta del av.

Det skulle kunna hävdas att tillgång till uppgifter som brottsbekämpningen i dag inte kan ta del av utgör en ökad integritetsrisk för såväl den som utsätts för åtgärden som för tredje man, t.ex. den som kommunicerar krypterat med målpersonen. Lagstiftningen på det hemliga tvångsmedelsområdet, så som den ser ut, är emellertid balanserad utifrån vilka uppgifter som de olika tvångsmedlen *kan ge* tillgång till, dvs. vilka uppgifter som *får* hämtas in, och alltså inte utifrån vilka uppgifter åtgärderna ger *faktisk tillgång* till. Således är det t.ex. tillåtet för de brottsbekämpande myndigheterna att försöka dekryptera krypterade uppgifter som man fått in vid hemlig avlyssning av elektronisk kommunikation. Hemlig dataavläsning är, om åtgärden används för att läsa av innehållsuppgifter eller uppgifter om meddelanden, närmast att jämföra med sådan dekryptering. Metoden utgör då i praktiken ett sätt att komma runt vissa av de problem som

SOU 2012:44 och SOU 2016:41, ger stöd för att nuvarande regler på området är välbalanserade.

finns i verkställighetsfasen med de nämnda tvångsmedlen. Vår bedömning är därför att det inte föreligger någon ökad risk för den personliga integriteten om hemlig dataavläsning används för att läsa av innehåll i och uppgifter om meddelanden. En annan sak är att metoden i sig kan medföra integritetsrisker. Till dessa återkommer vi.

9.4.3 Hemlig dataavläsning för att ta del av lokaliseringsuppgifter

Genom hemlig övervakning av elektronisk kommunikation och inhämtning enligt inhämtningslagen kan brottsbekämpande myndigheter samla in dels uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, dels i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. De sistnämnda uppgifterna skulle också kunna samlas in med teknik för hemlig dataavläsning, t.ex. genom att en mobiltelefons GPS-utrustning aktiveras och att dessa uppgifter sedan läses av.

I den befintliga lagstiftningen som möjliggör inhämtning av lokaliseringsuppgifter görs ingen skillnad på hur detaljerade uppgifter som kan erhållas. I stadsmiljö finns det fler master som en mobiltelefon kan koppla upp sig mot och där är det därför möjligt att med bättre precision än på landsbygden, där antalet master är färre, erhålla lokaliseringsuppgifter. Med hemlig dataavläsning skulle uppgifterna om lokalisering kunna bli mer detaljerade än i stadsmiljö och det skulle dessutom inte fordras uppkoppling mot en mast för att lokaliseringsuppgifter skulle kunna hämtas in. Vår bedömning är därför att hemlig dataavläsning för att ta del av lokaliseringsuppgifter innebär en *visst ökad risk* för den personliga integriteten jämfört med dagens ordning.

9.4.4 Hemlig dataavläsning för att ta del av kameraövervaknings- och rumsavlyssningsuppgifter

Genom hemlig kameraövervakning får brottsbekämpande myndigheter använda fjärrstyrda TV-kameror, andra optisk-elektroniska instrument eller därmed jämförbara utrustningar för optisk personövervakning. Det är också möjligt för dessa myndigheter att genom

hemlig rumsavlyssning, med ett tekniskt hjälpmedel som är avsett att återge ljud, lyssna av eller ta upp tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till. Hemlig dataavläsning skulle kunna ge tillgång till motsvarande uppgifter, t.ex. genom att en mobiltelefons kamera eller mikrofon aktiverades och att uppgifterna därefter lästes av. Om åtgärden användes med motsvarande begränsningar (främst avseende krav på vilka platser åtgärderna får, och inte får, användas på) som gäller för hemlig kameraövervakning eller hemlig rumsavlyssning enligt gällande lagstiftning gör vi bedömningen att det inte skulle föreligga någon ökad risk för den personliga integriteten eftersom de uppgifter som då skulle kunna läsas av i sin helhet skulle motsvaras av de som får hämtas in i dag.

Annorlunda skulle det emellertid förhålla sig om motsvarande begränsningar avseende plats som gäller för hemlig kameraövervakning och hemlig rumsavlyssning inte skulle gälla för hemlig dataavläsning. Genom att aktivera t.ex. en mikrofonfunktion i en mobiltelefon kan det bli möjligt att höra varje ord på alla de platser som den misstänkte befinner sig. Det innebär risker för den personliga integriteten inte bara för den som utsätts för åtgärden utan också för andra som befinner sig i sådan närhet till denne att ljud från samtal de för kan fångas upp och samlas in. Även aktivering av kamera i t.ex. en mobiltelefon oberoende av plats skulle kunna innebära motsvarande integritetsrisker som de nyss nämnda.

När reglerna om hemlig kameraövervakning infördes diskuterade regeringen frågan om tillståndet skulle knytas till person eller plats. Man konstaterade först att ändamåls-, behovs- och proportionalitetsprinciperna skulle bli svåra att tillämpa om tillståndet skulle avse en person. Som exempel anfördes att det inte skulle gå att tillämpa proportionalitetsprincipen eftersom det på förhand inte vore 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.[46]

Om hemlig dataavläsning tilläts utan krav på plats för att läsa av kameraövervaknings- eller rumsavlyssningsuppgifter skulle det förhålla sig på motsvarande sätt som nyss anfördes, dvs. det skulle vara snudd på omöjligt att ta ställning till vilka integritetsintrång åtgärden skulle kunna medföra i det enskilda fallet. Därtill skulle det alltså vara möjligt, i vart fall teoretiskt, att dygnet runt ta del av vad den enskilde som är föremål för åtgärden, och personer i dennes omgivning, sa och gjorde. Det skulle således också bli fråga om en betydligt större mängd uppgifter, inte sällan också integritetskänsliga sådana, som samlades in som helt saknar betydelse för det ärende åtgärden vidtas i. Vår bedömning är att en sådan ordning skulle innebära *allvarligt ökade risker* för den personliga integriteten. Denna bedömning gäller beträffande den som utsätts för åtgärden men särskilt för personer som befinner sig i dennes närhet.

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

Teknik för hemlig dataavläsning skulle kunna möjliggöra avläsning av elektroniskt lagrade uppgifter och uppgifter som visar hur viss teknisk utrustning (t.ex. en dator eller mobiltelefon) används. Det finns i dag inget hemligt tvångsmedel som kan ge tillgång till sådana uppgifter.[47] Däremot får brottsbekämpande myndigheter ta del av elektroniskt lagrade uppgifter t.ex. i samband med undersökning av i beslag tagen elektronisk kommunikationsutrustning eller vid undersökning av sådan utrustning i samband med husrannsakan.

Enligt vår uppfattning är den största integritetsrisken på detta område själva uppgiftsinhämtningen, dvs. att brottsbekämpande myndigheter alls kan få tillgång till uppgifter som den som utsätts för åtgärden inte valt att dela med sig av. Denna risk föreligger alltså redan i dag vid husrannsakan eller beslag. Dessa åtgärder kan användas vid väsentligt mindre allvarlig brottslighet än den som våra direk-

[46] Prop. 1995/96:85 s. 29.
[47] Det finns dock möjlighet att, enligt 28 kap. 7 § andra stycket rättegångsbalken genomföra en husrannsakan med fördröjd underrättelse till den hos vilken husrannsakan företas.

tiv anvisar oss att analysera. Således får uppgifterna i dag hämtas in beträffande väsentligt fler brott än vad som kommer att vara möjligt vid hemlig dataavläsning.

Icke desto mindre skulle, om hemlig dataavläsning fick användas för att samla in elektroniskt lagrad information, ytterligare uppgifter än de som i dag är möjliga att samla in med hemliga tvångsmedel vara möjliga att samla in genom hemlig tvångsmedelsanvändning. Det kan dessutom förväntas bli fråga om betydande mängder uppgifter som kan göras tillgängliga för de brottsbekämpande myndigheterna. Bland de elektroniskt lagrade uppgifterna kan det också typiskt sett förväntas finnas både betydande mängder integritetskänslig information (t.ex. privata fotografier, uppgifter om enskildas ekonomi, och inloggningsuppgifter) och mycket som helt saknar betydelse för det ärende som föranlett åtgärden. Att hemlig dataavläsning utförs i hemlighet innebär därtill att den enskilde som utsätts, och andra vilkas personliga integritet riskerar att bli kränkt, inte får kännedom om eller kan bevaka sin rätt.

Möjligen kan, avseende den omständigheten att de brottsbekämpande myndigheterna alls kan ta del av uppgifterna, sägas att integritetsriskerna ökar beträffande de hemliga tvångsmedlen (eftersom någon motsvarande hemlig insamlingsmöjlighet för de uppgifter som avses inte finns i dag) men att den sammanlagda integritetsrisken är tämligen konstant (eftersom uppgifterna i och för sig redan kan samlas in av brottsbekämpande myndigheter). Mot bakgrund av att behovet föreligger inte bara i verksamhet där uppgifter kan samlas in i dag (förundersökningsfallen) utan också i sådan verksamhet där det inte finns motsvarande möjligheter (underrättelsefallen) och att det, om åtgärden införs, blir fråga om en hemlig realtidsövervakning är vår sammantagna bedömning att insamling av elektroniskt lagrade uppgifter inom ramen för hemlig dataavläsning innebär en *viss ökad risk* för den personliga integriteten jämfört med dagens förhållanden.

När det gäller den omständigheten att hemlig dataavläsning kan användas för att samla in uppgifter som visar hur teknisk utrustning används är det främst fråga om en typ av övervakning av hur den enskilde använder denna. De uppgifter som avses är exempelvis författande i ett elektroniskt dokument som inte sparas av användaren och angivande av vissa inloggningsuppgifter. Sådana uppgifter torde typiskt sett vara integritetskänsliga. Som framhölls i behovsavsnittet synes det närmast slumpmässigt vilka av dessa uppgifter som lagras

respektive inte lagras (i vart fall i den tekniska utrustningens temporära minne). I vissa fall torde det således förekomma att de uppgifter som här avses finns lagrade, eller i vart fall är möjliga att återskapa, vid t.ex. en undersökning av ett beslag. Detta talar för att bedömningen i denna del bör vara densamma som för risken det innebär att hemlig dataavläsning möjliggör insamling av lagrade uppgifter, dvs. att åtgärden utgör en *viss ökad risk* för den personliga integriteten jämfört med dagens förhållanden.

9.4.6 Hemlig dataavläsning – ett supertvångsmedel?

Om alla de uppgifter som hemlig dataavläsning skulle kunna tillgängliggöra alltid kunde samlas in i ett sammanhang, genom ett enda tillstånd, blir åtgärden väsentligt kraftfullare än något av de befintliga hemliga tvångsmedlen. Det skulle då kunna vara möjligt för den brottsbekämpande myndigheten som använder metoden att närmast fullständigt kartlägga och övervaka den person som utsätts för åtgärden. En sådan totalövervakning av en person innebär naturligtvis synnerligen stora risker för den personliga integriteten för den som utsätts för åtgärden, och ibland också för andra.

Det bör framhållas att det redan i dag förekommer att flera olika tvångsmedel används samtidigt mot en person och att det således redan är möjligt att genom hemlig tvångsmedelsanvändning i förening med andra åtgärder, såsom spaning, göra omfattande kartläggningar och vidta långtgående övervakning av den som utsätts för åtgärderna. Emellertid skulle hemlig dataavläsning, om åtgärden införs som ett enda tvångsmedel som alltid möjliggör insamling av alla uppgifter som vi konstaterat ett behov för alltså bli avsevärt mer kraftfullt än något av de hemliga tvångsmedel som finns i dag.

Den omständigheten att hemlig dataavläsning kan innebära synnerligen långtgående kartläggning och övervakning av den som utsätts för åtgärden innebär enligt vår bedömning en *allvarligt ökad risk* från integritetssynpunkt jämfört med dagens förhållanden.

9.4.7 Intrång i samband med verkställighet

Intrång i fysiska utrymmen

I avsnittet som behandlar hur hemlig dataavläsning kan verkställas har framkommit att det ibland kommer att vara nödvändigt för den myndighet som ska verkställa åtgärden att skaffa sig tillgång till den fysiska utrustningen som åtgärden ska avse. Det kan därför tänkas att det kan bli nödvändigt med intrång i annars skyddade utrymmen (exempelvis bostäder) för att möjliggöra verkställighet av hemlig dataavläsning. Sådana intrång är i dag möjliga efter särskilt tillstånd vid hemlig rumsavlyssning och vid husrannsakan. Vid hemlig kameraövervakning är det endast möjligt att få sådant tillträdestillstånd om det samtidigt ska genomföras hemlig rumsavlyssning. Tillträdestillstånd kan inte meddelas för verkställighet av hemlig avlyssning eller övervakning av elektronisk kommunikation. Om det för att hemlig dataavläsning ska kunna verkställas krävs att brottbekämpande myndigheter ges tillstånd att tränga in i annars skyddade utrymmen ökar således risken för integritetsintrång jämfört med nuvarande reglering.

I jämförelse med risken för den personliga integriteten som själva insamlingen av uppgifter med hemlig dataavläsning innebär framstår det nu anförda intrånget som en mindre risk. Dessutom är det redan i dag tillåtet med sådana intrång i vissa fall, t.ex. vid husrannsakan. Som påtalades i förarbetena till lagen om hemlig rumsavlyssning är dock en bostad många gånger en kärna i den enskildes privatliv.[48] Vår bedömning är att det föreligger en *viss ökad risk* från integritetssynpunkt om de brottsbekämpande myndigheterna får tillstånd att göra intrång i bostäder och andra skyddade utrymmen för att verkställa hemlig dataavläsning.

Intrång i teknisk utrustning

Som nämnts i avsnitt 8.4.1 kan olika tekniker aktualiseras vid verkställighet av hemlig dataavläsning, t.ex. utnyttjande av kända inloggningsuppgifter eller av sårbarheter i teknisk utrustning. Intrång av sådana slag som krävs torde – om de inte är sanktionerade i lagstift-

[48] Prop. 2005/06:178 s. 60.

ningen – utgöra straffbara dataintrång. Utöver det faktiska (fysiska eller virtuella) intrånget i teknisk utrustning skulle, som också redovisats i avsnitt 8.4.1, hemlig dataavläsning många gånger komma att fordra att installation sker av program- eller hårdvara för att åtgärden ska kunna fungera.

Av redovisningen i kapitel 6 avseende användningen av ny teknik framgår att datorer, mobiltelefoner och annan teknisk utrustning i dag har en central plats i många människors dagliga liv. Många är också de som använder teknisk utrustning för att förvara känsliga uppgifter i. Att utan lov från innehavaren ta sig in i dennes tekniska utrustning eller installera programvara i den, alternativt fästa hårdvara på den, kan därför för en del personer förväntas vara intrång som är jämförbara med exempelvis intrång i en bostad.

Liksom vad vi nyss anförde om intrång i annars skyddade utrymmen framstår dock själva intrånget (och installation av program eller hårdvara) i utrustningen som en mindre integritetsrisk än den risk det innebär att representanter för staten i hemlighet kan ta del av personlig information som finns tillgänglig i utrustningen (eller kommuniceras med den). Redan intrånget i utrustningen (och installationen av program eller hårdvara) utgör enligt vår mening dock en *viss ökad risk* från integritetssynpunkt.

9.4.8 Risk för tillämpningsglidningar

I direktiven anges att vi så långt som det är möjligt ska välja en teknikneutral reglering vid utarbetandet av lagstiftning. Ett sådant krav finns främst till för att lagstiftningen ska stå sig över tid, oberoende av den tekniska utvecklingen. Det har dock framhållits att teknikneutral lagstiftning kan öka risken för det som kallas tillämpningsglidningar, vilket innebär att lagstiftningen i takt med exempelvis en snabb teknisk utveckling får ett mer omfattande tillämpningsområde än vad som var tänkt från början.[49] Problemet med en sådan utveckling, i detta sammanhang, är att riskerna för den personliga

[49] Se t.ex. Markus Naarttijärvis avhandling För din och andras säkerhet, Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel, i vilken kapitel 9 ägnas problematiseringar av målsättningen om teknikneutralitet i lagstiftning, däribland risk för tillämpningsglidningar.

integriteten typiskt sett torde öka om regler om tvångsmedel ges ett vidare tillämpningsområde än de från början var tänkta att ha.

Som framgår i kapitel 6 har den tekniska utvecklingen på för utredningen relevanta områden varit väldigt snabb. Det finns ingenting som tyder på att utvecklingen kommer att avstanna. Lika viktigt som det är att hemlig dataavläsning kan stå sig trots att de tekniska förutsättningarna förändras i framtiden är det dock att åtgärden inte utan att lagstiftaren får tillfälle att väga av olika intressen mot varandra kan användas för att samla in andra uppgifter än sådana som åtgärden är avsedd att samla in när allt fler saker blir uppkopplade (sakernas internet[50]) eller när det är betydligt enklare än i dag att analysera väsentligt större datamängder (big data[51]).

Den snabba tekniska utvecklingen på relevanta områden kan innebära en risk för att lagstiftning om hemlig dataavläsning i framtiden kan komma att tillämpas på ett sätt som inte var avsett när reglerna infördes. Även om det av lätt insedda skäl är svårt att värdera hur stor denna risk är bedömer vi att redan risken för tillämpningsglidningar om hemlig dataavläsning införs innebär en *viss ökad risk* för den personliga integriteten.

9.4.9 Informationssäkerhet

En särpräglad risk om hemlig dataavläsning införs är risken för minskad informationssäkerhet dels i den tekniska utrustningen som är föremål för åtgärden, dels i andra tekniska utrustningar. Mot bakgrund av den centrala plats informationssäkerhet har i informationssamhället är det viktigt att nya metoder för de brottsbekämpande myndigheterna inte riskerar att få negativa återverkningar för informationssäkerheten i stort. I olika internationella sammanhang har det framförts att frågan om hemlig dataavläsning (och andra metoder för att komma runt bl.a. problem med kryptering och anonymisering) snarare än att väga säkerhets- och effektivitetsfrågor mot integritetsfrågor handlar om att väga säkerhet/effektivitet mot informationssäkerhet.[52] Med detta avses således att vikten av en funge-

[50] Se t.ex. SOU 2016:41 avsnitt 12.5.
[51] Se t.ex. SOU 2016:41 avsnitt 21.2.
[52] Se t.ex. House Homeland Security Committee Majority Staff Report, *Going dark, going forward*, publicerad på https://homeland.house.gov/wp-content/uploads/2016/07/Staff-

rande informationssäkerhet för samhället i stort och dess invånare bör ställas mot vikten av säkerhet och en effektiv brottsbekämpning i samhället.

Av det anförda följer att frågan om risker för informationssäkerheten alltså inte endast är en integritetsfråga. Risker för informationssäkerheten kan, men behöver således inte, påverka frågor om risker för den personliga integriteten. Om exempelvis de åtgärder som de brottsbekämpande myndigheterna vidtar innebär att det uppstår tillfälliga eller bestående säkerhetsrisker i den tekniska utrustning åtgärderna avser (t.ex. hål som andra kan ta sig in genom) kan emellertid risker för den enskildes personliga integritet uppstå, om det blir enklare för andra att komma åt personlig information om denne. Vi har därför funnit skäl att behandla frågan i detta avsnitt, som ju annars handlar om vad som kan kallas rena integritetsrisker.

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 program i systemet. Det kan handla om att genom s.k. exploits (se avsnitt 8.4.1) utnyttja sårbarheter i informationssystemet. Oavsett vilken typ av sårbarhet som utnyttjas för att bereda sig tillträde till systemet kan risker för informationssäkerheten uppstå om inte nödvändiga åtgärder vidtas.

Mot bakgrund av vikten för samhället i stort av fungerande informationssäkerhet och de integritetsrisker som kan bli följden av en minskad sådan bedömer vi att det föreligger en *påtagligt ökad risk* för den personliga integriteten om hemlig dataavläsning innebär att informationssäkerheten i den utrustning som åtgärden avser försvagas. Vi bedömer att det utgör en *allvarligt ökad risk* för den personliga integriteten om hemlig dataavläsning kan innebära att informationssäkerheten utanför den tekniska utrustning som åtgärden avser minskar.

Till det anförda kommer, eftersom risken för minskad informationssäkerhet alltså inte enbart innebär en risk för den personliga

---

Report-Going-Dark-Going-Forward.pdf. Se även rapporten *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparision of Practices*, en studie för LIBE-kommittén inom Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor, publicerad på www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

integriteten utan också utgör en risk i sig, att informationssäkerhetsrisker bör beaktas i ett vidare perspektiv än som integritetsrisker.

9.5 Inledande avvägningar mellan intressena

Utredningens bedömning: Det är proportionerligt att införa regler om hemlig dataavläsning under förutsättning att dessa balanserar de ökade integritetsriskerna och riskerna för informationssäkerheten som kan uppstå med hemlig dataavläsning.

9.5.1 Utgångspunkter

Vi har nu var för sig behandlat frågor om behov, effektivitet och integritetsrisker. Det som återstår är avvägningar avseende hur intresset av en effektiv brottsbekämpning bör balanseras mot de integritetsrisker som identifierats.

Vid avvägningar som vi gör i detta avsnitt ska givetvis reglerna i regeringsformen, Europakonventionen och EU:s rättighetsstadga beaktas. Vår bedömning är att hemlig dataavläsning är en åtgärd som kan medföra intrång både i det skydd som enskilda tillförsäkras enligt 2 kap. 6 § regeringsformen och de intressen som skyddas i artikel 8 i Europakonventionen och artikel 7 i rättighetsstadgan. För att en inskränkning av det skydd som regeringsformen och Europakonventionen (samt rättighetsstadgan) erbjuder ska vara tillåten krävs, utöver ett godtagbart ändamål, att det finns ett påtagligt behov av att använda hemlig dataavläsning som ett straffprocessuellt tvångsmedel, att mindre ingripande åtgärder inte är tillräckliga och att tvångsåtgärderna står i rimlig proportion till vad som står att vinna med dem. Det är dessa utgångspunkter och det i inledningen av detta kapitel citerade uttalandet som Integritetsskyddskommittén gjorde i SOU 2007:22 om proportionalitetsavvägningen som vi haft vid de bedömningar och avvägningar som redovisas nedan.

Det måste emellertid också beaktas att var och en som vistas i Sverige har rätt att göra anspråk på att staten vidtar effektiva åtgärder för att skydda hans eller hennes säkerhet. I detta ligger bl.a. att staten måste anstränga sig för att se till att brott förebyggs och utreds samt att gärningsmän ställs till ansvar för sina brottsliga hand-

lingar. Staten har således ett ansvar för att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda. Detta följer av bl.a. artikel 8 i Europakonventionen (se t.ex. Europadomstolens dom i rättsfallet Söderman mot Sverige den 12 november 2013, punkt 78). Det ska således finnas en välfungerande brottsbekämpning där de brottsbekämpande myndigheterna ska ha tillgång till effektiva utredningsverktyg i såväl fysisk som elektronisk miljö. Om så inte är fallet kan staten anses kränka de rättigheter som följer av Europakonventionen. Ett exempel på detta är Europadomstolens dom den 2 december 2008 i målet K.U. mot Finland där en person gjort sig skyldig till förtal eller möjligen sexuellt ofredande av ett 12-årigt barn. Förövaren kunde inte identifieras på grund av att den nationella lagstiftningen inte möjliggjorde att uppgift om vem som använt en IP-adress inte kunde hämtas in från operatören. Europadomstolen ansåg att ett praktiskt och effektivt skydd behövde finnas för att kunna identifiera och åtala förövaren men att sådant skydd inte fanns eftersom en effektiv utredning inte kunde vidtas på grund av att lagstiftningens krav på konfidentialitet (för IP-adresser). Domstolen uttalade vidare att även om yttrandefrihet och konfidentialitet för kommunikation är grundläggande rättigheter (eng. primary considerations) och att användare av telekommunikationer och internettjänster måste garanteras dessa rättigheter så kan rättigheterna inte vara absoluta i förhållande till andra intressen, t.ex. förebyggande av brott och skyddet för andras fri- och rättigheter. Domstolens slutsats blev att det är lagstiftarens uppgift att skapa ett regelverk som förenar de olika krav som konkurrerar om skydd enligt konventionen, se särskilt punkt 49 i den angivna domen.

Med de nu angivna utgångspunkterna redovisar vi i det följande våra inledande avvägningar beträffande om hemlig dataavläsning bör införas som ett nytt hemligt tvångsmedel. Först behandlas själva metoden för hemlig dataavläsning och om de ökade integritetsrisker som vi konstaterat i avsnitt 9.4, som sammanhänger med metoden, alls kan accepteras eller behöver balanseras i lagstiftning om åtgärden. Därefter behandlas själva informationsinhämtningen som kan ske med hemlig dataavläsning på motsvarande vis. Som avslutning på avsnittet gör vi en samlad inledande proportionalitetsavvägning.

9.5.2 Hemlig dataavläsning som metod

Hemlig dataavläsning – ett supertvångsmedel?

Oavsett vad de avvägningar vi gör i det följande leder fram till bör inledningsvis något sägas om det som ibland framhållits som den största risken med hemlig dataavläsning, nämligen att åtgärden kan bli ett slags ”supertvångsmedel”. Med tekniken för hemlig dataavläsning kan ju, åtminstone teoretiskt, en synnerligen omfattande kartläggning av en persons förehavanden genomföras. Detta eftersom den moderna människan i väldigt hög utsträckning använder den nya tekniken (särskilt mobiltelefoner) som en integrerad del i sitt liv. Det vore således möjligt att ha kontroll på var den som blir föremål för åtgärden befinner sig, vem hen talar med, vad de säger och gör i princip dygnet runt. Detta har vi bedömt som en *allvarligt ökad risk* från integritetssynpunkt (se avsnitt 9.4.6).

Det bör dock framhållas att redan dagens regelverk på tvångsmedelsområdet kan ge tillgång till i stort sett alla de typer av uppgifter som hemlig dataavläsning skulle kunna ge tillgång till. Det finns inget som formellt hindrar att samtliga befintliga hemliga tvångsmedel samtidigt kan riktas mot en och samma person om de proportionalitetsavvägningar som behöver göras för de olika tvångsmedlen leder till att det är godtagbart i ett enskilt fall. Vad som emellertid 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. Vår bedömning är att det då vore mycket svårt att balansera integritetsintresset i lagstiftningen på ett rimligt sätt. I dag skiljer det sig t.ex. väsentligt avseende vilka brott som det ska finnas misstanke om för att de nuvarande hemliga tvångsmedlen ska få användas (jämför t.ex. kraven för hemlig övervakning av elektronisk kommunikation med kraven för hemlig rumsavlyssning). Det är också delvis olika reglerat 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 har bedömts kunna uppstå om brottsbekämpande myndigheter får tillgång till de olika

uppgifterna. Dessa skillnader består även om uppgifterna hämtas in med metoden för hemlig dataavläsning.

Det anförda talar enligt vår mening med styrka för att inte låta hemlig dataavläsning bli ett ”supertvångsmedel”. Även om det är nödvändigt att införa åtgärden för att komma åt de skiftande slag av uppgifter som det enligt behovsanalysen finns behov av bör åtgärden differentieras. Med det avses att behovet av uppgifter i varje enskilt fall bör vara styrande för vad hemlig dataavläsning, i det enskilda fallet, får och ska kunna användas för. Är det exempelvis så att det är uppgifter från en misstänkts krypterade kommunikation via en mobiltelefon som den brottsbekämpande myndigheten behöver komma åt så bör åtgärden inte också per automatik ge tillgång även till alla bilder, filer och lösenord som finns sparade i telefonen. Om lagstiftning om hemlig dataavläsning balanseras med tydliga regler i detta avseende blir enligt vår bedömning riskerna för den personliga integriteten med hemlig dataavläsning mindre än om åtgärden införs som ett tvångsmedel som ”alltid kan ge tillgång till allt”.

För den förordade lösningen talar också de svårigheter som kan förväntas uppstå vid tillståndsgivningen om hemlig dataavläsning genom ett enda tillstånd får användas för att samla in alla uppgifter som metoden skulle kunna ge tillgång till. Hur en reell proportionalitetsavvägning i ett sådant fall skulle gå till är svårt att se framför sig. En inledande bedömning är därför att hemlig dataavläsning för varje uppgiftstyp som åtgärden bedöms nödvändig bör anses utgöra ett komplement till befintliga tvångsmedel. På så vis kan regler om hemlig dataavläsning, när det är lämpligt, knyta an till befintliga regler om hemliga tvångsmedel. Vi återkommer nedan till vilka uppgiftstyper hemlig dataavläsning bör tillåtas för.

Informationssäkerhet och hemlig dataavläsning

När det gäller frågan om informationssäkerhet har vi bedömt att det kan utgöra en *påtagligt ökad risk* för den personliga integriteten om hemlig dataavläsning innebär att informationssäkerheten i den utrustning som åtgärden avser försvagas eller en *allvarligt ökad risk* om hemlig dataavläsning kan innebära att informationssäkerheten utanför den tekniska utrustningen som åtgärden avser minskar.

Stark informationssäkerhet är ett så viktigt samhällsintresse i dag att det knappast kan accepteras att åtgärder som vidtas av brottsbekämpande myndigheter leder till minskad informationssäkerhet i någon annan utrustning än den som åtgärderna avser. Vi gör därför den inledande bedömningen att hemlig dataavläsning, trots de fördelar som åtgärden kan innebära för brottsbekämpningen, kan tillåtas endast om det vidtas nödvändiga och tillräckliga åtgärder för att informationssäkerheten i system utanför utrustningen som åtgärden avser inte ska minska till följd av åtgärden. Enligt vår bedömning kan detta inte säkerställas utan tydlig reglering som ålägger de brottsbekämpande myndigheterna att vidta aktiva åtgärder under hela den tid som verkställighet ska pågå. Vi återkommer i nästa kapitel avseende hur en sådan reglering närmare bör utformas för att balansera integritets- och informationssäkerhetsintressen.

Frågan är då om det kan accepteras att hemlig dataavläsning innebär minskad informationssäkerhet i den tekniska utrustning som åtgärden avser. I detta sammanhang bör man fråga sig vilka alternativ som finns till åtgärden. Vi bortser här från noll-alternativet, dvs. att behålla dagens ordning och därmed acceptera att de brottsbekämpande myndigheterna även i fortsättningen kommer att ha stora och framöver troligen än större svårigheter än i dag att samla in de uppgifter som tillståndet till tvångsmedelsanvändning omfattar. Då återstår enligt vår uppfattning två alternativ för att brottsbekämpande myndigheter ska kunna förbättra möjligheterna att komma åt uppgifter som det finns behov av. Båda torde enligt vår bedömning ha en större negativ inverkan på informationssäkerheten (och därmed också för riskerna för den personliga integriteten) än användning av teknik för hemlig dataavläsning. Det första är att kräva av teknikföretag och tjänstetillhandahållare att de ska kunna gå förbi säkerheten i sina egna system och tjänster för att bistå brottsbekämpningen. Riskerna för informationssäkerheten 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, t.ex. illasinnade hackare, vilket kan medföra stora risker för informationssäkerheten för alla, dvs. inte bara de kriminella. Ett annat, närliggande alternativ, är att systematiskt arbeta med att försvaga krypteringslösningar eller standarder för kryptering. Såvitt avser det senare alternativet framstår det som att det i än högre utsträckning sätter informationssäkerheten på spel.

Att generellt eller systematiskt försvaga krypteringslösningar för att komma åt uppgifter kan få oerhörda återverkningar på hela den legitima användningen av den moderna tekniken. Inget av de angivna alternativen till hemlig dataavläsning framstår mot bakgrund av det anförda som reella alternativ till hemlig dataavläsning. Dessutom framstår hemlig dataavläsning – en åtgärd som riktar sig mot en person och dennes tekniska utrustning och som dessutom utnyttjar dolda säkerhetsbrister – i jämförelse med alternativen som en klart mindre risk i ett informationssäkerhetsperspektiv.

För att hemlig dataavläsning ska införas krävs att de uppgifter som åtgärden kan förväntas ge tillgång till är av stor betydelse för brottsbekämpningen. Vår analys av om åtgärden bör införas ska dessutom utgå från förhindrande och utredande av mycket allvarlig brottslighet. Det är därför vår inledande bedömning att de risker som kan uppstå till följd av minskad informationssäkerhet i den tekniska utrustning som åtgärden avser kan accepteras om de balanseras mot väl avvägda regleringar för att hålla informationssäkerhetsrisker till ett minimum och att det sedan åtgärden har avslutats inte finns några kvardröjande informationssäkerhetsrisker.

Risker för tillämpningsglidning

Vi har också tagit upp risken för tillämpningsglidning som en *visst ökad integritetsrisk*. Med tillämpningsglidning avses risken för att en tvångsåtgärd får ett vidare tillämpningsområde än vad som var tänkt när den infördes t.ex. på grund av teknisk utveckling. Fenomenet bör i sig motverkas av att det tydligt i lagstiftningen om hemlig dataavläsning anges vilka förutsättningar som gäller för att en viss typ av uppgifter ska få samlas in med metoden. Därtill bör domstolsprövning och användande av offentligt ombud vid prövning av ansökan om åtgärden motverka risken för tillämpningsglidning. Även en viss tekniskspecificering avseende vilken typ av utrustning åtgärden får avse och vilken typ av uppgifter som får samlas in motverkar risken för framtida tillämpningsglidningar. Också framtida utvärderingar av åtgärden inklusive kontroll av hur tillämpningen ser ut kan hjälpa till att motverka denna risk. Vi återkommer i nästa kapitel till överväganden på dessa områden.

Intrång

För att kunna verkställa hemlig dataavläsning kan det bli aktuellt att göra intrång i såväl teknisk utrustning som i annars skyddade utrymmen. Vi har bedömt att sådana intrång utgör en *visst ökad risk* för den personliga integriteten om hemlig dataavläsning införs, se avsnitt 9.4.7. Eftersom sådana intrång som nu avses vissa gånger kommer att vara en förutsättning för att alls kunna genomföra hemlig dataavläsning bör de kunna tillåtas om åtgärden i övrigt är nödvändig, trots den ökade integritetsrisken intrången medför. En förutsättning bör dock vara att regler kring sådana intrång är tydliga och upprätthåller högt ställda krav på rättssäkerhet. När det är fråga om intrång i skyddade utrymmen (t.ex. bostäder) bör exempelvis som ett minimikrav gälla att den tekniska utrustning som hemlig dataavläsning ska avse finns på platsen där intrånget ska ske. Beträffande intrånget i utrustningen bör särskilt de informationssäkerhetsaspekter som diskuterats ovan få en framträdande plats.

9.5.3 De uppgifter som kan läsas av med hemlig dataavläsning

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

Det föreligger tungt vägande behov av en ny metod för att de brottsbekämpande myndigheterna i hemlighet ska kunna bereda sig tillgång till uppgifter i teknisk utrustning beträffande innehåll i och uppgifter om meddelanden som överförs eller överförts i elektroniskt kommunikationsnät, dvs. uppgifter som i dag kan hämtas in genom hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation eller inhämtning enligt inhämtningslagen, se avsnitt 9.2.3. Hemlig dataavläsning skulle kunna vara en effektiv metod för att få tillgång till sådana uppgifter, se avsnitt 9.3. Det uppstår enligt vår bedömning inga ökade risker för den personliga integriteten, utöver de integritetsrisker som följer av själva metoden för hemlig dataavläsning, om uppgifter som de brottsbekämpande myndigheterna redan i dag kan få tillstånd att hämta in i vissa fall i stället hämtas in genom hemlig dataavläsning.

Mot bakgrund av det tungt vägande behovet av nya åtgärder bör därför hemlig dataavläsning införas som metod för att brottsbekämpande myndigheter ska kunna få tillgång till innehåll i och uppgifter om meddelanden som de annars inte skulle kunna ta del av i klartext. I enlighet med direktivens anvisning bör hemlig dataavläsning endast få användas för att läsa av sådana uppgifter beträffande brott som kan föranleda användning av hemlig avlyssning av elektronisk kommunikation.

Hemlig dataavläsning för att ta del av lokaliseringsuppgifter

Det föreligger tungt vägande behov av nya och bättre metoder för att samla in lokaliseringsuppgifter, dvs. uppgifter som kan hämtas in genom hemlig övervakning av elektronisk kommunikation och inhämtning enligt inhämtningslagen, se avsnitt 9.2.3. Hemlig dataavläsning skulle kunna ge tillgång till mer precisa uppgifter som redan 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. I integritetsriskavseende har vi bedömt att det, utöver de integritetsrisker som följer av själva metoden för hemlig dataavläsning, föreligger en *visst ökad risk* om hemlig dataavläsning får användas på detta sätt jämfört med dagens förhållanden, se avsnitt 9.4.3.

Den ökade integritetsrisken är inte så stor att det tungt vägande behovet av nya och bättre metoder bör ge vika. En viss ökad risk för den personliga integriteten får därför accepteras för att ge de brottsbekämpande myndigheterna mer effektiva åtgärder. Hemlig dataavläsning bör således få användas för att ta del av lokaliseringsuppgifter. För att balansera integritetsriskerna bör dock lokaliseringsuppgifter inte få läsas av med hemlig dataavläsning för mindre allvarliga brott än sådana som kan föranleda användning av hemlig avlyssning av elektronisk kommunikation.

Hemlig dataavläsning för att ta del av kameraövervaknings- och rumsavlyssningsuppgifter

Det föreligger tungt vägande behov av nya metoder för att samla in sådana uppgifter som i dag får samlas in efter tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning, se avsnitt 9.2.3.

Hemlig dataavläsning skulle kunna ge tillgång till sådana uppgifter om det t.ex. vore tillåtet att aktivera en kamera eller mikrofon i en mobiltelefon och sedan läsa av uppgifterna. Vi har bedömt integritetsriskerna olika beroende på hur åtgärden används. Om motsvarande krav som gäller för hemlig kameraövervakning och hemlig rumsavlyssning (t.ex. avseende plats och vilka brott som kan föranleda åtgärderna) skulle gälla för hemlig dataavläsning för att ta upp sådana uppgifter har vi bedömt att det inte skulle uppstå någon ökad integritetsrisk, utöver de som följer av själva metoden för hemlig dataavläsning. Om däremot åtgärden tilläts för att, utan krav på plats där åtgärden får användas, läsa av kameraövervaknings- eller rumsavlyssningsuppgifter har vi bedömt att det kan uppstå allvarligt ökade risker för den personliga integriteten, se avsnitt 9.4.4.

Det anförda leder till slutsatsen att hemlig dataavläsning i vart fall bör få användas för att läsa av kameraövervaknings- eller rumsavlyssningsuppgifter under motsvarande förhållanden som gäller för hemlig kameraövervakning och hemlig rumsavlyssning i dag, dvs. i praktiken vara ett nytt sätt att verkställa dessa. När det gäller frågan om detta ska vara möjligt oberoende av var den som är föremål för åtgärden befinner sig gör vi följande bedömning.

Det är framför allt tre fördelar med att inte ha något krav på plats som lyfts fram av experterna från de brottsbekämpande myndigheterna. Den första är att de sammanhang som kriminella diskuterar det som brottsbekämpande myndigheter vill komma åt sällan är bundet till en bestämd plats, vilket medför att intressanta uppgifter i dag inte kan samlas in vid möten på sådana platser där avlyssning eller övervakning inte får ske. Den andra fördelen är att det blir svårare för kriminella som är väl införstådda med de brottsbekämpande myndigheternas arbetssätt och vilka begränsningar som gäller för tvångsmedelsanvändning att helt undvika att bli avlyssnade eller övervakade. Den tredje fördelen som lyfts fram tar sikte på möjligheten att använda en kamera eller mikrofon i teknisk utrustning för att kunna verifiera t.ex. vem som skriver ett meddelande eller identifiera vem som använder t.ex. en mobiltelefon.

Vi har i integritetsavsnittet redovisat vad regeringen framhöll när man införde platskravet i lagen om hemlig kameraövervakning 1995. Det som där nämndes om att ändamåls-, behovs- och proportionalitetsprinciperna skulle bli svåra att tillämpa om ett tillstånd till åtgärden skulle avse en person i stället för en plats gör sig gällande

även om ett tillstånd till hemlig dataavläsning knyts till viss teknisk utrustning i stället för till person. Också det exempel som regeringen anförde om att det inte skulle gå att tillämpa proportionalitetsprincipen eftersom det på förhand inte vore känt vilka eller hur många platser som skulle komma att övervakas gör sig gällande. Till argumentet kommer att det, med en närmast oinskränkt rätt att avlyssna eller kameraövervaka en person genom t.ex. dennes mobiltelefon, kan förväntas en väsentligt ökad insamling av information som helt saknar intresse för utredningen. Det är svårt att se hur det ska kunna undvikas att upptagningar görs av helt ovidkommande uppgifter, t.ex. när den som är föremål för åtgärden reser med kollektiva färdmedel, befinner sig på en restaurang eller på andra publika platser. Det ska framhållas att tillstånd till hemlig kameraövervakning och hemlig rumsavlyssning som utgångspunkt kan meddelas på sådana platser som nu nämnts redan i dag, t.ex. när det finns uppgifter om att ett intressant möte ska ske där. Vad som emellertid då kan (och bör) beslutas av den enskilde domaren som meddelar tillståndet är vilka åtgärder som den brottsbekämpande myndigheten ska vidta för att begränsa integritetrisker för andra än den som åtgärden avser, t.ex. beträffande kameravinkel eller mikrofonplacering. Enligt vad som framkom vid den kartläggning som gjordes i SOU 2012:44 synes sådana inskränkningar i tillstånd förekomma tämligen ofta.[53] Någon motsvarande sådan möjlighet till detaljerade begränsningar i tillståndet skulle i praktiken knappast kunna finnas utan motsvarande krav på plats eftersom domaren då inte skulle ha möjlighet att överblicka vilka platser som åtgärden skulle komma att vidtas på. I stället skulle domaren rimligen vara hänvisad till någon slags generella begränsningar. Konsekvensen av detta torde vara antingen att de generella begränsningarna blir så omfattande att åtgärdens effektivitet kraftigt hämmas eller så vaga att enskildas integritet åsidosätts.

Trots det tungt vägande behovet och de fördelar som skulle kunna uppnås utan ett platskrav är vår bedömning att de skäl som anfördes vid införandet av lagen om hemlig kameraövervakning fortfarande har skäl för sig. De svårigheter som kommer att uppstå i praktiken med att begränsa det potentiellt mycket stora integritetsintrånget i det enskilda fallet väger så tungt att det inte bör gälla något annat för

[53] SOU 2012:648 f.

hemlig dataavläsning när åtgärden används för att läsa av kameraövervaknings- eller rumsavlyssningsuppgifter än vad som gäller för hemlig kameraövervakning och hemlig rumsavlyssning.

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

Vi har bedömt att det föreligger tungt vägande behov av nya åtgärder för att de brottsbekämpande myndigheterna i hemlighet, löpande i realtid, ska kunna samla in även andra uppgifter än de som dagens hemliga tvångsmedel tillåter. De uppgifter som avses är elektroniskt lagrade uppgifter och uppgifter som visar hur viss teknisk utrustning används, se avsnitt 9.2.4. Det bedömda behovet föreligger både i brottsförhindrande och brottsutredande verksamhet. Vi har vidare bedömt att hemlig dataavläsning som metod för att samla in uppgifterna skulle kunna vara en effektiv metod, se avsnitt 9.3.

I avsnitt 9.4.5 har vi bedömt att en möjlighet till hemlig realtidsinsamling av elektroniskt lagrade uppgifter och uppgifter som visar hur viss teknisk utrustning används, utöver de integritetsrisker som följer av själva metoden för hemlig dataavläsning, utgör en *viss ökad risk* för den personliga integriteten jämfört med dagens förhållanden.

Det kan konstateras att de möjligheter som lagstiftningen i dag ger de brottsbekämpande myndigheterna, med hänsyn till den tekniska utvecklingen, inte är tillräckliga för att de ska kunna ta del av elektroniskt lagrade uppgifter och uppgifter som visar hur viss teknisk utrustning används. Som framhållits i behovsavsnittet är sådana uppgifter av väsentlig betydelse för en effektiv brottsbekämpning. De undersökningar av teknisk utrustning som kan genomföras i samband med husrannsakan och beslag har, liksom flera av de hemliga tvångsmedlen, tappat i effektivitet till följd av bland annat en allt högre krypteringsgrad och annan teknisk utveckling (t.ex. raderingsprogram).

Husrannsakan och beslag (och därmed undersökning av teknisk utrustning i samband med dessa) 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 det för att husrannsakan ska få genomföras krävs att det misstänkta brottet har fängelse i straffskalan. Båda åtgärderna kan således användas av brottsbekäm-

pande 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. I vart fall torde underrättelse till denne ske i tidigare skede vid sådana tvångsmedel än vid användning av hemliga tvångsmedel.

De uppgifter som de brottsbekämpande myndigheterna skulle kunna få del av, om hemlig dataavläsning tillåts för att samla in elektroniskt lagrade uppgifter och uppgifter som visar hur teknisk utrustning används, motsvarar i allt väsentligt de uppgifter som de kan få rätt att ta del av vid undersökningar i samband med husrannsakningar eller beslag. Vad som skiljer sig åt mellan dessa åtgärder och hemlig dataavläsning är att hemlig dataavläsning skulle kunna innebära en hemlig och löpande realtidsövervakning eller realtidskontroll av den tekniska utrustning åtgärden avser. Dessutom har vi bedömt att det föreligger behov av hemlig dataavläsning för insamling av elektroniskt lagrade uppgifter och uppgifter som visar hur teknisk utrustning används även i brottsförhindrande verksamhet, där ju husrannsakan och beslag inte kan förekomma i dag.

Det tungt vägande behovet och de fördelar åtgärden skulle innebära för intresset av en effektiv brottsbekämpning gör att vi bedömer att det, trots ökade integritetsrisker, är nödvändigt att brottsbekämpande myndigheter ges möjlighet till sådan uppgiftsinsamling som här avses. För att balansera integritetsriskerna bör dock 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.

9.5.4 Är det proportionerligt att införa hemlig dataavläsning?

Vi har nu vägt de integritetsrisker som vi särskilt identifierat beträffande hemlig dataavläsning mot de behov vi bedömt föreligger av nya åtgärder och dessas effektivitet. Sammanfattningsvis kan sägas att hemlig dataavläsning, oberoende av vilka uppgifter åtgärden ska användas för att ta del av, skulle inskränka de rättigheter och det skydd som tillkommer enskilda enligt 2 kap. 6 § regeringsformen, artikel 8.1 i Europakonventionen och artikel 7 i EU:s rättighets-

stadga. 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. 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.

Den bortre gränsen för i vilken grad den personliga integriteten i Sverige får inskränkas framgår av andra meningen i 2 kap. 21 § regeringsformen. Där framgår bland annat att en begränsning aldrig får sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar.

Allt för 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. För att motverka sådan misstro och ryktesspridning behöver reglering om hemlig dataavläsning förses med tydliga ramar och begränsningar av de situationer där åtgärden får vidtas. Redan genom att åtgärden aldrig får användas, varken under förundersökning eller i underrättelseverksamhet, vid annan brottslighet än sådan som kan föranleda hemlig avlyssning av elektronisk kommunikation finns enligt vår mening sådana ramar och begränsningar. Under förutsättning att fortsatta överväganden utgår från den begränsningen utgör hemlig dataavläsning enligt vår mening inte ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar.

För att regleringen ska vara proportionerlig krävs därutöver att de integritetsbalanserande åtgärder som vi nämnt i avsnitt 9.5.2 och 9.5.3 beaktas vid de fortsatta övervägandena. Därtill krävs att regleringen kringgärdas av starka rättssäkerhetsgarantier och innehåller så tydliga och strikta ramar att det inte ens kan misstänkas att regelsystemet utnyttjas utöver vad det ska tillåta. Regleringen måste även i övrigt utformas på ett sådant sätt att metoden kan accepteras av allmänheten som ett nödvändigt och godtagbart verktyg för de brottsutredande myndigheterna i kampen mot den allra allvarligaste kriminaliteten. Till närmare överväganden om sådana frågor oh till proportionalitetsavvägningar beträffande enskilda bestämmelser återkommer vi i nästa kapitel.

9.6 Något om egendomsskyddet

I direktiven anges, i anslutning till anvisningarna om de proportionalitetsavvägningar vi ska göra, att vi också behöver beakta frågor om hur metoden skulle påverka enskildas egendomsskydd när det gäller tekniska utrustningars lagringsutrymme (eventuella begränsningar i överföring av datamängd och kapacitet) och kostnader för enskilda. Vi har funnit skäl att göra det här i anslutning till de inledande proportionalitetsavvägningarna.

Av 2 kap. 15 § regeringsformen följer 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. Den som tvingas avstå från sin egendom ska ha rätt till ersättning för förlusten. Detsamma gäller vid vissa rådighetsinskränkningar som avser användningen av mark eller byggnad. Ersättningen ska bestämmas enligt grunder som anges i lag. Denna rättighet gäller på motsvarande sätt även utlänning här i riket.

Med expropriation eller annat sådant förfogande avses att en förmögenhetsrätt – dvs. äganderätt eller annan rätt med ett ekonomiskt värde, t.ex. nyttjanderätt, servitut eller vägrätt – tvångsvis överförs eller tas i anspråk. Lagstiftning som möjliggör sådana ingrepp finns i expropriationslagen (1972:719) men även i annan lagstiftning, som exempelvis plan- och bygglagen (2010:900). Utanför bestämmelsens tillämpningsområde faller ingrepp som innebär att egendom förstörs t.ex. på grund av risk för smitta. Inte heller skatt, böter, viten och exekutiva åtgärder omfattas av bestämmelsen. Som exempel på förfoganden som är likställda med expropriation har nämnts nationalisering och socialisering av egendom (prop. 2009/10:80 s. 163 f.).

Bestämmelserna om skydd för egendom i 2 kap. 15 § regeringsformen har inte ansetts hindra straffrättsliga regler om förverkande (se NJA 2007 s. 918 med vidare hänvisning till SOU 1993:40 s. 47 och Bengtsson, *Ersättning vid offentliga ingrepp 1*, 1986 s. 77 och 133). Inte heller de beslut som tas för att säkerställa ett förverkande, såsom beslag och hantering av beslagtagen egendom, eller försäljning och andra åtgärder med beslagtagen egendom, är mot bakgrund av det redovisade förarbetsuttalandet om omfattningen av skyddet för egendom en sådan inskränkning i äganderätten som omfattas av

regeringsformens särskilda skydd (prop. 2014/15:26 s. 24 f.). Mot denna bakgrund gjorde regeringen bedömningen att försäljning eller förstöring av ett fordon som tagits i beslag i förverkandesyfte innan förverkandefrågan prövats slutligt var förenlig med regeringsformens bestämmelser om skyddet för äganderätten (a. prop. s. 26).

Förverkande av egendom, samt nämnda åtgärder såsom försäljning eller förstöring av egendomen innan lagakraftvunnet förverkandebeslut, har långtgående verkningar för den enskilde eftersom en slutlig förlust av möjligheten att använda egendomen blir konsekvensen av sådana beslut. Den inskränkning i lagringsutrymme eller kapacitet i övrigt som hemlig dataavläsning skulle kunna innebära är typiskt sett gällande under en begränsad tid och avser dessutom inte egendomen i sin helhet. Det framstår som orimligt att låta den mindre inskränkningen av äganderätten (hemlig dataavläsning), men inte den större (förverkande), omfattas av regeringsformens skydd för egendomen. Vår slutsats blir därför, i analogi med vad som anses gälla för förverkande och beslut som tas för att säkerställa ett förverkande (t.ex. beslag), att de åtgärder som behöver vidtas vid hemlig dataavläsning och som kan innebära begränsningar av t.ex. lagringsutrymme eller annan kapacitet hos enskilds tekniska utrustning inte kan anses innebära en sådan inskränkning i äganderätten som omfattas av regeringsformens särskilda skydd. När det gäller sådant ianspråktagande av enskildas lagringsutrymme i teknisk utrustning eller kapacitet i övrigt vid hemlig dataavläsning bör dessutom framhållas att det ligger i brottsbekämpningsintresset att begränsa sådant eftersom ett allt för stort ianspråktagande kan leda till en ökad upptäcktsrisk. Det finns därför skäl att utgå från att lagringsutrymme och annan kapacitet hos den tekniska utrustning som åtgärden avser endast i mycket begränsad utsträckning kommer att påverkas av åtgärden.

Det är emellertid inte enbart regeringsformen som är av intresse i sammanhanget. Också Europakonventionens bestämmelser har betydelse för bedömningen. I artikel 1 i första tilläggsprotokollet till Europakonventionen finns bestämmelser om skydd för egendom.

Enligt första stycket ska varje fysisk eller juridisk person 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.

I andra stycket anges att bestämmelserna i första stycket inte inskränker en stats rätt att genomföra sådan lagstiftning som staten finner nödvändig för att reglera nyttjandet av egendom i överensstämmelse med det allmännas intresse eller för att säkerställa betalning av skatter eller andra pålagor eller av böter och viten.

Begreppet egendom har en autonom och vidsträckt innebörd. Det omfattar inte bara fast och lös egendom av olika slag utan också begränsade sakrätter av ekonomiskt värde liksom fordringar och immateriella rättigheter. Även olika typer av ekonomiska intressen och förväntningar omfattas av begreppet (se t.ex. Danelius, *Mänskliga rättigheter i europeisk praxis*, femte uppl., s. 572). Mot bakgrund av den vidsträckta innebörd som egendomsbegreppet i artikeln givits torde förväntningar på sådant lagringsutrymme eller annan kapacitet som den enskilde betalat för inrymmas i begreppet.

Europadomstolen har slagit fast att artikel 1 i det första tilläggsprotokollet innehåller tre regler, nämligen

– principen att egendom ska respekteras,
– villkoren för att någon ska få berövas sin egendom och
– frågan om hur ägarens rätt att utnyttja sin egendom får begränsas.

Den första regeln återfinns i första styckets första mening, den andra i första styckets andra mening och den tredje i andra stycket. Domstolen har emellertid förklarat att de tre reglerna emellertid inte är separata i den meningen att de inte har något samband med varandra. De andra och tredje reglerna avser särskilda fall av ingrepp i äganderätten och måste därför tolkas i ljuset av den allmänna principen som är angiven i den första regeln (a.a.s. 577 f.).

Det är av betydelse under vilket av styckena i artikeln om egendomsskyddet som hemlig dataavläsning kan bedömas höra när det gäller eventuella begränsningar i lagringsutrymme eller kapacitet i övrigt som åtgärden kan medföra. Frågan är således om det handlar om ett sådant berövande av egendom som regleras i första stycket andra meningen eller om det handlar om en sådan nyttjandeinskränkning som avses i andra stycket. Som framgår av artikelns utformning är skyddet mot nyttjandeinskränkningar i andra stycket klart mera begränsat än skyddet mot berövande av egendom i första stycket.

Det saknas, så vitt känt, praxis från Europadomstolen avseende hur sådana inskränkningar i egendomsskydd och äganderätt som

hemliga tvångsmedel kan innebära bör bedömas. Däremot finns flera rättsfall som behandlar förverkande och beslag. Det ligger nära till hands att, liksom vi gjorde vid bedömningen av egendomsskyddet enligt regeringsformen, göra jämförelser med vad som gäller för sådana inskränkningar av enskildas äganderätt även här.

Europadomstolen har i flera rättsfall behandlat beslag och förverkande som åtgärder syftande till att kontrollera användningen av egendom, se t.ex. Handyside mot Förenade kungariket och Yildirim mot Italien. Inte sällan har sådana åtgärder ansetts legitima då syftet varit att förhindra brottslig verksamhet eller vara led i kampen mot organiserad brottslighet, se t.ex. Silickienė mot Litauen och Arcuri m.fl. mot Italien.

Enligt vår mening har de inskränkningar som hemlig dataavläsning kan ha på enskildas äganderätt, såvitt avser exempelvis lagringsutrymmes- och kapacitetsbegränsningar, ett nära samband med de begränsningar som uppstår när egendom tas i beslag. Det är därför naturligt att anta att bedömningen även i dessa fall ska göras utifrån det rättighetsskydd som följer av andra stycket i artikel 1. Det betyder att möjligheten att införa en ordning med metoder för hemlig dataavläsning är i enlighet med konventionens bestämmelser om åtgärden bedöms nödvändig i det allmännas intresse.

Även för artikel 1 andra stycket gäller emellertid att en proportionalitetsbedömning måste göras. Om det inte finns en rimlig balans mellan det allmänna intresset och den enskilde ägarens intresse strider en inskränkning av rätten att utnyttja egendom mot artikel 1. När det gäller inskränkningar i rätten att använda egendom har Europadomstolen anlagt ett för den enskilde relativt strängt synsätt och funnit att även ganska tyngande begränsningar av ägarens rättigheter har kunnat accepteras i det allmännas intresse. Staterna har alltså tillerkänts ett relativt stort utrymme för att bedöma vilka inskränkningar som ter sig rimliga med hänsyn till allmänna intressen (se Danelius, *Mänskliga rättigheter i europisk praxis*, 4 uppl., 2012 s. 562). Vid avgörandet om ingripandet är proportionerligt tas vidare hänsyn till om den enskilde tillerkänns ersättning och i övrigt till de omständigheter under vilka ingreppet sker, se t.ex. James m.fl. mot Förenade kungariket.

En möjlighet att genomföra hemlig dataavläsning vilar på intresset av att förbättra förutsättningarna för att kunna utreda och förhindra allvarlig brottslighet. När man bedömer om den åtgärden kan

anses proportionerlig bör man ha i åtanke att det kommer att uppställas krav på såväl misstankegrad (förundersökningsfallen) eller annars en viss grad av risk (förhindrandefallen) som en kvalificering av vilka brott som kan föranleda åtgärden. Dessutom, vilket nämnts ovan, kommer de inskränkningar som här avses vara av mycket begränsad omfattning eftersom risken för upptäckt annars kommer att öka. Till detta kommer att det ekonomiska värdet av inskränkningen kommer att vara mycket begränsat, i de flesta fall rimligen noll eller i vart fall så litet för den enskilde att denne inte kommer att uppmärksamma det. Det kan övervägas om en lagreglerad rätt till ersättning för den vars lagringsutrymme eller kapacitet i övrigt begränsas borde införas. Det finns dock mot bakgrund av det som nu anförts och att en sådan rättighet skulle riskera att bli en chimär i många fall, eftersom underrättelse inte kommer att vara möjlig att lämna (och den enskilde således inte veta om att denne utsatts för åtgärden), skäl att inte införa en sådan möjlighet. Att underlåta detta innebär enligt vår mening inte att hemlig dataavläsning – såvitt avser egendomsskyddet – är en oproportionerlig åtgärd.

Vår slutsats av det anförda är att de begränsningar som hemlig dataavläsning skulle kunna innebära avseende lagringsutrymme och kapacitetsutnyttjande i övrigt är förenliga med Europakonventionens och regeringsformens bestämmelser om skyddet för äganderätten.

10 Hemlig dataavläsning – en ny lag

10.1 En ny lag om hemlig dataavläsning införs

Utredningens förslag: En ny lag införs med bestämmelser om hemlig dataavläsning. Lagen tidsbegränsas till att gälla i fem år efter införandet för att en utvärdering av hemlig dataavläsning ska kunna göras när lagen har tillämpats en tid.

Vi har i föregående kapitel redovisat våra inledande avvägningar avseende om hemlig dataavläsning alls kan införas som metod i den svenska brottsbekämpningen. Som framgått där har vi bedömt att det, trots de risker för den personliga integriteten åtgärden kan tänkas medföra, bör göras möjligt för de brottsbekämpande myndigheterna att använda hemlig dataavläsning för informationsinhämtning. Vi ska nu övergå till att redovisa de överväganden vi gjort för den reglering av åtgärden som vi föreslår. Även i denna del blir det i många avseenden fråga om intresseavvägningar, bl.a. mellan behovet av en effektiv brottsbekämpning och integritetsintressen.

10.1.1 Tre olika alternativ – och vårt val

Som framgått tidigare kan metoden för hemlig dataavläsning användas både för att hämta in uppgifter som de brottsbekämpande myndigheterna redan i dag kan få tillstånd att hämta in med hemliga tvångsmedel och för att hämta in andra uppgifter, såsom lagrade uppgifter och uppgifter om hur viss teknisk utrustning används. I föregående kapitel har vi kommit till slutsatsen att det finns tungt vägande behov i de brottsbekämpande myndigheternas verksamhet att komma åt dessa uppgifter i klartext, att hemlig dataavläsning kan tillgodose detta behov och att det är proportionerligt att införa regler

om hemlig dataavläsning om dessa förses med vissa begränsningar. Vi har mot denna bakgrund övervägt olika alternativ till lagstiftning. Det har utkristalliserat sig tre egentliga alternativ till lagstiftning, där de två första i någon mening är varandras motsatser och det tredje är en slags hybridlösning eller sammanvägning av de andra alternativen. Att de två första alternativen är varandras motsatser innebär att de fördelar som kan finnas med det ena av dem ofta blir en nackdel med det andra, och vice versa. När vi i det följande beskriver alternativen behandlar vi därför de två första alternativen tillsammans, varefter vi presenterar alternativ tre för sig självt. Det ska redan här sägas att vårt val har fallit på det tredje alternativet.

De två ”ytterlighetsalternativen”

Alternativ 1

> Införande av dels kompletterande verkställighetsregler i befintlig tvångsmedelslagstiftning som tillåter tekniken för hemlig dataavläsning att användas som en ren verkställighetsmetod för nuvarande hemliga tvångsmedel, dels regler om ett nytt hemligt tvångsmedel som ger brottsbekämpande myndigheter möjlighet att i hemlighet hämta in elektroniskt lagrade uppgifter eller uppgifter som visar hur teknisk utrustning används (där tekniken för hemlig dataavläsning får användas i verkställighetsfasen).

Alternativ 2

> Införande av bestämmelser om hemlig dataavläsning som ett enda hemligt tvångsmedel vilket, när tillstånd till det har meddelats, alltid ger möjlighet att hämta in alla typer av uppgifter som kan hämtas in med metoden.

Det går en tydlig skiljelinje mellan de två presenterade alternativen eftersom det första, men inte det andra, utgår från att den struktur som råder i dag på det hemliga tvångsmedelsområdet upprätthålls. Med detta avses att när det är fråga om att hämta in uppgifter som den brottsbekämpande myndigheten redan i dag kan få tillstånd att hämta in så innebär hemlig dataavläsning i praktiken endast att en ny teknik får användas för att genomföra detta. Med det andra alternativet blir gränsen till nuvarande hemliga tvångsmedel mer otydlig eftersom det möjliggör inhämtning av både samma typer av uppgif-

ter som får hämtas in med andra hemliga tvångsmedel och andra uppgifter.

Vår bedömning är att alternativ 1 på ett tydligare sätt än alternativ 2 beskriver vad som är vad och mer dynamiskt anger när tekniken för hemlig dataavläsning används för verkställighet respektive som ett eget tvångsmedel. Samtidigt innebär det första alternativet att en och samma teknik i vissa fall blir en verkställighetsmetod och i andra situationer i praktiken ett eget tvångsmedel. I det avseendet är alternativ 2 tydligare eftersom den tekniska metoden i det fallet utgör själva avgränsningen för åtgärden. På det sättet kan man säga att alternativ 2 liknar några av de nuvarande hemliga tvångsmedlen, vilka också avgränsas bl.a. av den tekniska metod som ska användas (jfr t.ex. hemlig rumsavlyssning där en del av definitionen av åtgärden är att avlyssningen kan ske ”med ett tekniskt hjälpmedel som är avsett att återge ljud”). I någon mening kan nog det andra alternativet vara en aning mer lättillgängligt för den som ska ta del av bestämmelserna. Därtill kommer att alternativ 2 på ett enklare vis skulle kunna regleras i en lag medan det första alternativet sannolikt skulle kräva reglering såväl i en ny lag som i de nuvarande lagarna som reglerar den hemliga tvångsmedelsanvändningen.

Mot det andra alternativet talar de svårigheter som vi nämnt i föregående kapitel med att avgränsa när åtgärden får användas med avseende på bl.a. integritetsfrågor, eftersom det är fråga om ett kraftfullt verktyg, se diskussionen om ”supertvångsmedel” och differentiering av hemlig dataavläsning i avsnitt 9.5.2. De nuvarande hemliga tvångsmedlen är, som redan nämnts, reglerade på olika vis beroende på de integritetsintrång som de kan medföra. Skillnaden i vilka brott som kan föranleda hemlig övervakning av elektronisk kommunikation och de som kan leda till användning av hemlig rumsavlyssning är stor. Det är svårt att se framför sig hur man i alternativ 2 skulle kunna göra rimliga överväganden som innebär att intresset för den personliga integriteten kan upprätthållas på det sätt som befintlig lagstiftning föreskriver. I detta avseende skulle det första alternativet vara väsentligt enklare eftersom det med detta vore möjligt att föreskriva att samma integritetshänsyn som redan tas också ska tas när hemlig dataavläsning blir ett sätt att verkställa andra hemliga tvångsmedel. I den mån det bedöms nödvändigt att införliva även andra skyddsmekanismer vore det också förhållandevis enkelt i alternativ 1, t.ex. genom att samma regler som redan gäller ska gälla även vid

verkställighet med teknik för hemlig dataavläsning men att det då också ska gälla vissa andra skyddsregler. I den del alternativ 1 innebär ett nytt hemligt tvångsmedel vore det också möjligt att gradera den risk för integritetsintrång som åtgärden innebär och då bestämma vilken nivå integritetsskyddsreglerna ska hamna på i förhållande till andra hemliga tvångsmedel.

Sammanfattningsvis har vi funnit såväl för- som nackdelar med båda de presenterade alternativen. Mot denna bakgrund har vi övervägt om det är möjligt att ”plocka russinen ur kakan” på ett sätt som innebär att fördelarna med vart och ett av alternativen kan behållas utan att nackdelarna som framhållits blir kvar. Vi har konstaterat att det är möjligt med ett tredje alternativ. Det kallar vi för hybridalternativet.

Hybridalternativet

Alternativ 3

> En kombination av de två alternativen ovan som innebär införande av bestämmelser om hemlig dataavläsning där åtgärden i och för sig är ett nytt tvångsmedel men där det tvångsmedlet kan användas för inhämtning av både uppgifter som får hämtas in med andra tvångsmedel och de andra typer av uppgifter som vi funnit tungt vägande behov av att hämta in. I alternativet kan också en differentiering göras beroende på vilka typer av uppgifter som ska hämtas in.

Genom alternativ 3 kan man kombinera fördelarna som vi framhållit med de två tidigare alternativen, nämligen tydligheten med alternativ 1 och enkelheten med alternativ 2. Med detta alternativ blir hemlig dataavläsning visserligen ett nytt tvångsmedel, som i alternativ 2, men dess användningsområde begränsas till vilka typer av uppgifter som åtgärden i det enskilda fallet ska användas för att hämta in, liksom i alternativ 1. På så vis kan också de risker som teknik för hemlig dataavläsning kan medföra, se avsnitt 9.5.2, tas om hand och balanseras på ett rimligt sätt. Med hybridalternativet blir åtgärden förvisso inte en ren verkställighetsåtgärd, såsom skulle bli fallet enligt alternativ 1, men i praktiken ett tvångsmedel som kan användas för att hämta in uppgifter som också får hämtas in efter tillstånd till andra tvångsmedel, när förutsättningar för dessa föreligger. Genom att reglera hemlig dataavläsning på detta vis slipper man

också de särskilda svårigheterna att värna den personliga integriteten som föreligger med alternativ 2.

Som kommer att framgå i det följande föreslår vi att hemlig dataavläsning blir *ett* nytt hemligt tvångsmedel. Det innebär att det är för att få använda hemlig dataavläsning som den brottsbekämpande myndigheten begär tillstånd. Dock kommer hemlig dataavläsning inte, som i alternativ 2, bli ett tvångsmedel som det är möjligt att *alltid* hämta in en massa olika typer av uppgifter med. I stället ska förutsättningarna i det enskilda fallet, och vilka uppgifter som är av intresse för den brottsbekämpande myndigheten, vara avgörande för hur åtgärden får användas.

10.1.2 En tidsbegränsad lag om hemlig dataavläsning införs

Vi har således funnit skäl att gå vidare med överväganden som utgår från alternativ 3. Innan vi kommer in på mer detaljerade frågor om själva lagstiftningen bör något dock sägas om var de nya bestämmelserna ska placeras och om skälen för och emot att tidsbegränsa ny lagstiftning.

Man skulle kunna tänka sig att, eftersom det redan finns upparbetade regelverk om hemliga tvångsmedel i både rättegångsbalken (förundersökningsfallen) och vissa speciallagar (underrättelsefallen), placera regler om ett nytt tvångsmedel i redan gällande lagar. Det är möjligt även om de nya reglerna ska tidsbegränsas, se t.ex. 3 § lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). En fördel med att placera de nya reglerna i existerande lagar är att det går att använda den redan befintliga lagtekniska strukturen i dessa. En annan fördel är att det blir mer lättillgängligt med hänvisningar till bestämmelser i samma lag än med motsvarande hänvisningar till andra lagar.

I stort sett samtliga lagar på det hemliga tvångsmedelsområdet som medfört nya tvångsmedel eller gjort existerande hemliga tvångsmedel tillämpliga på nya områden har tidsbegränsats. Det har motiverats med att en utvärdering av lagstiftningen bör ske när lagen har tillämpats en tid. Även om vi i effektivitetsanalysen bedömt att hemlig dataavläsning bör vara en effektiv metod är det inte möjligt att fullt ut konstatera det eller vilken nytta metoden faktiskt kom-

mer att ge förrän den har tillämpats en tid. Mot denna bakgrund och med beaktande av att hemlig dataavläsning blir en ny åtgärd i Sverige som innebär särskilda risker för den personliga integriteten bör den nya lagen tidsbegränsas. En senare utvärdering av lagens tillämpning kommer att utgöra ett ytterligare underlag inför ett ställningstagande om det finns skäl att permanenta lagen. De nya bestämmelserna bör med hänsyn till att lagen tidsbegränsas inte tas in i rättegångsbalken eller de andra lagar som reglerar hemliga tvångsmedel utan i en särskild lag.

När det gäller hur lång tid som lagen bör vara i kraft innan en utvärdering kan göras bör beaktas att tekniska experter vid de brottsbekämpande myndigheterna bedömt att antalet ärenden där den nya metoden kommer att kunna användas, åtminstone till en början kommer att vara begränsat. Det framstår därför inte som ändamålsenligt att föreslå allt för kort giltighetstid för lagen.

När lagen om hemlig rumsavlyssning infördes begränsades dess giltighetstid till tre år. Den utredning som sedan tillsattes för att utvärdera lagen konstaterade att antalet fall av hemlig rumsavlyssning var så få att det inte utifrån dessa gick att dra några säkra slutsatser om den hemliga rumsavlyssningens effektivitet och praktiska värde.[1] Det finns risk för att tre års giltighetstid för en lag om hemlig dataavläsning leder till samma resultat. Lagen bör därför tidsbegränsas till att gälla i fem år från dess införande.

10.2 Innebörden av hemlig dataavläsning

Utredningens förslag: Hemlig dataavläsning innebär 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 eller ett användarkonto till, eller en på motsvarande sätt avgränsad del av, en kommunikationstjänst, lagringstjänst eller liknande tjänst.

[1] Se SOU 2009:70 s. 160.

10.2.1 Objektet för hemlig dataavläsning

En ny lag om hemlig dataavläsning bör inledas med en definition som avgränsar åtgärden. Vid utformningen av en sådan definition är det naturligt att dels inspireras av utformningen av definitioner för andra hemliga tvångsmedel, dels knyta an till straffbestämmelsen om dataintrång, vilken ju begränsar möjligheten att använda tekniker för hemlig dataavläsning i dag.

Ett gemensamt drag i definitionerna för andra hemliga tvångsmedel är att samtliga slår fast vad objektet för åtgärden är, dvs. de uppgifter som åtgärden får användas för att hämta in. Vid exempelvis hemlig avlyssning av elektronisk kommunikation är objektet innehållet i meddelanden. När det gäller hemlig dataavläsning kommer åtgärden vara en metod för att hämta in olika typer av uppgifter, se avsnitt 10.3. Samtliga uppgiftstyper måste därför täckas in i det begrepp som används för att beskriva objektet för hemlig dataavläsning.

I brottsbalkens bestämmelse om dataintrång används begreppet *uppgift som är avsedd för automatiserad behandling* för att beskriva vilka uppgifter som omfattas av bestämmelsen. När lydelsen infördes i 4 kap. 9 c § brottsbalken angavs bl.a. följande i förarbetena. Avsikten med det nya begreppet "uppgift som är avsedd för automatiserad behandling" är att förtydliga att alla uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form omfattas av bestämmelsen. I detta ligger att även program av olika slag omfattas. Det är för tillämpningen av begreppet utan betydelse var uppgifterna finns eller förvaras i systemet. Det innebär att alla uppgifter oavsett på vilket datamedium de finns omfattas. Därmed innefattas också uppgifter som finns i en dators temporära minne. Det innebär vidare att uppgifter som är under befordran omfattas. Det senare gäller oavsett på vilket sätt befordran sker.[2]

Mot bakgrund av att hemlig dataavläsning kommer att utgöra ett undantag från dataintrångsbestämmelsen och att begreppet *uppgift som är avsedd för automatiserad behandling* torde täcka samtliga de uppgiftstyper som kan aktualiseras vid hemlig dataavläsning framstår det som lämpligt att använda samma begrepp i den nya lagen. Lydelsen ger således en klar koppling mellan hemlig dataavläsning

[2] Prop. 2006/07:66 s. 49.

och bestämmelsen om dataintrång. Den tydliggör dessutom på ett teknikneutralt och ändamålsenligt vis vilka uppgifter åtgärden får användas för att hämta in.

Objektet består också av själva inhämtandet av uppgifterna. Denna process beskrivs på olika sätt i definitionerna för de gällande hemliga tvångsmedlen. I bestämmelsen om hemlig avlyssning av elektronisk kommunikation anges t.ex. att meddelanden i hemlighet *avlyssnas eller tas upp*, se 27 kap. 18 § rättegångsbalken. Hemlig dataavläsning kommer kunna innebära en rad olika typer av inhämtning, t.ex. avlyssning, övervakning och inhämtning. Som ett samlingsbegrepp bör *avläsning* användas. Det bör, liksom vid hemlig avlyssning av elektronisk kommunikation också anges att uppgifterna får *tas upp* för att tydliggöra att det inte endast är i realtid som granskning av uppgifterna får ske.

10.2.2 Metoden och hemlighållandet av åtgärden

Redan i beskrivningen av vad hemlig dataavläsning är bör det anges hur avläsningen (eller upptagningen) går till. Eftersom det inte är fråga om någon enhetlig teknisk metod och det dessutom kan tänkas att olika tekniker kan komma att utvecklas bör i lagstiftningen ett teknikneutralt begrepp väljas. Att ange att den brottsbekämpande myndigheten får läsa av eller ta upp uppgifterna med ett *tekniskt hjälpmedel* framstår som ändamålsenligt. Redan 1995 förklarade regeringen i en proposition att detta begrepp avser såväl hårdvara som programvara.[3]

Det säger sig självt att hemlig dataavläsning är en åtgärd som, när den utförs, ska ske utan att den enskilde mot vilken den riktas känner till detta. Av denna anledning behöver det i definitionen av åtgärden framgå att den ska ske i hemlighet.

[3] Prop. 1994/95:227 s. 29.

10.2.3 Det är uppgifter i ett informationssystem som åtgärden ska avse

Det bör också av definitionen av hemlig dataavläsning framgå var de uppgifter som ska läsas av ska finnas. Av direktiven framgår att åtgärden är tänkt att riktas mot ”en dator eller annan teknisk utrustning som används för kommunikation”. Begreppet utrustning, utan annan förklaring, leder tankarna till fysiska ting. Typiskt sett är det nog också uppgifter i fysisk utrustning som det kommer att bli aktuellt att rikta åtgärden mot. Emellertid står det klart att även icke fysisk utrustning, t.ex. ett användarkonto till en kommunikations- eller lagringstjänst på internet, kan vara av mycket stort intresse i den brottsbekämpande verksamheten. I Norge är det möjligt att använda hemlig dataavläsning inte bara avseende fysisk utrustning utan också mot uppgifter som finns tillgängliga via sådana konton. Eftersom det bör vara behovet av uppgifterna, snarare än var och hur de lagras, som ligger till grund för hur hemlig dataavläsning avgränsas finns inget egentligt skäl till att inte tillåta avläsning av uppgifter som finns tillgängliga via användarkonton (se dock diskussionen om jurisdiktion i nästa kapitel). Vårt förslag innebär därför att hemlig dataavläsning ska få användas även beträffande sådana uppgifter. Mot den bakgrunden behövs ett annat begrepp än *dator eller teknisk utrustning som används för kommunikation*. Beredningen för rättsväsendets utveckling (BRU) använde i sitt förslag till hemlig dataavläsning (SOU 2005:38) begreppet informationssystem. Som skäl för det begreppet anförde BRU bl.a. att informationssystem används i många författningar och i andra sammanhang utan att det kan sägas finnas någon vedertagen definition och att begreppet täcker in de informationsmöjligheter och informationsvägar som finns nu och som kommer att finnas i framtiden.[4]

Vad BRU anförde har fortfarande skäl för sig och informationssystem framstår även i övrigt som ett lämpligt begrepp att använda. Det finns dock anledning att i definitionen av hemlig dataavläsning avgränsa vad som ska avses med informationssystem, bl.a. för att minska risken för tillämpningsglidningar. En sådan avgränsning kan dessutom förenkla för den som ska tillämpa lagstiftningen eftersom den blir en utgångspunkt vid tolkningen av reglerna. Därigenom kan

[4] SOU 2005:38 s. 419.

en avgränsning i viss mån tillgodose att riskerna för den personliga integriteten inte blir större än vad som är absolut nödvändigt.

Informationssystem kan vara antingen elektronisk kommunikationsutrustning…

Informationssystem av fysisk karaktär kan vara t.ex. datorer, mobiltelefoner, surfplattor, smarta armbandsur och servrar. Vid bedömningen av vad som bör framgå i lagtext kan man först konstatera att de nämnda exemplen, enligt en rent tekniskt språklig analys torde falla in under begreppet dator. En dator är en ”programstyrd anordning för bearbetning och hantering av data” eller en ”programstyrd digital maskin för matematiska och logiska beräkningar”.[5]

Begreppet *dator och liknande utrustning* skulle således kunna användas för att avgränsa vad som utgör informationssystem i lagens mening. Det finns emellertid redan i dag ett begrepp i reglerna om tvångsmedel som torde motsvara det som avses, nämligen elektronisk kommunikationsutrustning. Det begreppet används både i bestämmelserna om hemliga tvångsmedel, se t.ex. 27 kap. 19 § rättegångsbalken och 1 § inhämtningslagen, och i andra sammanhang under förundersökning, se t.ex. 23 kap. 9 a § rättegångsbalken. När det senare lagrummet infördes klargjordes att med elektronisk kommunikationsutrustning avses all slags utrustning som kan användas för att kommunicera elektroniskt.[6] Begreppet, med den innebörden, bör därför lämpligen användas i definitionen för att beskriva vad ett informationssystem i lagens mening kan vara när det är fråga om fysisk utrustning. Uttrycket är teknikneutralt på ett sätt som gör att även framtida teknisk utrustning som kan användas för elektronisk kommunikation kommer att omfattas av det. Samtidigt avgränsar det användningsområdet för hemlig dataavläsning så att om ny teknik inte kan anses rymmas i begreppet får åtgärden inte användas i utrustningen.

[5] Definitionerna är hämtade från Svenska datatermgruppens ordlista, www.datatermgruppen.se/ordlista.html respektive webbsidan it-ords definition, https://it-ord.idg.se/ord/dator/
[6] Se prop. 2015/16:68 s. 74.

… eller användarkonton till vissa tjänster

Även beträffande uppgifter i informationssystem som inte är elektronisk kommunikationsutrustning bör det alltså finnas en möjlighet att tillåta hemlig dataavläsning. De informationssystem som det är fråga om är främst internetbaserade kommunikations- eller lagringstjänster. Naturligtvis är dessa informationssystem uppbyggda genom fysisk utrustning och infrastruktur som den som tillhandahåller tjänsterna förfogar över. Det är dock vare sig utrustning eller infrastruktur som är av relevans här. I stället är det den enskildes användande av själva tjänsterna. Givetvis måste de brottsbekämpande myndigheternas tillgång till uppgifter i sådana tjänster därför begränsas till endast de delar av informationssystemet som den som utsätts för åtgärden har behörighet till. I Norge 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. I motiven till de norska reglerna anfördes bl.a. följande i detta sammanhang.

> Hver bruker har et virtuelt avgrenset område som er identifisert ved et brukernavn, og som kan benyttes fra et hvilket som helst passende datasystem med nødvendig nettverksforbindelse og programvare, ved å oppgi brukernavnet og som regel et passord eller en annen form for tilgangskode. Dersom mistenkte bruker slike tjenester via mange ulike nettverkstilkoblinger (for eksempel trådløse internettsoner) og flere forskjellige datasystemer, kan politiet være avskåret fra effektiv kontroll gjennom dataavlesing rettet mot bestemte datasystemer. Politiet bør derfor ha en viss adgang til å gjøre seg kjent med mistenktes bruk av en slik brukerkonto, uavhengig av hvilke datasystemer den mistenkte benytter for å skaffe seg tilgang til kontoen. Avlesing som begrenser seg til en bestemt brukerkonto kan også være mindre inngripende enn avlesing av for eksempel all aktivitet på en datamaskin.[7]

Vad som anfördes i det citerade uttalandet gäller i lika hög grad vid införande av hemlig dataavläsning i Sverige. Hemlig dataavläsning bör därför, när de relevanta uppgifterna finns i sådana tjänster som här diskuteras, endast få avse det som är virtuellt avgränsat till den enskilde användaren. Det bör kunna uttryckas som att med infor-

[7] Se den norska propositionen Prop. 68 L (2015-2016) s. 270.

mationssystem avses ett användarkonto eller en på motsvarande sätt avgränsad del av en viss tjänst.

De tjänster som kan vara relevanta vid hemlig dataavläsning bör avgränsas till kommunikations- och lagringstjänster och liknande tjänster. Kommunikationstjänster bör innefatta sådana tjänster som avses med elektroniska kommunikationstjänster i 1 kap. 7 § lagen om elektronisk kommunikation men även kommunikationstjänster som inte ryms i det begreppet. Exempel på kommunikationstjänster kan vara webbmejl-, samtals- och andra meddelandetjänster.

För lagringstjänster finns inte någon sådan legaldefinition som finns för elektroniska kommunikationstjänster. Vad det är fråga om är emellertid tjänster som möjliggör lagring av data och information 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 detta inte är det primära syftet med tjänsten. 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. Ett tillägg avseende liknande tjänster som kommunikations- och lagringstjänster bör därför göras i definitionen av vad ett informationssystem kan vara.

10.3 Vilka uppgiftstyper får hemlig dataavläsning omfatta?

Utredningens förslag: Hemlig dataavläsning får användas 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 första punkten,
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 informationssystemet används men inte avses i 1–6.

Åtgärden får endast användas efter tillstånd enligt lagen. När det är fråga om att använda hemlig dataavläsning för att läsa av eller ta upp uppgifter enligt punkterna 1 eller 2 får meddelanden hindras från att nå fram.

Eftersom hemlig dataavläsning kan användas för att läsa av eller ta upp en rad olika typer av uppgifter föreslår vi att en uttrycklig regel förs in i den nya lagen som klargör vilka uppgifter hemlig dataavläsning kan få användas för att läsa av eller ta upp.[8] Den föreslagna bestämmelsen är central för lagen om hemlig dataavläsning eftersom den blir utgångspunkt i varje enskilt fall när det ska bestämmas vilka uppgifter som ska få läsas av eller tas upp. Det är alltså inte fråga om en katalog med uppgiftstyper som alltid får läsas av eller tas upp när ett tillstånd till hemlig dataavläsning har beslutats utan bedömningen av vilka uppgiftstyper som får läsas av eller tas upp görs alltid i det enskilda fallet, se vidare i avsnitt 10.9.4.

10.3.1 Hemlig dataavläsning för att ”verkställa” andra hemliga tvångsmedel

Mot bakgrund av att vi i vår behovsanalys kommit fram till att det finns ett tungt vägande behov av nya metoder för att komma åt sådana uppgifter som får hämtas in med gällande hemliga tvångsmedel bör det klargöras att hemlig dataavläsning får användas för att läsa av eller ta upp motsvarande uppgifter som kan hämtas in med de tvångsmedlen. De uppgifter som avses kan således ge tillgång till följande information.

[8] Jfr t.ex. SOU 2012:44 s. 767 där Utredningen om vissa hemliga tvångsmedel, beträffande det tidigare förslaget om hemlig dataavläsning (SOU 2005:38), anförde att ”avgränsningen av vilken informationsinhämtning som får ske inte är helt klar”.

1. Historiskt innehåll och realtidsinnehåll i meddelanden, vilket 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, vilket motsvarar uppgifter som kan hämtas in genom hemlig övervakning av elektronisk kommunikation och genom inhämtning enligt inhämtningslagen (kommunikationsövervakningsuppgifter).
3. Historiska uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits, vilket motsvarar uppgifter som kan hämtas in genom hemlig övervakning av elektronisk kommunikation och genom inhämtning enligt inhämtningslagen (lokaliseringsuppgifter).
4. Realtidsuppgifter som innebär optisk personövervakning, vilket motsvarar uppgifter som kan hämtas in genom hemlig kameraövervakning (kameraövervakningsuppgifter).
5. Realtidsuppgifter som avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till, vilket motsvarar uppgifter som kan hämtas in genom hemlig rumsavlyssning (rumsavlyssningsuppgifter).

Åtgärden kan, när den används för att läsa av eller ta upp någon av de nämnda uppgifterna, i praktiken jämföras med ett sätt att verkställa andra hemliga tvångsmedel. Det bör framhållas att den möjlighet som finns enligt 27 kap. 19 § första stycket 2 rättegångsbalken och 1 § 2 inhämtningslagen att hämta in lokaliseringsuppgifter avseende vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område inte finns med bland de uppräknade uppgifterna. Det hänger samman med att de uppgifterna hämtas in efter s.k. basstationstömningar. Hemlig dataavläsning ska riktas mot enskilda informationssystem och kan således inte ge motsvarande information.

När ett tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation har meddelats får åtgärderna enligt 27 kap. 19 § andra stycket rättegångsbalken användas för att hindra med-

delanden från att nå fram. Motsvarande rätt bör, mot bakgrund av att det i praktiken är fråga om att verkställa dessa åtgärder, tillkomma de brottsbekämpande myndigheterna när tillstånd till hemlig dataavläsning har meddelats för att läsa av eller ta upp kommunikationsavlyssnings- eller kommunikationsövervakningsuppgifter.

10.3.2 Hemlig dataavläsning för avläsning eller upptagning av andra uppgifter

Av vår behovsanalys framgår också att det finns tungt vägande behov av nya åtgärder för att de brottsbekämpande myndigheterna i hemlighet ska kunna bereda sig tillgång även till elektroniskt lagrade uppgifter och uppgifter som visar hur informationssystemet används i realtid. Det bör därför framgå att uppgifter som finns elektroniskt lagrade i ett informationssystem ska få läsas av eller tas upp. För att tydligt skilja de olika informationstyperna åt, vilket är en förutsättning för bl.a. vårt förslag om anpassning av verkställighetsteknik som en särskild åtgärd för att minska riskerna för integritetsintrång (se avsnitt 10.10.2), bör det framgå att det är elektroniskt lagrade uppgifter som inte får hämtas in med nuvarande hemliga tvångsmedel som avses. De uppgifter som kan träffas är således exempelvis uppgifter som lagrats i filer, såsom bilder, dokument och ljudklipp. Även uppgifter som lagras i ett temporärt minne kan avses.

Det bör också framgå att hemlig dataavläsning får användas för att läsa av eller ta upp uppgifter som visar hur ett informationssystem används. Med detta avses realtidsuppgifter om vad en användare av ett informationssystem använder detta till. Det blir således fråga om en slags realtidsövervakning av själva informationssystemet. Exempel på sådana uppgifter som avses kan vara vilka program eller appar som körs, elektroniska anteckningar som görs men inte sparas och hur informationssystemet i andra avseenden används. Eftersom uppgifter om hur ett informationssystem används skulle kunna ge mycket omfattande information som innefattar sådana uppgifter som nämnts i det föregående bör motsvarande avgränsning som för lagrade uppgifter göras.

10.3.3 Hemlig dataavläsning får endast användas efter tillstånd

Som framgått kan hemlig dataavläsning användas för att komma åt samma uppgifter som får hämtas med andra hemliga tvångsmedel. För att tydliggöra att tekniken för hemlig dataavläsning inte får användas som rena verkställighetsmetoder för dessa tvångsmedel, vilket utifrån t.ex. ordalydelsen i 27 kap. 25 § rättegångsbalken inte framstår som helt uteslutet (jfr dock avsnitt 4.3.4), bör det framgå direkt av lagtexten att det krävs tillstånd enligt lagen för att hemlig dataavläsning ska få användas.

10.4 Proportionalitet och behov m.m.

Utredningens förslag: En bestämmelse om att proportionalitetsprincipen gäller tas in i lagen om hemlig dataavläsning.

10.4.1 De allmänna principerna vid all tvångsmedelsanvändning

För all tvångsmedelsanvändning gäller tre allmänna principer. De tre principerna, som anknyter till innehållet i 2 kap. 6 § regeringsformen, är ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. 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. 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. Proportionalitetsprincipen har lagfästs bl.a. i 27 kap. 1 § tredje stycket rättegångsbalken men gäller, liksom de andra två principerna, vid all tvångsmedelsanvändning även om det inte framgår av lag.

10.4.2 Proportionalitetsprincipen bör lagfästas i lagen om hemlig dataavläsning

Det finns inget skäl att inte redovisa proportionalitetsprincipen direkt i lagtext. Så sker i snart sagt all tvångsmedelslagstiftning. Mot bakgrund av de särskilda risker för integritet och informationssäkerhet som föreligger med hemlig dataavläsning framstår det som särskilt viktigt att principen får en framträdande plats även i lagen om hemlig dataavläsning, trots att den ju gäller oavsett om den finns uttryckt i skrift eller inte.

Det bör beträffande proportionalitetsavvägningen särskilt framhållas vikten av att noggrant pröva samtliga omständigheter och väga de som talar för, mot de som talar emot att tillåta hemlig dataavläsning i det enskilda fallet. Denna prövning kan leda till att en åtgärd inte tillåts trots att de krav som lagen i övrigt uppställer är uppfyllda.

I frågan om hemlig dataavläsning ska tillåtas i ett enskilt fall kan proportionalitetsprincipen få särskild betydelse när en ansökan avser flera uppgiftstyper. Så är fallet redan i dag när en ansökan avser flera olika hemliga tvångsmedelsåtgärder. Ju fler tvångsmedelsåtgärder eller uppgiftstyper som en ansökan avser, desto större blir integritetsriskerna för den enskilde. Domstolen måste vid sin tillståndsprövning i ärenden om hemlig dataavläsning alltså, utöver andra omständigheter som åberopas i det enskilda fallet, ställa sig frågan om det är proportionerligt att tillåta avläsning eller upptagning av flera olika uppgiftstyper. Endast undantagsvis, i de allra allvarligaste fallen, bör det vara möjligt att få tillstånd till avläsning eller upptagning av samtliga uppgiftstyper samtidigt.

Också frågor om informationssäkerhet och företagshemligheter kan få stor betydelse vid den prövning av åtgärdens proportionalitet som ska göras. Även om vi föreslår regler för att begränsa risker på de områdena ingår det i rättens proportionalitetsprövning att väga in 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 bör innebära att även om det inte är formellt uteslutet med hemlig dataavläsning avseende sådana uppgifter så kan åtgärden vara utesluten eller behöva begränsas till sin omfattning efter en strikt prövning av proportionalitetsprincipen.

Sin kanske allra största betydelse torde proportionalitetsprincipen dock få vid en prövning av om hemlig dataavläsning ska få avse uppgifter i informationssystem som används av någon som inte är misstänkt för brott. Hemlig dataavläsning avseende uppgifter i informationssystem som används av någon som inte är misstänkt ska redan enligt de regler vi föreslår i det följande få förekomma endast i undantagsfall. Även om uppgiftstyperna som får läsas av eller tas upp i de fallen är begränsade så är de tillkommande riskerna med hemlig dataavläsning jämfört med när motsvarande uppgifter får hämtas in med befintliga hemliga tvångsmedel betydande, särskilt såvitt avser informationssäkerhetsaspekter. Det påkallar att restriktivitet iakttas i samband med proportionalitetsprövningen, utöver den restriktivitet som ska gälla enligt den bestämmelse prövningen görs mot, för att hemlig dataavläsning endast i de allra allvarligaste fallen ska få avse uppgifter i informationssystem som används av annan än en misstänkt person. Åtgärden bör dock inte vara helt utesluten; t.ex. i fall när det finns underrättelser om förestående terroristbrottslighet eller annan brottslighet som Säkerhetspolisen har ansvar för att förebygga och förhindra. Också i vissa förundersökningssituationer beträffande sådan brottslighet och beträffande grovt organiserad brottslighet kan det tänkas vara både nödvändigt och proportionerligt att i vissa fall använda hemlig dataavläsning mot sådana personer för att komma åt den misstänkte.

Som en utgångspunkt för proportionalitetsprövningen bör gälla att hemlig dataavläsning för en viss uppgiftstyp endast är proportionerlig om andra åtgärder för att komma åt uppgifterna som eftersöks inte är tillräckliga, skulle vara väsentligt svårare att genomföra än vad hemlig dataavläsning kan förväntas vara eller kan förväntas leda till större integritetsintrång än vad hemlig dataavläsning kan förväntas göra.

10.5 Hemlig dataavläsning under en förundersökning

10.5.1 Några utgångspunkter

Utredningens bedömning: För hemlig dataavläsning i syfte att läsa av eller ta upp uppgifter som får hämtas in med andra 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 som utgångspunkt motsvarande krav för tillstånd gälla som gäller för tillstånd till hemlig avlyssning av elektronisk kommunikation. Vissa undantag från de nämnda utgångspunkterna bör dock göras.

Vid utformningen av regler som anger vilka förutsättningar som ska gälla för hemlig dataavläsning finns det anledning att dels göra en jämförelse med de krav som ställs vid övriga hemliga tvångsmedel, dels jämföra med vilka möjligheter som finns att komma åt uppgifterna på annat sätt än genom hemliga tvångsmedel i dag och de krav som då ställs. Dessutom måste givetvis riskerna för den personliga integriteten som avläsningen kan innebära beaktas vid bestämmande av vilka förutsättningar som ska föreligga för att åtgärden ska få aktualiseras.

I avsnitt 10.3 framgår vilka olika uppgiftstyper som ett tillstånd till hemlig dataavläsning kan tillåta avläsning eller upptagning av. Uppgiftstyperna består av dels uppgifter som får hämtas in med de nu gällande reglerna om hemliga tvångsmedel, dels uppgifter som inte får hämtas in med hemliga tvångsmedel. I de förstnämnda delarna har hemlig dataavläsning närmast karaktären av verkställighetsmetod för de gällande hemliga tvångsmedlen. Om inte annat är särskilt påkallat bör därför som en utgångspunkt de krav, avseende exempelvis vilka brott som kan föranleda åtgärden, som gäller för de befintliga hemliga tvångsmedlen gälla även vid hemlig dataavläsning.

När det gäller de delar av hemlig dataavläsning som inte motsvaras av något gällande hemligt tvångsmedel konstaterade vi i föregående kapitel att det utgör en visst ökad integritetsrisk att brottsbekämpande myndigheter kan ta del av uppgifterna efter användande av hemlig dataavläsning jämfört med dagens förhållanden. Bedömningen där var dock generell. Här är det i stället fråga om att i integritetsriskhänseende jämföra hemlig dataavläsning i det aktuella avseendet med andra hemliga tvångsmedel för att bestämma hur en reglering av åtgärden bör utformas.

Jämförelse med andra hemliga tvångsmedel

Bland de nuvarande hemliga tvångsmedlen ställs, beträffande brott som kan leda till användning av dessa, högst krav beträffande hemlig rumsavlyssning. Det hänger enligt förarbetena samman med det tvångsmedlets särskilt ingripande karaktär, som föranledde regeringen att uttala att det fanns starka skäl att vara synnerligen restriktiv beträffande när åtgärden skulle få användas.[9] Av de tvångsmedel som riktas mot elektronisk kommunikation anses hemlig övervakning av elektronisk kommunikation medföra ett klart mindre integritetsintrång än hemlig avlyssning av elektronisk kommunikation, eftersom det förstnämnda tvångsmedlet inte ger uppgifter om innehållet i samtal eller meddelanden.[10] Det har föranlett att hemlig övervakning av elektronisk kommunikation kan användas vid betydligt fler brott, och vid brott av mindre allvarlig beskaffenhet, än hemlig avlyssning av elektronisk kommunikation, se 27 kap. 18 och 19 §§ rättegångsbalken. Hemlig kameraövervakning och hemlig avlyssning av elektronisk kommunikation har – trots att metoderna är mycket olika varandra och därmed svåra att jämföra – ansetts medföra integritetsintrång på typiskt sett likvärdiga nivåer och har därför samma brottskataloger.[11]

När Utredningen om vissa hemliga tvångsmedel redovisade sin utvärdering av de hemliga tvångsmedlen år 2012 konstaterades att inget kommit fram vid utredningens omfattande kartläggning som talade mot att det ovan anförda typiskt sett gäller. Utredningen framhöll dock följande.

> Samtidigt måste betonas att vilket tvångsmedel som vid tillämpningen är det mest kännbara från integritetssynpunkt alltid beror av omständigheterna i det enskilda fallet. En hemlig rumsavlyssning av ett möte på en restaurang kan t.ex. från integritetssynpunkt vara avsevärt lindrigare än teleavlyssning av en bostadstelefon som pågår under en längre tid.[12]

Mot bakgrund av att brottsbekämpande myndigheter redan i dag i ett så tidigt skede som vid husrannsakan kan få rätt att ta del av elektroniskt lagrade uppgifter kan åtgärden, trots att den vid hemlig dataavläsning sker i hemlighet för den som utsätts för den, enligt vår

[9] Prop. 2005/06:178 s. 51.
[10] Se t.ex. prop. 2002/03:74 s. 23 f.
[11] Prop. 1995/96:85 s. 21 f.
[12] SOU 2012:44 s. 515.

mening inte anses som lika ingripande som hemlig rumsavlyssning. Det talar med styrka emot att använda sig av lika höga skyddsnivåer för den enskilde som vid det tvångsmedlet. Hemlig dataavläsning, som ju i detta sammanhang ger tillgång till innehållsuppgifter som många gånger kan förväntas vara av känslig karaktär, utgör inte heller ett så begränsat intrång som hemlig övervakning av elektronisk kommunikation ansetts medföra. Det talar med styrka emot att använda sig av de skyddsnivåer som tillämpas vid den åtgärden. Dessutom talar direktivens ordalydelse emot att tillämpa de, i sammanhanget, lägre skyddsnivåer som gäller för hemlig övervakning av elektronisk kommunikation.

Vid en samlad bedömning framstår det som att integritetsrisken vid hemlig dataavläsning för att läsa av eller ta upp lagrade uppgifter eller uppgifter som visar hur ett informationssystem används motsvarar den risk som gäller vid hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. Det framstår därför som ändamålsenligt att låta de skyddsnivåer som gäller för de åtgärderna gälla även för hemlig dataavläsning.

10.5.2 Vid vilka brott ska hemlig dataavläsning få användas?

Utredningens förslag: Hemlig dataavläsning får aldrig användas vid förundersökning om annat brott än sådant som kan föranleda tillstånd till hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § rättegångsbalken. När hemlig dataavläsning ska användas för att läsa av eller ta upp rumsavlyssningsuppgifter krävs att det är fråga om brott som kan föranleda tillstånd till hemlig rumsavlyssning.

Nyss har vi sagt att en utgångspunkt ska vara att när hemlig dataavläsning används för att läsa av eller ta upp uppgifter som får hämtas in genom andra hemliga tvångsmedel så ska de krav som gäller för de ”bakomliggande” hemliga tvångsmedlen gälla även vid hemlig dataavläsning. En annan utgångspunkt är att det enligt direktiven ligger i vårt uppdrag att undersöka om hemlig dataavläsning kan tillåtas för brott som i dag kan föranleda hemlig avlyssning av elektronisk kommunikation. När oförenlighet råder mellan dessa två utgångspunkter bör den senare ha företräde. Det kan motiveras av att metoden för

hemlig dataavläsning i sig anses innebära en ökad risk för den personliga integriteten och informationssäkerheten. När det således gäller avläsning eller upptagning av kommunikationsövervakningsoch lokaliseringsuppgifter, dvs. uppgifter som i dag får hämtas in genom hemlig övervakning av elektronisk kommunikation bör kravet för hemlig dataavläsning således sättas högre än vad som gäller för inhämtning av uppgifterna enligt nuvarande regler. För avläsning eller upptagning av sådana uppgifter, liksom för kommunikationsavlyssnings- och kameraövervakningsuppgifter samt lagrade uppgifter och uppgifter som visar hur ett informationssystem används, bör därför de brott som kan föranleda tillstånd till hemlig avlyssning av elektronisk kommunikation krävas. Det bör alltså framgå av lagen om hemlig dataavläsning att åtgärden inte får användas vid förundersökning om andra brott än sådana som kan aktualisera det tvångsmedlet.

När det däremot gäller hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter bör kraven beträffande vilka brott som kan föranleda åtgärden sättas lika högt som vid hemlig rumsavlyssning. Det hänger samman med att hemlig dataavläsning då i det närmaste är ett sätt att verkställa hemlig rumsavlyssning och att de brott som kan föranleda den åtgärden är betydligt allvarligare, se 27 kap. 20 d § rättegångsbalken.

10.5.3 Brottsmisstankens styrka och behovet av åtgärden

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

När det gäller brottsmisstankens styrka kan till en början konstateras att samma krav, skälig misstanke, gäller för samtliga nuvarande hemliga tvångsmedel under förundersökning. Som en undantagsregel gäller emellertid för hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning att de under vissa förhållanden får genomföras även utan krav på en skäligen misstänkt person, se om detta vid hemlig dataavläsning i avsnitt 10.5.5.

Misstankegraden skälig misstanke används också vid t.ex. reseförbud, anhållande och s.k. utredningshäktning. Den ställer högre

krav på misstankens styrka än vad som avses med uttrycket att en person "kan misstänkas" för brott men innebär ett lägre krav än ”sannolika skäl”. Det har anförts att en högre grad av brottsmisstanke än skäligen misstänkt skulle innebära att hemliga tvångsmedel i princip skulle komma att sakna betydelse i den brottsutredande verksamheten.[13] Det hänger samman med att ett krav på exempelvis sannolika skäl, som bland annat används vid häktning, innebär att den mesta bevisningen redan är säkrad medan hemliga tvångsmedel typiskt sett används för att samla in uppgifter som kan leda till att misstankegraden når upp till sannolika skäl. Att använda ett högre krav än skäligen misstänkt framstår därför inte som ändamålsenligt. Mot bakgrund av hur frågan om misstankegrad är reglerad för övriga hemliga tvångsmedel och den integritetsrisk som åtgärden innebär framstår det inte heller som lämpligt att välja ett lägre krav i detta fall, jfr prop. 1988/89:124 s. 43 f. och 1995/96:85 s. 28. Åtgärden bör därför få användas om någon är skäligen misstänkt för ett brott som angetts i föregående avsnitt. Kravet bör gälla för samtliga uppgiftstyper som hemlig dataavläsning kan användas för att läsa av eller ta upp.

När det sedan gäller behovet av åtgärden gäller för samtliga nuvarande hemliga tvångsmedel att dessa endast får användas om åtgärden är av synnerlig vikt för utredningen. Begreppet "synnerlig vikt för utredningen" har definierats vid ett flertal tillfällen i fråga om användning av tvångsmedel. I dessa sammanhang har man ofta återkommit till vad regeringen anförde i samband med införandet av hemlig teleavlyssning och hemlig teleövervakning i rättegångsbalken år 1989. Eftersom dessa uttalanden fortfarande torde äga giltighet finns skäl att här citera delar av vad som där angavs, se prop. 1988/89:124 s. 44 f.

> Uttrycket synnerlig vikt för utredningen behöver inte nödvändigtvis avse att avlyssningen skall ge avgörande bevisning som omedelbart kan leda till fällande dom. I de flesta fall har telefonavlyssning en indirekt verkan: den bidrar till att kartlägga kontaktvägar och förehavanden, ger uppslag till vidare spaning och bildar underlag för andra åtgärder. En annan […] förekommande verkan är att avlyssningen kan föra en på olika sätt uppkommen misstanke till nolläget, dvs. rentvå den misstänkte.
>
> Synnerlig vikt för utredningen inrymmer ett kvalitetskrav beträffande de upplysningar som avlyssningen kan ge. Dessa får sålunda inte

[13] Se t.ex. SOU 1998:46 s. 389 f.

> inskränka sig till obetydliga detaljer, som man kan både ha och mista. Uttrycket innefattar emellertid därutöver ett krav på att utredningsläget gör avlyssningen nödvändig. Vad som kan vinnas genom åtgärden får i princip inte vara åtkomligt med andra, mindre ingripande metoder. En slentrianmässig bedömning får inte förekomma i fråga om vare sig utredningsläget eller de andra förutsättningarna som gäller för tvångsmedlet. En granskning av utredningsmöjligheterna i det enskilda fallet måste alltid verkställas. Granskningen måste mynna ut i bedömningen att utredningen i princip inte kan föras framåt med andra medel och att det finns skäl att räkna med att avlyssningen – ensam eller i förening med andra åtgärder – verkligen kan få effekt.
>
> I och för sig behöver något absolut hinder inte föreligga mot att få fram information på andra vägar. Det krävs dock att hindret är sådant att det inte skäligen kan begäras att man skall avstå från teleavlyssning. Kan personlig övervakning (skuggning) eller andra åtgärder användas som alternativ, bör det ändå vara tillåtet med teleavlyssning, om alternativen skulle kräva en orimligt hög personalinsats eller vara förenade med avsevärd risk att den pågående utredningen avslöjas för tidigt. Utgångspunkten bör dock vara att i första hand pröva andra metoder.

Enligt vår mening är det naturligt att samma krav, "synnerlig vikt för utredningen", uppställs som villkor för användningen av hemlig dataavläsning som för nuvarande hemliga tvångsmedel. Vi kan inte se att kravet skulle vara för lågt i förhållande till t.ex. integritetsrisker eller för högt i förhållande till brottsbekämpningens effektivitetsintresse. Kravet förefaller, såvitt känt, inte heller ha föranlett några särskilda tillämpningsproblem. Om så ändå skulle vara fallet bör de nyss återgivna uttalandena i allt väsentligt kunna vara vägledande för hur uttrycket synnerlig vikt för utredningen bör uppfattas vid prövning av ärenden om hemlig dataavläsning. Vi föreslår därför att hemlig dataavläsning endast ska få användas om det är av synnerlig vikt för utredningen.

Vid bedömningen av om det är av synnerlig vikt att hemlig dataavläsning ska få användas i ett enskilt fall bör själva metoden för uppgiftsinhämtningen få en särskilt framträdande plats. Riskerna för informationssäkerheten som finns med metoden, jämfört med vad som gäller för de metoder som får användas för att hämta in motsvarande uppgifter i dag, talar för att åtgärden endast bör få användas när andra metoder inte är tillräckliga, är svårare att genomföra än hemlig dataavläsning eller förväntas leda till större integritetsintrång.

Exempel på när andra metoder inte är tillräckliga är då de inte förväntas ge önskat resultat, t.ex. när kommunikation förväntas vara krypterad så att traditionella metoder för hemlig avlyssning eller

övervakning av elektronisk kommunikation inte ger uppgifter i klartext eller när den elektroniska kommunikationsutrustning som används är krypterad och därför inte kommer kunna undersökas om den inte är upplåst när den tas i beslag. Exempel på när det är väsentligt svårare att genomföra en annan åtgärd än hemlig dataavläsning kan vara att ett utrymme där hemlig rumsavlyssning ska genomföras aldrig lämnas obevakat eller den plats som hemlig kameraövervakning ska ske på inte ger möjlighet att fästa kamerautrustningen någonstans. Det kan inte heller uteslutas att hemlig dataavläsning vid en sammanvägd bedömning faktiskt kan innebära ett förväntat mindre integritetsintrång än andra åtgärder.

10.5.4 Platskrav vid avläsning eller upptagning av kameraövervaknings- eller rumsavlyssningsuppgifter

Utredningens förslag: Motsvarande platskrav som gäller vid hemlig kameraövervakning och hemlig rumsavlyssning ska gälla när hemlig dataavläsning används för att läsa av eller ta upp kameraövervaknings- respektive rumsavlyssningsuppgifter.

Avläsning eller upptagning av kameraövervaknings- eller rumsavlyssningsuppgifter kan ske efter att den brottsbekämpande myndigheten har aktiverat funktionalitet i ett informationssystem, se avsnitt 10.10.1. Sådan funktionalitet kan exempelvis vara en mobiltelefons kamera eller mikrofon.

I föregående kapitel har vi kommit fram till att kravet på plats vid tillståndsgivning till hemlig dataavläsning för att läsa av eller ta upp rumsavlyssnings- eller kameraövervakningsuppgifter bör vara detsamma som gäller i dag för hemlig rumsavlyssning respektive hemlig kameraövervakning. Den slutsatsen stämmer väl överens med utgångspunkten i avsnitt 10.5.1 att kraven för hemlig dataavläsning ska motsvara kraven för tillstånd till det ”bakomliggande” tvångsmedlet.

När det gäller platskravet för hemlig kameraövervakning kan detta sägas bestå av två delar.[14] Den första delen, som framgår ut-

[14] Vi bortser här från att hemlig kameraövervakning enligt 27 kap. 20 c § rättegångsbalken får användas för att övervaka den plats där brottet har begåtts eller en nära omgivning till en

tryckligen av 27 kap. 20 b § rättegångsbalken, är att åtgärden endast får avse en sådan plats där den misstänkte kan antas komma att uppehålla sig. Motsvarande krav bör införas i lagen om hemlig dataavläsning beträffande avläsning eller upptagning av kameraövervakningsuppgifter. Den andra delen, som framgår uttryckligen av förarbetena (se t.ex. prop. 1995/96:85 s. 30 och prop. 2013/14:237 s. 154 f,) och indirekt av lagstiftningen[15], är att det inte är tillåtet att övervaka någon som befinner sig i en stadigvarande bostad med en kamera som finns i den bostaden. Detta har motiverats med de mycket betydande integritetsintrång sådan övervakning skulle kunna medföra. Eftersom det vore möjligt att använda hemlig dataavläsning för att läsa av eller ta upp kameraövervakningsuppgifter utan att göra intrång för att installera tekniska hjälpmedel i någons stadigvarande bostad (t.ex. då uppgifterna läses av från en mobiltelefon vars kamera aktiverats) finns det skäl att i lagen om hemlig dataavläsning uttryckligen förbjuda avläsning eller upptagning i någons stadigvarande boende.

Platskravet för hemlig rumsavlyssning kan sägas innehålla tre delar, vilka samtliga framgår av 27 kap. 20 e § rättegångsbalken. Den första delen är att åtgärden får avse endast en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Den andra är att om åtgärden avser någon annan stadigvarande bostad än den misstänktes får den endast användas om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. Det är således ett högre ställt krav än vad som gäller för den första delen. Den tredje delen är att vissa platser är helt undantagna från hemlig rumsavlyssning, t.ex. tidningsredaktioner och advokatbyråer. Motsvarande vad som gäller för hemlig rumsavlyssning i de tre beskrivna delarna bör gälla när hemlig dataavläsning ska användas för att avläsa eller ta upp rumsavlyssningsuppgifter.

Det är den brottsbekämpande myndigheten som ska verkställa åtgärden som har att se till att kravet angående plats efterlevs.

---

sådan plats eftersom det är svårt att se hur hemlig dataavläsning skulle kunna användas för att läsa av eller ta upp sådana uppgifter.

[15] Av 27 kap. 25 a § andra stycket rättegångsbalken framgår bl.a. att särskilt tillträdestillstånd till utrymme som annars skyddas mot intrång inte får avse tillträde för installation av tekniska hjälpmedel för hemlig kameraövervakning i någons stadigvarande bostad.

10.5.5 Kopplingen mellan enskild och informationssystem

Utredningens förslag: Hemlig dataavläsning får avse avläsning eller upptagning av uppgifter i ett identifierbart informationssystem som används av eller det finns särskild anledning att anta har använts eller kommer att användas av den misstänkte.

Undantag gäller för avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter där hemlig dataavläsning i vissa fall, i enlighet med vad som gäller vid hemlig avlyssning och övervakning av elektronisk kommunikation, får avse avläsning eller upptagning av uppgifter i andra informationssystem än sådana som används av en misstänkt.

Nuvarande regler i rättegångsbalken om koppling till enskild

I rättegångsbalken finns vissa regler om vilken koppling mellan en enskild och teknisk utrustning som krävs för att hemliga tvångsmedel ska få användas. Detta är integritetsskydds- och rättssäkerhetsregler som ska minska risken för att personer som är ovidkommande för utredningen drabbas av åtgärderna.[16]

Enligt 27 kap. 20 § första stycket rättegångsbalken gäller för hemlig avlyssning och övervakning av elektronisk kommunikation att åtgärderna 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. Därutöver finns enligt en andra punkt i samma bestämmelse möjlighet att rikta åtgärderna 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.

När den andra punkten infördes år 2003 anförde regeringen att det, mot bakgrund av integritetsintrånget det innebär att rikta avlyssning och övervakning mot annan än den misstänkte, måste ställas särskilt höga krav på kopplingen mellan den misstänkte och adressen

[16] Se t.ex. prop. 1988/89:124 s. 46.

som åtgärden riktas mot. Begreppet *synnerlig anledning att anta* som slutligen valdes innebär enligt regeringen att det ska finnas tillförlitliga uppgifter som medför att man kan vara så gott som säker på att den misstänkte kommer att kontakta den aktuella adressen. Regeringen framhöll också att avlyssning eller övervakning, eftersom åtgärden riktas mot annan än den misstänkte i dessa fall, endast undantagsvis bör omfatta andra meddelanden än sådana som kommer in till adressen.[17]

Utöver de nu nämnda reglerna gäller enligt 27 kap. 20 § andra stycket rättegångsbalken att hemlig övervakning av elektronisk kommunikation också får ske i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Till skillnad från vad som gäller för hemlig övervakning av elektronisk kommunikation i övriga fall får åtgärden, när den innebär att uppgifter hämtas in om meddelanden, dock endast avse förfluten tid.

Huvudregeln vid hemlig dataavläsning innebär att det ska finnas en koppling mellan den misstänkte och informationssystemet

Även beträffande hemlig dataavläsning behövs, till skydd för den personliga integriteten för personer som är helt utan betydelse för ärendet, som utgångspunkt en koppling mellan den misstänkte och det informationssystem som de uppgifter åtgärden avser finns i. Av de uttryckssätt som finns i de nuvarande reglerna för att göra kopplingen (innehas eller används) är begreppet *används* det som bäst stämmer överens med vår definition av informationssystem. Givetvis kan en elektronisk kommunikationsutrustning innehas men frågan är om de informationssystem som inte avgränsas fysiskt (t.ex. ett användarkonto till en kommunikationstjänst) som vi ansett ska omfattas av definitionen kan innehas i den mening som avses. Det är därför lämpligare att genomgående utgå från själva användandet av informationssystemet.

När den brottsbekämpande myndigheten vet om att den misstänkte löpande använder en viss mobiltelefon eller ett e-postkonto torde kravet på användning inte vålla några problem. Det bör dock

[17] Prop. 2002/03:74 s. 38 f.

krävas att användandet inte är rent tillfälligt. Något absolut krav på omfattningen av användandet bör emellertid inte ställas upp eftersom det då skulle vara tämligen enkelt för kriminella att vidta motåtgärder. Vi föreslår därför inte något särskilt uttryck beträffande omfattningen av användandet men vill erinra om att det ingår som ett led i proportionalitetsprövningen.

Även om det kan förväntas att hemlig dataavläsning i de allra flesta fall inte kommer att sättas in förrän andra, mindre resurskrävande, åtgärder visat sig eller bedömts inte vara verkningsfulla och att de brottsbekämpande myndigheterna därför kommer ha god kontroll på kopplingen mellan den misstänkte och ett visst informationssystem kan det rimligen inte uppställas krav på full bevisning. Frågan är då vilken grad av säkerhet beträffande kopplingen som ska krävas.

Beviskravet för kopplingen bör sättas högt

Ett alternativ skulle kunna vara att använda det ganska låga beviskravet *kan antas,* som ju alltså används i t.ex. bestämmelsen om hemlig avlyssning av elektronisk kommunikation. Att använda samma beviskrav som i den regeln framstår i viss mån som ändamålsenligt, i vart fall när hemlig dataavläsning ska avse avläsning eller upptagning av kommunikationsavlyssningsuppgifter eftersom åtgärden då i praktiken är ett sätt att verkställa den åtgärden. I doktrinen har rent allmänt uttalats att begreppet antagligt (och därmed även ”kan antas”) betyder en mindre sannolikhetsövervikt för att antagandet är riktigt.[18] Det innebär således att det måste finnas åtminstone någon konkret omständighet som leder till slutsatsen att det finns en koppling. Som redan nämnts torde det vanliga förfarandet dock vara att annan åtgärd har prövats, eller bedömts overksam, innan tillstånd till hemlig dataavläsning söks. Dessutom fordrar åtgärden inte sällan tämligen omfattande kartläggning. De nu anförda faktorerna, i förening med det intrång det kan innebära i enskildas personliga integritet om åtgärden används mot någon som inte har med utredningen att göra, talar emellertid för att ett något högre beviskrav bör ställas. Att sätta detta krav så högt som *synnerlig anledning att anta* är

[18] Se t.ex. Ekelöf m.fl., *Rättegång, fjärde häftet*, 7 uppl., s. 85.

i det närmaste detsamma som att vara helt säker, vilket framstår som väl högt med hänsyn till det tidiga skede i utredningar det ofta kommer vara fråga om, se mer om begreppet i prop. 2005/06:178 s. 61. Mer ändamålsenligt framstår det då att använda beviskravet *särskild anledning att anta*. Med ett sådant rekvisit ställs enligt vår mening ett tillräckligt högt krav men, mot bakgrund av förutsättningarna att komma över uppgifter om vem som använder informationssystemet, inte så högt att åtgärden endast kommer kunna användas när den brottsbekämpande myndigheten är helt säker.

Slutsatsen blir därför att huvudregeln ska vara att det ska finnas en koppling mellan en misstänkt och informationssystemet så att hemlig dataavläsning endast får avse uppgifter i ett informationssystem som används av eller som det annars finns särskild anledning att anta har använts eller kommer att användas av den misstänkte.

Ett krav på att informationssystemet är identifierbart bör också ställas upp. Ett sådant krav innebär både att det ska vara möjligt för domstolen att ta ställning till kopplingen mellan den som ska utsättas för åtgärden och informationssystemet (eller delen av detta) och att det klargörs för den verkställande myndigheten och tillsynsmyndigheten vilket informationssystem som avses.

Ett undantag från huvudregeln görs för uppgifter i informationssystem som den misstänkte kontaktar i vissa fall

Eftersom 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 bör motsvarande gälla för hemlig dataavläsning för att läsa av eller ta upp uppgifter som får hämtas in med de tvångsmedlen. Det bör därför föreskrivas ett undantag från huvudregeln om att åtgärden endast får avse uppgifter i informationssystem som används av en misstänkt när det är fråga om avläsning eller upptagning av sådana uppgifter. Undantaget bör dock endast kunna tillämpas i mycket särpräglade situationer. Motsvarande krav som gäller enligt rättegångsbalken för hemlig avlyssning och övervakning av elektronisk kommunikation bör ställas upp beträffande kopplingen mellan den misstänkte och informationssystemet. Det innebär att det ska finnas synnerlig anledning att anta

att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta informationssystemet. Det ska således vara så gott som säkert att den misstänkte kommer att kontakta det aktuella informationssystemet.

De grundläggande kraven på att åtgärden ska vara proportionerlig och av synnerlig vikt för utredningen gäller givetvis även här. Av såväl integritets- som informationssäkerhetsskäl bör särskild restriktivitet vara påkallad vid dessa prövningar när informationssystemet används av någon som inte är misstänkt för brott.

Ett ytterligare undantag till huvudregeln i särpräglade fall

I vissa fall får domstol lämna tillstånd till hemlig övervakning av elektronisk kommunikation även om det inte finns någon misstänkt person, se 27 kap. 20 § andra stycket rättegångsbalken. Så får ske för att utreda vem som skäligen kan misstänkas för ett brott. De uppgifter som övervakningen i dessa fall kan ge de brottsbekämpande myndigheterna tillgång till är samma uppgifter som får hämtas in enligt inhämtningslagen, nämligen historiska uppgifter om meddelanden (dvs. inte realtidsuppgifter) och lokaliseringsuppgifter, både historiska och i realtid.

När uppgifterna är möjliga att hämta in från teleoperatörerna på det sätt som befintlig lagstiftning ger möjlighet till i dag torde det varken föreligga ett tillräckligt behov av hemlig dataavläsning enligt behovsprincipen eller vara av synnerlig vikt för utredningen. Det kan dock tänkas att den brottsbekämpande myndigheten har kännedom om att en viss telefon varit involverad i viss brottslighet eller har funnits på en brottsplats vid brottstillfället och att dagens metoder för att komma åt informationen inte är tillräckliga. Eftersom vi ansett att motsvarande ska gälla för hemlig dataavläsning för att läsa av eller ta upp uppgifter som får hämtas in med befintliga tvångsmedel som det som gäller för det bakomliggande tvångsmedlet bör hemlig dataavläsning i och för sig få användas i de här aktuella situationerna.

Syftet med bestämmelsen i 27 kap. 20 § andra stycket rättegångsbalken är att utreda vem som skäligen kan misstänkas för brottet. Samma syfte bör framgå för hemlig dataavläsning i nu aktuellt avseende.

Av samma anledningar som framhölls i föregående avsnitt finns även i nu förevarande situationer skäl att tillämpa kravet på synnerlig vikt och proportionalitetskravet restriktivt. För att understryka detta bör det lämpligen redan i lagtexten begränsas när åtgärden får tillgripas. Så bör vara möjligt t.ex. när en dator har använts som brottsverktyg eller en telefon har funnits på eller i anslutning till en brottsplats. Därtill bör åtgärden vara möjlig att vidta även av annan anledning, om uppgifterna i informationssystemet är av synnerlig betydelse för att utreda vem som skäligen kan misstänkas för brott.

Det bör föreskrivas särskilt att en sådan åtgärd som diskuteras här inte får avse uppgifter i informationssystem som tillhör operatörer.

10.6 Hemlig dataavläsning i underrättelseverksamhet

10.6.1 Några utgångspunkter

Utredningens bedömning: För hemlig dataavläsning i syfte att läsa av eller ta upp uppgifter som får hämtas in genom andra hemliga tvångsmedel bör som utgångspunkt även i underrättelseverksamhet gälla att kraven för hemlig dataavläsning ska motsvara kraven för tillstånd till det ”bakomliggande” tvångsmedlet enligt de lagar som reglerar hemliga tvångsmedel i underrättelseverksamhet.

Vid hemlig dataavläsning i underrättelseverksamhet för att läsa av eller ta upp lagrade uppgifter eller uppgifter som visar hur ett informationssystem används bör som utgångspunkt motsvarande krav gälla som gäller för tillstånd till hemlig avlyssning av elektronisk kommunikation. Vissa undantag från dessa utgångspunkter bör emellertid göras.

Vi har i avsnitt 10.5.1 redogjort för några utgångspunkter vid hemlig dataavläsning under förundersökning. Det som anfördes där beträffande hemlig dataavläsning för att läsa av eller ta upp uppgifter som kan hämtas in med befintliga hemliga tvångsmedel gäller även i underrättelseverksamhet. Utgångspunkten bör därför även i sådan verksamhet vara att kraven för hemlig dataavläsning ska motsvara kraven för tillstånd till det ”bakomliggande” tvångsmedlet.

Reglerna om hemlig tvångsmedelsanvändning i underrättelseverksamhet finns i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen), lagen om särskild utlänningskontroll (LSU) och inhämtningslagen. Hemlig rumsavlyssning är inte tillåten i någon av de nämnda lagarna. Med den angivna utgångspunkten bör därför inte heller hemlig dataavläsning avseende rumsavlyssningsuppgifter få förekomma i sådan verksamhet, se även avsnitt 9.2.3.

I avsnitt 10.5.1 kom vi fram till att hemlig dataavläsning i förundersökningsfallen bör få användas för att läsa av eller ta upp lagrade uppgifter eller uppgifter som visar hur ett informationssystem används. I väsentliga delar gör sig det som anfördes där gällande även i frågan om detta också bör tillåtas i brottsbekämpande myndigheters underrättelseverksamhet, jfr även prop. 2005/06:177 s. 52. Det finns därför skäl att tillåta hemlig dataavläsning för att läsa av eller ta upp elektroniskt lagrade uppgifter och uppgifter som visar hur ett informationssystem används även i underrättelseverksamhet. Slutsatsen att åtgärden i integritetsriskhänseende kan jämföras med hemlig avlyssning av elektronisk kommunikation eller hemlig kameraövervakning bör dock innebära att den endast ska få användas vid sådan brottslighet och under sådana förutsättningar som i dag kan föranleda dessa tvångsmedel.

Hemlig avlyssning av elektronisk kommunikation kan användas i underrättelseverksamhet under de förutsättningar som anges i preventivlagen och under de förutsättningar som framgår av LSU. De situationer då de två nämnda lagarna möjliggör hemlig tvångsmedelsanvändning är begränsade. I båda fallen krävs att särpräglade förhållanden föreligger. Enligt preventivlagen ska det finnas påtaglig risk för utövande av den särskilt allvarliga brottslighet som anges i lagen. Enligt LSU krävs att åtgärden är av betydelse för att utreda om en utlänning som utvisats enligt den lagen, på grund av att det kan befaras att hen kommer att begå eller medverka till terroristbrottslighet, eller en organisation eller grupp som utlänningen tillhör eller verkar för planlägger eller förbereder terroristbrott. Det är således endast när sådana förhållanden föreligger som hemlig dataavläsning för att läsa av eller ta upp elektroniskt lagrade uppgifter eller uppgifter som visar hur ett informationssystem används bör få användas i underrättelseverksamhet. Inte i några andra fall.

Det är viktigt att understryka att vi alltså inte föreslår en generell möjlighet att använda hemlig dataavläsning i underrättelseverksamhet utan de möjligheter som ges är, liksom möjligheterna att i dag i sådan verksamhet använda hemlig avlyssning av elektronisk kommunikation eller hemlig kameraövervakning, starkt begränsade till allvarlig brottslighet under vissa särskilda förhållanden.

När vi i det följande talar om vilka förutsättningar som ska gälla för att hemlig dataavläsning ska få användas i underrättelseverksamhet delas framställningen in i tre avsnitt, vilket sammanhänger med de olika grunderna som vi diskuterar. Vi benämner då hemlig dataavläsning med stöd av sådana förutsättningar som gäller enligt preventivlagen för preventivlagsfallen. På motsvarande vis kallas åtgärderna med stöd av LSU för LSU-fallen och med stöd av inhämtningslagen för inhämtningslagsfallen.

10.6.2 Hemlig dataavläsning i preventivlagsfallen

Grundläggande förutsättningar

Utredningens förslag: 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 preventivlagens krav för hemlig kameraövervakning tillämpas.

I preventivlagsfallen får hemlig dataavläsning inte användas för att läsa av eller ta upp rumsavlyssningsuppgifter.

I preventivlagen finns möjlighet att få tillstånd till hemlig avlyssning och övervakning av elektronisk kommunikation samt hemlig kameraövervakning. När det gäller förutsättningarna för användning av åtgärderna enligt preventivlagen skiljer de sig åt jämfört med rättegångsbalkens bestämmelser.

Enligt 1 § första stycket preventivlagen får tillstånd till hemliga tvångsmedel enligt lagen meddelas om det med hänsyn till omständigheterna finns en *påtaglig risk* för att en person kommer att utöva viss i lagen angiven särskilt allvarlig brottslighet. Enligt samma bestämmelses andra stycke får tillstånd 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. Den närmare innebörden av de kursiverade kraven framgår av förarbetena till preventivlagen, se t.ex. prop. 2013/14:237 s. 106 ff. Den brottsliga verksamhet som kan föranleda hemliga tvångsmedel enligt preventivlagen består genomgående av mycket allvarliga brott. Vidare uppställs i preventivlagen 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.

Mot bakgrund av de i avsnitt 10.6.1 angivna utgångspunkterna bör hemlig dataavläsning i samtliga avseenden utom för avläsning eller upptagning av rumsavlyssningsuppgifter få användas när det föreligger förhållanden som kan leda till tvångsmedelsanvändning enligt preventivlagen. De grundläggande förutsättningarna för tillstånd enligt 1 § preventivlagen bör skrivas ut direkt i lagen om hemlig dataavläsning för att tydliggöra i vilka situationer åtgärden får användas. Dock framstår det inte som nödvändigt att i lagen även skriva ut motsvarande brottskatalog som finns i preventivlagen avseende vilka brott den brottsliga verksamheten ska innefatta för att omfattas. Den katalogen är tämligen omfattande och kan förväntas tynga lagen om hemlig dataavläsning. Det är därför tillräckligt med en hänvisning till preventivlagen i den delen.

Kravet på att åtgärden ska vara av synnerlig vikt för att förhindra den brottsliga verksamheten (5 § 1 preventivlagen) motsvarar kravet på synnerlig vikt för utredningen enligt rättegångsbalken, se avsnitt 10.5.3. Det kravet bör uttryckligen framgå i lagen om hemlig dataavläsning för preventivlagsfallen. Även motsvarande platskrav som preventivlagen föreskriver för hemlig kameraövervakning bör framgå av lagen om hemlig dataavläsning när det är fråga om avläsning eller upptagning av kameraövervakningsuppgifter i preventivlagsfallen. Liksom i förundersökningsfallen, se avsnitt 10.5.4, behöver det klargöras direkt i lagen att sådana uppgifter inte får läsas av eller tas upp i någons stadigvarande bostad.

Kopplingen mellan enskild och informationssystem

Utredningens förslag: Hemlig dataavläsning får avse avläsning eller upptagning av uppgifter i ett identifierbart informationssystem som används av eller det finns särskild anledning att anta har använts eller kommer att användas av en person som anges i 1 § preventivlagen.

Undantag gäller endast beträffande hemlig dataavläsning avseende kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter. I de fallen är det möjligt att låta avläsningen eller upptagningen avse uppgifter i identifierbara informationssystem som det finns synnerlig anledning att anta att en person som anges i 1 § preventivlagen har kontaktat eller kommer att kontakta.

2 § första stycket 1 preventivlagen motsvarar den i avsnitt 10.5.5 beskrivna regeln i 27 kap. 20 § första stycket 1 rättegångsbalken beträffande hemlig avlyssning och övervakning av elektronisk kommunikation med den skillnaden att kopplingen mellan personen och telefonnumret, adressen eller kommunikationsutrustningen inte avser en misstänkt utan i stället en person som kan bli föremål för åtgärd enligt preventivlagen. Det finns också i 2 § första stycket 2 preventivlagen en motsvarande regel som den i rättegångsbalken om att hemlig avlyssning eller övervakning av elektronisk kommunikation får avse telefonnummer, annan adress eller elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att en person som avses i 1 § preventivlagen under den tid tillståndet avser har kontaktat eller kommer att kontakta.

Det finns inte skäl att här göra en annan bedömning än den vi gjorde för förundersökningsfallen, se avsnitt 10.5.5. Det innebär att i preventivlagsfallen bör huvudregeln vara att hemlig dataavläsning avser uppgifter i ett identifierbart 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. Enda undantaget från huvudregeln gäller uppgifter i ett identifierbart informationssystem som det finns synnerlig anledning att anta att en sådan person kommer att kontakta. Undantagsregeln tar sikte på avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- och lokaliseringsupp-

gifter. I övrigt gör sig samma skäl gällande som redogjordes för i avsnitt 10.5.5. Det innebär bl.a. att undantaget i preventivlagsfallen ska tillämpas med den restriktivitet som anfördes där.

10.6.3 Hemlig dataavläsning i LSU-fallen

Grundläggande förutsättningar

Utredningens förslag: Motsvarande förutsättningar som gäller för tillstånd till hemlig avlyssning av elektronisk kommunikation enligt LSU ska gälla för tillstånd till hemlig dataavläsning i LSU-fallen.

I LSU-fallen får hemlig dataavläsning inte avse avläsning eller upptagning av kameraövervaknings- eller rumsavlyssningsuppgifter.

LSU har en särskild struktur eftersom reglerna om hemliga tvångsmedel i den endast får tillämpas efter att en behörig domstol eller myndighet har fattat beslut om att sådan tillämpning ska ske beträffande en viss person. Sådant beslut får endast meddelas avseende en utlänning som omfattas av ett utvisningsbeslut enligt 1 § 2 den lagen, 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. Först när dessa förutsättningar föreligger kan ett beslut om tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation meddelas. Inga andra hemliga tvångsmedel får således användas med stöd av LSU.[19] Den personkrets som kan bli föremål för åtgärderna är därför mycket liten, liksom antalet tillfällen per år som reglerna alls tillämpas.

De hemliga tvångsmedlen enligt LSU får endast användas om 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. Åtgärder enligt LSU syftar således till att förebygga terroristbrott.

[19] Vi bortser här från möjligheten till postkontroll enligt 20 § LSU.

Det uppställs inte något krav på brottsmisstanke för att tvångsmedel ska få användas och det saknar också betydelse om det finns någon misstanke mot just den person som drabbas av tvångsmedlet, eftersom användningen av detta syftar till att utröna om organisationen eller gruppen som sådan planlägger eller förbereder ett terroristbrott. En viktig begränsning är enligt 20 § att det ska finnas synnerliga skäl för att tvångsmedel ska få tillgripas. Vad gäller rekvisitet synnerliga skäl framgår av förarbetena att lagstiftaren har tänkt på situationen där det finns en överhängande fara för att den politiska organisationen eller gruppen ska utföra eller låta utföra brottsliga handlingar som innefattar bruk av våld, hot eller tvång, och att andra metoder inte kan antas vara tillräckliga för att avvärja denna fara.

Mot bakgrund av de i avsnitt 10.6.1 angivna utgångspunkterna bör hemlig dataavläsning i samtliga avseenden utom för avläsning eller upptagning av kameraövervaknings- och rumsavlyssningsuppgifter få användas när det föreligger förhållanden som kan leda till tvångsmedelsanvändning enligt LSU. Motsvarande krav som gäller enligt den lagen bör föreskrivas i lagen om hemlig dataavläsning.

Det innebär för det första att för att hemlig dataavläsning i LSU-fallen alls ska kunna aktualiseras krävs att det meddelats ett utvisningsbeslut med stöd av 1 § 2 LSU och att behörig domstol eller myndighet bestämt att reglerna om hemlig dataavläsning ska tillämpas på utlänningen. Dessa förutsättningar bör skrivas ut i lagen om hemlig dataavläsning. För att inte tynga lagen bör hänvisningar göras till de bestämmelser i LSU som föreskriver när beslut om att tillämpa tvångsmedelsregler mot utlänningen får fattas. I lagen om hemlig dataavläsning bör också uttryckligen skrivas ut ändamålet med åtgärden, dvs. att den får användas om 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. Endast under den förutsättningen kan alltså hemlig dataavläsning få användas i LSU-fallen. Därtill bör skrivas ut att det ska finnas synnerliga skäl för åtgärden och att den inte får avse avläsning eller upptagning av kameraövervaknings- eller rumsavlyssningsuppgifter.

Kopplingen mellan enskild och informationssystem

Utredningens förslag: Hemlig dataavläsning får i LSU-fallen avse avläsning eller upptagning av uppgifter i ett identifierbart informationssystem som används av eller det finns särskild anledning att anta har använts eller kommer att användas av en utlänning som kan bli föremål för hemliga tvångsmedel enligt LSU.

I LSU finns inget uttryckligt krav på koppling mellan person och det telefonnummer, adress eller kommunikationsutrustning som hemlig avlyssning eller övervakning av elektronisk kommunikation avser. Dock är det endast en utlänning som anges i den lagen som kan bli föremål för dessa åtgärder, se t.ex. 18 § LSU, prop. 1989/90:86 s. 48 och prop. 2005/06:177 s. 55.

Det finns mot bakgrund av integritets- och informationssäkerhetsskäl anledning att uppställa samma huvudregel som i förundersökningsfallen och preventivlagsfallen (se avsnitt 10.5.5 och 10.6.2), dvs. att hemlig dataavläsning endast får avse uppgifter i ett identifierbart informationssystem som används av eller det finns särskild anledning att anta har använts eller kommer att användas av en viss person. För att uppnå överensstämmelse med LSU bör denna person i LSU-fallen vara den utlänning som tvångsmedelsbestämmelserna tillämpas på.

10.6.4 Hemlig dataavläsning i inhämtningslagsfallen

Utredningens förslag: Hemlig dataavläsning i inhämtningslagsfallen får endast avse historiska kommunikationsövervakningsuppgifter och lokaliseringsuppgifter, såväl historiska som i realtid.

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

I lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) regleras vilka uppgifter som brottsbekämpande myndigheter får hämta in från teleoperatörer. De uppgifter som får

hämtas in enligt inhämtningslagen är samma sorts uppgifter som får hämtas in efter beslut om hemlig övervakning av elektronisk kommunikation under förundersökning när det inte finns en skäligen misstänkt, se ovan avsnitt 10.5.5.

Som krav för att inhämtning enligt inhämtningslagen ska få ske gäller enligt 2 § inhämtningslagen att åtgärden ska vara 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. Enligt en tidsbegränsad regel i 3 § inhämtningslagen får inhämtning 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 brottslighet, vars straffskalor inleds lägre än två års fängelse. Det ska dock framhållas att samtliga brott i den tidsbegränsade brottskatalogen är sådana att de kan föranleda tillämpning av hemlig avlyssning av elektronisk kommunikation under förundersökning.

Med utgångspunkten i avsnitt 10.6.1, att kraven för hemlig dataavläsning ska motsvara kraven för tillstånd till det ”bakomliggande” tvångsmedlet, bör hemlig dataavläsning i inhämtningslagsfallen endast få avse avläsning eller upptagning av historiska kommunikationsavlyssningsuppgifter och lokaliseringsuppgifter, såväl historiska som realtidsuppgifter. Detta bör uttryckligen anges i lagen om hemlig dataavläsning. Där bör också föreskrivas att åtgärden endast får vidtas för sådant ändamål som anges i inhämtningslagen, dvs. att för att förebygga, förhindra eller upptäcka viss brottslig verksamhet. Den brottsliga verksamheten som avses kan innefatta antingen brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år eller mer eller brott som anges i 3 § inhämtningslagen. För att inte tynga lagen om hemlig dataavläsning är det tillräckligt med en hänvisning till den senare bestämmelsen.

Vidare bör det liksom enligt inhämtningslagen ställas krav på åtgärdens betydelse. Eftersom hemlig dataavläsning är en åtgärd som kan innebära större integritetsrisker, särskilt i fråga om informationssäkerhetsaspekter, än inhämtning enligt inhämtningslagen bör kravet ställas högre än enligt den lagen. Det finns således skäl att bestämma kravet på åtgärdens betydelse för ändamålet så att åtgärden ska vara av synnerlig vikt för att förebygga, förhindra eller upptäcka den brottsliga verksamheten. Begreppet synnerlig vikt bör i detta sammanhang tolkas i enlighet med vad vi angett tidigare om

begreppet när det är fråga om att rikta åtgärder mot personer som inte är misstänkta för brott, se t.ex. avsnitt 10.5.5. Bedömningen av om det föreligger synnerlig vikt får inte bygga enbart på spekulationer eller allmänna antaganden utan måste grundas på faktiska omständigheter.[20]

Liksom i övriga bestämmelser om hemlig dataavläsning bör krävas att informationssystemet är identifierbart. Något uttryckligt krav på koppling mellan systemet och en enskild person bör dock inte ställas upp eftersom ett sådant krav avsevärt skulle minska möjligheterna att nå framgång i underrättelsearbetet, jfr prop. 2011/12:55 s. 84. Däremot bör särskilt föreskrivas i lagen om hemlig dataavläsning att informationssystemet inte får tillhöra ett företag som tillhandahåller elektroniska kommunikationstjänster eller elektroniska kommunikationsnät, jfr avsnitt 10.5.5. Detta är aktörer från vilka inhämtningen enligt inhämtningslagen kan ske i dag.

10.7 Förbud mot hemlig dataavläsning

10.7.1 Utgångspunkter

I rättegångsbalken finns regler som förbjuder användningen av hemlig rumsavlyssning på vissa platser. Förbudet kom till mot bakgrund av att de yrkeskategorier som avses i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, dvs. yrkeskategorier i verksamheter som omfattas av tystnadsplikt vilken i många fall hindrar personerna i verksamheten från att vittna i en rättegång, ofta utövar sitt yrke i lokaler som används endast och just för den verksamheten. Det ansågs helt enkelt att en strikt tillämpning av proportionalitetsprincipen inte var tillräcklig. De regler som gällde enligt lagen om hemlig rumsavlyssning fördes sedan oförändrade in i rättegångsbalken i samband med att lagen om hemlig rumsavlyssning togs in i balken.

Bestämmelsen i 27 kap. 20 e § tredje stycket rättegångsbalken innebär att hemlig rumsavlyssning inte får avse följande platser.

[20] Jfr prop. 2011/12:55 s. 121.

- 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.
- 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).
- 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.

Någon motsvarande förbudsbestämmelse beträffande användning av övriga hemliga tvångsmedel finns inte i rättegångsbalken eller i någon av speciallagarna som reglerar underrättelseverksamhet. En strikt tillämpning av proportionalitetsprincipen torde emellertid i många fall hindra användning av övriga hemliga tvångsmedel beträffande personer i sådan verksamhet. Det finns däremot särskilda regler om avlyssningsförbud, vilka gäller både för kommunikationsavlyssning och för rumsavlyssning, se t.ex. 27 kap. 22 § rättegångsbalken och 11 § preventivlagen. Dessa bestämmelser är utformade så att avlyssning inte får avse samtal, annat tal eller meddelanden där någon som yttrar sig är undantagen från vittnesplikt på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken. Till skillnad från rumsavlyssningsförbudet gäller de nu nämnda reglerna under pågående verkställighet, dvs. det råder inget absolut förbud mot att rikta avlyssning mot sådana personer men uppgifter som de inte skulle kunna höras om som vittne får inte avlyssnas eller tas upp.

I 27 kap. 2 § första stycket rättegångsbalken finns också annat skydd för uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § rättegångsbalken inte får höras som vittne om (beslagsförbudet). Enligt beslagsförbudet får en skriftlig handling, om den kan antas innehålla sådana uppgifter och innehas av antingen en person som avses i 36 kap. 5 § rättegångsbalken eller av den som tystnadsplikten gäller till förmån för, inte tas i beslag. Högsta domstolen (HD) har fastslagit att fastän beslagsförbudet enligt dess ordalag tar sikte på skriftlig handling så rör det sig om ett infor-

mationsskydd. I ljuset av det fann HD att beslagsförbudet gäller såväl för information av annat slag än skrift som för andra bärare av information än papper samt att all information i en eftersökt fil (eller annan informationsenhet vars innehåll ska kommas åt med beslaget) omfattas av beslagsförbudet, om det kan antas att filen innehåller någon information som omfattas av frågeförbudet i 36 kap. 5 § rättegångsbalken, se NJA 2015. s. 631 p. 25 och 26.

10.7.2 Hemlig dataavläsning får aldrig avse uppgifter i vissa informationssystem

Utredningens förslag: Hemlig dataavläsning får inte avse uppgifter i informationssystem som stadigvarande används i verksamheter som tystnadsplikt gäller för och som anges i 36 kap. 5 § andra–sjätte styckena rättegångsbalken.

Vi vill så långt som möjligt uppnå överensstämmelse mellan regleringen för hemlig dataavläsning och övriga hemliga tvångsmedel. Samtidigt innebär hemlig dataavläsning användning av tekniker vid verkställighet som, åtminstone i teorin, skulle kunna ge tillgång till alla uppgifter som finns i det informationssystem som innehåller uppgifterna som ska läsas av eller tas upp. Mot bakgrund av det starka skydd för uppgifter i sådana verksamheter som omfattas av förbudet mot rumsavlyssning som rättegångsbalken föreskriver finns anledning att överväga om det bör införas ett generellt förbud mot hemlig dataavläsning i några fall. Med generellt förbud avses ett förbud som motsvarar det gällande platsförbudet för hemlig rumsavlyssning men som i stället för plats tar sikte på uppgifter i vissa informationssystem.

I 36 kap. 5 § andra–sjätte styckena rättegångsbalken föreskrivs att vissa personer inte får höras som vittnen om, huvudsakligen, uppgifter som anförtrotts dem i samband med deras yrkesutövning. Bestämmelserna har tillkommit av hänsyn till enskildas personliga integritet och privatliv. Lagstiftaren har ansett att den enskilde, utom när det är fråga om mycket allvarliga brott, och i vissa fall även då, ska kunna anförtro sig till vissa angivna personer utan rädsla för att samtalet eller de uppgifter hen lämnar i samband med det ska komma till tredje mans kännedom eller annars användas emot hen.

Bestämmelserna begränsar alltså möjligheten att inför domstol ställa frågor till ett vittne, och brukar därför beskrivas som frågeförbud.

Det kan på goda grunder antas att de allra flesta av de yrkeskategorier som omfattas av frågeförbudet (t.ex. advokater, läkare och journalister) använder modern teknik i sitt arbete. Datorer, servrar och mobiltelefoner som lagrar känsliga uppgifter torde vara legio i nästan alla de verksamheterna. I informationssystem som används i dessa verksamheter kommer det således oundvikligen finnas en mängd känsliga uppgifter som inte på något vis är av intresse för de ändamål som kan föranleda hemlig dataavläsning.

Hemlig dataavläsning kan, åtminstone i teorin, användas för att komma över alla uppgifter som finns i ett informationssystem. Vi föreslår visserligen regler som ska förhindra att andra uppgiftstyper än sådana som tillståndet avser kan läsas av eller tas upp, se t.ex. förslaget om krav på anpassning av verkställighetstekniken (avsnitt 10.10.2). Mot bakgrund av de syften som bär upp frågeförbudet bör uppgifter i informationssystem som används i verksamheter som omfattas av detta enligt vår mening emellertid tillförsäkras ett starkare skydd än uppgifter i andra informationssystem. Vi föreslår därför att det ska införas ett absolut förbud mot hemlig dataavläsning i dessa fall.

Bestämmelsen om förbud mot hemlig dataavläsning bör utformas med ledning av den regel som gäller förbud mot hemlig rumsavlyssning beträffande vissa platser (27 kap. 20 e § tredje stycket rättegångsbalken). Samma verksamheter som där anges bör omfattas av skyddet som den förbudsregel vi nu föreslår innebär.

Det kan noteras att förbudet vid hemlig rumsavlyssning inte omfattar verksamheter som kan omfattas av frågeförbudet enligt 36 kap. 5 § första stycket rättegångsbalken. Det hänger samman med att frågeförbudet i de fallen bärs upp av andra skyddsintressen än de som ligger till grund för frågeförbuden i andra–sjätte styckena. Därför ansåg regeringen att det inte var nödvändigt med något särskilt undantag för sådana platser. Vi gör ingen annan bedömning när det gäller uppgifter i informationssystem som hemlig dataavläsning ska kunna avse. Det finns därför inte skäl att helt undanta informationssystem i verksamheter som anges i 36 kap. 5 § första stycket rättegångsbalken. Proportionalitetsprövningen lär dock de allra flesta gånger hindra åtgärden även i dessa fall. Därtill får den ”beslagsförbudsregel” vi föreslår, se avsnitt 10.7.3, särskild betydelse för dessa fall.

Förbudsbestämmelsen beträffande hemlig dataavläsning bör således endast omfatta uppgifter i informationssystem som stadigvarande används i de verksamheter för vilka frågeförbud gäller enligt 36 kap. 5 § andra–sjätte styckena rättegångsbalken. 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. Dessutom innebär kravet på stadigvarande användning i sådan verksamhet typiskt sett att förbudsregeln inte träffar t.ex. privata mobiltelefoner eller datorer som i bland används i sådan verksamhet.

Prövningen av om informationssystemet omfattas av förbudet i bestämmelsen ska göras av domstolen eller, i förekommande fall åklagaren, innan beslut meddelas. Visar det sig sedan tillståndsbeslut har meddelats att det är fråga om ett förbjudet informationssystem bör den föreslagna bestämmelsen innebära att åtgärden omedelbart måste avbrytas, jfr avsnitt 10.9.7.

10.7.3 ”Beslagsförbud” vid hemlig dataavläsning

Utredningens förslag: Om det vid genomförande av hemlig dataavläsning kommer fram att uppgifter som läses av eller tas upp skyddas enligt 27 kap. 2 § första stycket rättegångsbalken ska avläsningen omedelbart avbrytas och upptagningarna omedelbart förstöras i de delar som de omfattas av skyddet.

Beslagsförbudet enligt 27 kap. 2 § första stycket rättegångsbalken innebär att en skriftlig handling inte får tas i beslag om

1. den kan antas innehålla uppgifter som en befattningshavare eller någon annan som avses i 36 kap. 5 § rättegångsbalken inte får höras som vittne om, och
2. handlingen innehas av honom eller henne eller av den som tystnadsplikten gäller till förmån för.

Högsta domstolen har slagit fast att skyddet enligt bestämmelsen inte bara omfattar uppgifter i skriftliga handlingar utan i stället innebär ett informationsskydd, dvs. det är uppgifterna som ska skyddas, se NJA 2015 s. 631.

Hemlig dataavläsning kommer kunna användas för att läsa av eller ta upp lagrade uppgifter. Det kan förekomma att lagrade uppgifter som läses av eller tas upp skulle ha omfattats av beslagsförbudsregelns skydd, om uppgifterna framkommit t.ex. vid en undersökning av en beslagtagen dator. I de fallen bör en särskild regel i lagen om hemlig dataavläsning klargöra att det skydd som uppgifterna skulle ha haft vid ett beslag också ska föreligga vid hemlig dataavläsning.

Genom den i avsnitt 10.7.2 föreslagna förbudsregeln beträffande uppgifter i informationssystem som stadigvarande används i verksamheter som omfattas av frågeförbudet enligt 36 kap. 5 § andra–sjätte styckena torde risken för avläsning eller upptagning av ”beslagsförbudsskyddade uppgifter” minska avsevärt. Emellertid omfattar den förbudsregeln inte informationssystem som används i 36 kap. 5 § första stycket rättegångsbalken (jfr punkt 1 i beslagsförbudsregeln) och inte heller informationssystem som används av den som tystnadsplikten gäller till förmån för (jfr punkt 2 i beslagsförbudsregeln).

Det bör därför införas en regel som tillförsäkrar uppgifter som är skyddade enligt beslagsförbudet ett adekvat skydd även när uppgifterna läses av eller tas upp vid hemlig dataavläsning. Lämpligen bör i en sådan bestämmelse en hänvisning göras till beslagsförbudet och ett klargörande införas som innebär att om beslagsförbudsskyddade uppgifter lästs av eller tagits upp så ska avläsningen avbrytas och upptagningen, i den del skydd föreligger, förstöras.

Till skillnad från förbudsregeln i avsnitt 10.7.2 bör den här föreslagna bestämmelsen gälla under pågående verkställighet. Det är således den brottsbekämpande myndigheten som verkställer hemlig dataavläsning som har att kontrollera att den efterlevs. Det motsvarar vad som gäller för skriftliga handlingar som omfattas av rättegångsbalkens beslagsförbud.

10.7.4 ”Avlyssningsförbud” vid hemlig dataavläsning

Utredningens förslag: Motsvarande avlyssningsförbud som gäller enligt 27 kap. 22 § rättegångsbalken och 11 § preventivlagen införs beträffande avläsning och upptagning av kommunikationsavlyssnings- och rumsavlyssningsuppgifter.

I både rättegångsbalken och preventivlagen finns bestämmelser om avlyssningsförbud. Reglerna har enhetlig utformning och finns dels i 27 kap. 22 § rättegångsbalken, dels i 11 § preventivlagen. De är utformade så att avlyssning inte får avse samtal, annat tal eller meddelanden där någon som yttrar sig är undantagen från vittnesplikt på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken. Om det under avlyssningen framkommer att uppgifterna är sådana att de inte får avlyssnas ska avlyssningen omedelbart avbrytas. Det innebär att det råder 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. Därtill får avlyssning som huvudregel inte ske vid samtal med personer som tillhör vissa andra yrkeskategorier, om samtalet har samband med deras yrkesutövning. De yrkeskategorier som avses är advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter och familjerådgivare enligt socialtjänstlagen (2001:453) samt sådana personers biträden. Vidare omfattas i vissa avseenden de som är verksamma inom medieföretag, auktoriserade patentombud och deras biträden samt personer med anknytning till viss statistisk verksamhet.

Hemlig dataavläsning kommer att kunna användas för att läsa av eller ta upp motsvarande uppgifter som de som avlyssningsförbudet avser. Uppgifterna bör då omfattas av samma skydd som enligt befintliga regler. Det bör därför införas en regel som föreskriver motsvarande avlyssningsförbud som det beskrivna i lagen om hemlig dataavläsning. Liksom i beslagsförbudsfallen torde risken för att avläsning eller upptagning av skyddade uppgifter minska genom förbudsregeln som föreslagits i avsnitt 10.7.2 och, beträffande rumsavlyssningsuppgifter, förbudsregeln beträffande platser som föreslagits i avsnitt 10.5.4. Icke desto mindre kan det förekomma situationer då kommunikationsavlyssnings- eller rumsavlyssningsuppgifter som skyddas av avlyssningsförbudet ändå läses av eller tas upp. Exempelvis kan så ske om hemlig dataavläsning avser uppgifter i informationssystem som används av en misstänkt när denne ringer eller skickar meddelande till sin försvarare.

Liksom i beslagsförbudsfallen gäller den bestämmelse som här föreslås under pågående verkställighet. Det är således den verk-

ställande myndigheten som har att kontrollera att den efterlevs, vilket motsvarar vad som gäller för befintliga avlyssningsförbud i dag.

10.8 Tillträdestillstånd

Utredningens förslag: 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 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.

Tillträdestillstånd får inte avse platser där hemlig rumsavlyssning enligt 27 kap. 20 e § tredje stycket rättegångsbalken inte får ske.

10.8.1 Tillträdestillstånd i dag

Det hemliga tvångsmedel som i dag kan föranleda intrång i annars skyddade utrymmen är hemlig rumsavlyssning. Utgångspunkten enligt 27 kap. 25 a § första stycket rättegångsbalken är att den verkställande myndigheten vid hemlig rumsavlyssning, efter särskilt tillstånd, i hemlighet får skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Om en plats ska bli föremål för både hemlig rumsavlyssning och hemlig kameraövervakning, får sedan en lagändring 2014 ett särskilt tillstånd till intrång meddelas även för kameraövervakningen. Tillståndet får dock inte avse tillträde för installation av tekniska hjälpmedel i någons stadigvarande bostad, vilket motiverades av det mycket betydande integritetsintrång det kan innebära med kameraövervakning i bostäder.[21] Värt att notera i detta sammanhang är emellertid att det inte var det fysiska intrånget som föranledde begränsningen utan i stället det integritetsintrång som själva kameraövervakningen skulle kunna innebära.

[21] Prop. 2013/14:237 s. 154 f.

I samband med den nyss nämnda ändringen anförde regeringen bl.a. följande.

> I likhet med majoriteten av remissinstanserna instämmer regeringen i utredningens bedömning att tillträde till utrymmen som inte utgör någons bostad i normalfallet får förväntas ge upphov till begränsade integritetsintrång. Det finns också ett behov av en möjlighet att få tillträde till sådana utrymmen. Tillträdestillstånd för verkställighet av hemlig rumsavlyssning bör därför kunna avse den typen av angränsande utrymmen. Enligt regeringens uppfattning gör sig integritetsaspekten däremot gällande på ett helt annat sätt när tillträdet avser en utomstående persons bostad. Även om det säkerligen kan finnas situationer där det uppstår behov av att kunna bereda sig tillträde till sådana utrymmen, har det inte framkommit att detta behov är så starkt att det kan anses uppväga integritetsintrånget. […] Tillträdestillstånd till ett angränsande utrymme bör alltså inte få avse någon annan stadigvarande bostad än den misstänktes. I den mån det är nödvändigt att utnyttja utomståendes personers bostäder vid verkställighet av beslut om hemlig rumsavlyssning får detta således även i fortsättningen lösas genom att innehavarens samtycke till åtgärden inhämtas.[22]

Det bör också framhållas att en husrannsakan kan ske utan att den som åtgärden riktas mot vet om detta och att underrättelse om åtgärden i sådana fall får fördröjas till dess den kan lämnas utan men för utredningen (28 kap. 7 kap. andra stycket rättegångsbalken).

10.8.2 Behovet av tillträdestillstånd vid hemlig dataavläsning

Hemlig dataavläsning kan genomföras på olika sätt. I vissa fall kommer det att vara nödvändigt för den som ska verkställa åtgärden att ha informationssystemet i sin fysiska besittning, t.ex. då hårdvara ska användas vid verkställighet eller när det inte är möjligt att på distans installera programvara. I dessa fall kommer det först och främst krävas att det alls är möjligt att klarlägga var den utrustning som åtgärden ska avse finns. Så torde kunna ske t.ex. genom sedvanlig spaning eller användning av andra hemliga tvångsmedel. När det väl står klart var utrustningen finns eller förväntas finnas blir frågan hur den som ska verkställa åtgärden ska få informationssystemet i sin besittning. Ett möjligt alternativ är att tillåta den brottsbekämpande myndigheten att få tillträde till utrymmen som

[22] Prop. 2013/14:237 s. 153 f.

annars är skyddade mot intrång, t.ex. enligt reglerna i 4 kap. brottsbalken.

Vi har i vår proportionalitetsavvägning, se föregående kapitel, kommit fram till att det är befogat att i vissa fall tillåta de brottsbekämpande myndigheterna att göra intrång i annars skyddade utrymmen för att hemlig dataavläsning ska kunna genomföras trots att detta utgör en utvidgning jämfört med vad som gäller i dag. För att balansera integritetsintresset angav vi dock där att det måste införas regler som uppställer krav på att informationssystemet finns på den plats ett tillträdestillstånd avser.

10.8.3 Hur bör en reglering om tillträdestillstånd utformas?

Eftersom det redan finns regler om tillträdestillstånd i nuvarande bestämmelser om hemliga tvångsmedel, som dessutom förhållandevis nyligen reviderats, ligger det nära till hands att utforma en bestämmelse om tillträdestillstånd vid hemlig dataavläsning så nära dessa som möjligt. En skillnad som måste beaktas är dock att det intressanta vid hemlig dataavläsning är att informationssystemet finns på platsen tillträdestillståndet ska gälla. En bestämmelse om tillträdestillstånd vid hemlig dataavläsning bör därför ta sikte på kopplingen mellan informationssystemet och platsen.

Som en grundförutsättning 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 rättegångsbalken). Vid hemlig dataavläsning bör ett liknande uttryckssätt användas men i stället bör det krävas att det finns särskild anledning att anta att informationssystemet finns på den plats som tillträdestillståndet ska avse. Det ska alltså inte bara 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.[23]

För att hemlig rumsavlyssning ska få ske i någon annan stadigvarande bostad än den misstänktes krävs att det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där

[23] Jfr prop. 2005/06:178 s. 101.

(27 kap. 20 e § andra stycket rättegångsbalken). Vid utformningen av denna bestämmelse gjordes en jämförelse med vad som krävs för att få utföra husrannsakan hos tredje man i syfte att söka efter någon som ska gripas, anhållas eller häktas, jfr 28 kap. 1 § andra stycket rättegångsbalken. För att en sådan åtgärd ska få vidtas krävs att det finns synnerlig anledning att anta att den som söks uppehåller sig där. JO har uttalat att rekvisitet synnerlig anledning att anta bör tolkas så att det ska *föreligga någon faktisk omständighet som påtagligt visar att man med fog kan förvänta sig* något (i exemplet att den som söks uppehåller sig på platsen).[24]

Ytterst höga krav bör ställas även vid tillträdestillstånd enligt lagen om hemlig dataavläsning när tillståndet ska avse någon annan stadigvarande bostad än en bostad där den misstänkte, eller en person som avses i preventivlags- och LSU-fallen, stadigvarande bor. Att helt utesluta möjligheten till tillträde i andra personers bostäder framstår däremot inte som ändamålsenligt bl.a. mot bakgrund av den risk för motåtgärder från kriminella som då kan förutses, t.ex. att aldrig lämna en telefon obevakad annat än i andras stadigvarande bostäder. Det framstår därför som väl avvägt att använda samma höga krav vid tillträdestillstånd för hemlig dataavläsning som vid tillträdestillstånd för hemlig rumsavlyssning.

Det bör av den föreslagna bestämmelsen också framgå vad syftet med tillträdestillståndet ska vara, nämligen att i hemlighet installera tekniska hjälpmedel.

Frågan är om det ska vara möjligt att meddela tillstånd till tillträde till alla skyddade utrymmen eller om möjligheten till tillträdestillstånd bör begränsas. Hemlig rumsavlyssning får inte användas på platser som stadigvarande används för verksamhet som omfattas av frågeförbudet enligt 36 kap. 5 § andra–sjätte styckena rättegångsbalken. Därför aktualiseras inte tillträdestillstånd till sådana platser. Samma bör gälla för dessa platser vid hemlig dataavläsning. En strikt tillämpning av proportionalitetsprincipen skulle visserligen innebära att tillträdestillstånd lämnades endast i undantagsfall. Det framstår emellertid inte som tillräckligt. Därför bör det framgå av lagen om hemlig dataavläsning att det inte är möjligt med tillträdestillstånd till sådana platser.

[24] Se t.ex. JO 1988/89 s. 68.

10.9 Tillståndsprövning m.m.

10.9.1 Domstolsprövning ska alltid ske

Utredningens förslag: Frågor om tillstånd till hemlig dataavläsning prövas alltid av domstol.

Frågor om hemliga tvångsmedel under förundersökning prövas enligt 27 kap. 21 § första stycket rättegångsbalken av rätten på ansökan av åklagaren. Frågan om tillstånd till tvångsmedel enligt preventivlagen prövas av Stockholms tingsrätt på ansökan av åklagaren. Frågan om tillstånd till hemliga tvångsmedel enligt LSU prövas av Stockholms tingsrätt på ansökan av Säkerhetspolisen eller Polismyndigheten. I samtliga nu nämnda fall är det således domstol som ska pröva om tillstånd till hemliga tvångsmedel ska tillåtas. Förfarandet avseende ansökan, prövning och tillståndsgivning har utvärderats och i allt väsentligt befunnits fungera väl, och dessutom tillgodose de krav som uppställs enligt både regeringsformen och Europakonventionen.[25]

Förfarandet för tillståndsgivning enligt inhämtningslagen ser annorlunda ut jämfört med vad som gäller för andra hemliga tvångsmedel. För närvarande ställs inte krav på domstolsprövning utan i stället fattas beslut om inhämtning av den brottsbekämpande myndigheten, antingen Polismyndigheten, Säkerhetspolisen eller Tullverket. Anledningen till denna beslutsordning var enligt regeringen att andra intressen gällde i underrättelseverksamhet än under en förundersökning.[26] Eftersom de svenska reglerna om inhämtning befunnits inte stå i överensstämmelse med EU-rätten[27] har bl.a. frågan om förhandskontroll enligt inhämtningslagen setts över. Utredningen om datalagring och EU-rätten har föreslagit att ansökan om inhämtning enligt inhämtningslagen ska göras till och prövas av åklagare, se avsnitt 12.8.4 i SOU 2017:75. Förslaget föreslås träda i kraft den 1 december 2018.

Som skäl för den beslutsordning som gäller enligt inhämtningslagen anfördes bl.a. att det är principiellt tveksamt att de allmänna

[25] Se t.ex. prop. 2013/14:237 s. 117 och där angivna hänvisningar till SOU 2012:44.
[26] Se prop. 2011/12:55 s. 88 f.
[27] Se EU-domstolens förhandsavgörande den 21 december 2016 i de förenade målen C-203/15 och C-698/15.

domstolarna på förhand rättsligt prövar olika åtgärder som vidtas inom ramen för underrättelseverksamhet och att domstolarnas möjlighet att fatta de snabba beslut som ofta behövs i underrättelseverksamhet är begränsad med hänsyn till att det saknas jourberedskap. När det gäller den första frågan kan konstateras att inhämtning enligt inhämtningslagen i flera avseenden motsvarar hemlig övervakning av elektronisk kommunikation vid förundersökning när det inte finns någon skäligen misstänkt enligt 27 kap. 20 § andra stycket rättegångsbalken, se avsnitt 10.5.5 och 10.6.4. De uppgifter som får hämtas in med de båda tvångsmedlen är t.ex. exakt samma. I de senare fallen är det domstol som prövar tillståndsfrågan. Även om det finns skäl att hålla med om att det är principiellt tveksamt att de allmänna domstolarna på förhand rättsligt prövar olika åtgärder som vidtas inom ramen för underrättelseverksamhet, är det svårt att se en tydlig principiell skillnad mellan de två situationerna. I båda fallen kan åtgärder riktas mot personer som inte är misstänkta för brott. Även om det i det ena fallet är fråga om åtgärder under förundersökningen är informationsinhämtningen enligt vår mening i praktiken mer att jämföra med underrättelseverksamhet (om än i syfte att bringa klarhet kring ett begånget brott i stället för att förebygga brottslighet).

Vi gör bedömningen att den externa kontroll som en domstolsprövning innebär alltid ska förekomma vid hemlig dataavläsning. Det är särskilt åtgärdens ingripande karaktär som motiverar detta ställningstagande. Dessutom innebär domstolsprövning utan tvivel att reglerna i denna del står i överensstämmelse med EU-rätten och Sveriges åtaganden enligt Europakonventionen.[28]

Det innebär således att samma ordning som i dag gäller för övriga hemliga tvångsmedel ska gälla för hemlig dataavläsning. För inhämtning enligt inhämtningslagen blir det dock en annan ordning än den som gäller i dag. De skäl som anförts för särreglering av inhämtning enligt inhämtningslagen gör sig nämligen enligt vår mening inte i samma grad gällande för hemlig dataavläsning i inhämtningslagsfallen.

[28] Jfr t.ex. EU-domstolens uttalanden i dom den 21 december 2016 i målet C 203/15, punkt 120 och Europadomstolens uttalanden i rättsfallet Zakharov mot Ryssland den 4 december 2015, §§ 268-270.

Vi har redan påpekat likheterna mellan beslut om inhämtning enligt inhämtningslagen och inhämtning efter tillstånd till hemlig övervakning av elektronisk kommunikation när det inte finns någon skäligen misstänkt (som domstolsprövas). Till det kommer att hemlig dataavläsning i inhämtningslagsfallen endast torde aktualiseras när uppgifter som får hämtas in enligt inhämtningslagen inte är möjliga att hämta in eller annars är otillräckliga. Om det är möjligt med inhämtning enligt inhämtningslagen och uppgifterna är tillräckliga torde kravet på att åtgärden, dvs. hemlig dataavläsning, ska vara av synnerlig vikt endast i undantagsfall vara uppfyllt. Det bör således vara sällan som hemlig dataavläsning alls aktualiseras i inhämtningslagsfallen.

Även om det skulle bli något nytt med domstolsprövning av frågor om hemlig dataavläsning i inhämtningslagsfallen är inte underrättelseverksamhet något helt nytt i domstol. Frågor om tillstånd till hemliga tvångsmedel enligt såväl preventivlagen som LSU domstolsprövas redan i dag. Såvitt avser frågan om domstolarnas öppettider och brist på jourverksamhet torde våra förslag om interimistiska åklagarbeslut kunna avhjälpa eventuella problem i den delen, se vidare i avsnitt 10.9.5.

10.9.2 Forum

Utredningens förslag: I förundersökningsfallen ska samma forumregler gälla som i rättegångsbalken medan det i underrättelsefallen är Stockholms tingsrätt som ska pröva ansökan.

När det gäller vilken domstol som ska pröva ansökan finns en ordning som framstår som väl fungerande för de nuvarande hemliga tvångsmedlen. Ordningen skiljer sig en aning mellan förundersökningsfallen och underrättelsefallen.

Under förundersökning gäller reglerna i 19 kap. rättegångsbalken om laga domstol i brottmål. Som huvudregel är rätten i den ort där brottet förövades behörig. Om det är lämpligt, får prövningen i stället ske 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. Som en särskild forumregel finns i 27 kap. 34 § rättegångsbalken en bestämmelse som innebär att

prövningen i vissa fall också får ske av Stockholms tingsrätt. Regeln infördes för att det fanns ett särskilt behov, främst av praktiska skäl, med Stockholms tingsrätt som alternativt forum vid brott som faller inom ramen för Säkerhetspolisens verksamhet. Samma forumregler som gäller för nuvarande hemliga tvångsmedel bör gälla för hemlig dataavläsning under förundersökning.

Såvitt avser underrättelsefallen (dock, som ovan nämnts, inte beträffande inhämtning enligt inhämtningslagen) gäller att Stockholms tingsrätt är exklusivt forum. När en bestämmelse om detta infördes i preventivlagen 2014 konstaterade regeringen först att som utgångspunkt gäller att samtliga mål och ärenden ska kunna handläggas av samtliga tingsrätter. Särlösningar i syfte att koncentrera handläggningen av vissa typer av mål till vissa domstolar bör därför användas endast när starka skäl talar för det.[29] Därefter anförde regeringen som skäl för att göra Stockholms tingsrätt till exklusivt forum för ärenden enligt preventivlagen bland annat följande. Den rättsliga regleringen vad gäller den aktuella typen av ärenden skiljer sig från vad som gäller för andra hemliga tvångsmedel i och med att preventiva tvångsmedel får användas trots att någon förundersökning inte har inletts. Det finns få rättsfall och möjligheterna för beslutsfattaren att samråda med kollegor är ytterst begränsade, både på grund av ärendenas karaktär och att underlaget för rättens bedömning till stor del består av mycket känslig sekretessbelagd information. Vidare anförde regeringen också praktiska skäl, bl.a. att det i Stockholmsområdet finns flest offentliga ombud med erfarenhet av denna typ av ärenden.[30]

Mot bakgrund av att den ordning som råder i dag beträffande hemliga tvångsmedel enligt preventivlagen och LSU förefaller fungera väl bör motsvarande forumregler gälla för hemlig dataavläsning som gäller för övriga hemliga tvångsmedel. De skäl som regeringen anförde beträffande underrättelseverksamhet synes fortfarande ha skäl för sig. Det talar med styrka för att låta Stockholms tingsrätt vara exklusivt forum när hemlig dataavläsning ska användas i underrättelseverksamhet, dvs. även när hemlig dataavläsning används i inhämtningslagsfallen.

[29] Prop. 2013/14:237 s. 162.
[30] Prop. 2013/14:237 s. 164

10.9.3 Vem ska ansöka om tillstånd till hemlig dataavläsning?

Utredningens förslag: Som utgångspunkt är åklagaren den som ansöker om tillstånd, men undantag gäller när det är fråga om hemlig dataavläsning i LSU-fallen.

När förundersökning pågår är det åklagaren som ska ansöka om tillstånd till hemliga tvångsmedel (27 kap. 21 rättegångsbalken). Samma sak gäller när det är fråga om hemliga tvångsmedel enligt preventivlagen (6 § preventivlagen). När det däremot är fråga om hemliga tvångsmedel enligt LSU är det i stället Säkerhetspolisen eller Polismyndigheten som ska göra ansökan (21 § andra stycket LSU). Det saknas skäl att avvika från den nuvarande ordningen när hemlig dataavläsning används för dessa ändamål.

När det gäller hemlig dataavläsning i inhämtningslagsfallen kan först noteras att åklagaren ansöker om hemliga tvångsmedel enligt preventivlagen och dessutom, när det saknas en skäligen misstänkt person i en förundersökning, om tillstånd till hemlig övervakning av elektronisk kommunikation för att utreda vem som skäligen kan misstänkas för brottet, se 27 kap. 21 § rättegångsbalken. Den senast nämnda åtgärden ligger synnerligen nära en ansökan om tillstånd till hemlig dataavläsning i inhämtningslagsfallen. Mot den bakgrunden, och eftersom åklagaren enligt Utredningen om datalagring och EU-rättens förslag framöver ska vara mer involverad i inhämtningslagssammanhang, är det ändamålsenligt att åklagaren ansöker om tillstånd till hemlig dataavläsning i inhämtningslagsfallen.

10.9.4 Vad ska beslutet om hemlig dataavläsning innehålla?

Utredningens förslag: 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.

Samtliga lagar som reglerar hemliga tvångsmedel innehåller ett krav på att den tid som tillståndet gäller ska antecknas i tillståndet. Reglerna är också i praktiken desamma beträffande hur länge ett tillstånd får gälla, nämligen att tiden inte får bestämmas längre än nödvändigt och, när det gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet. En tidsbegränsning av tillståndet är nödvändig av integritetsskäl och för att tillgodose de krav som Europadomstolen ställt upp. Tidsbegränsningen, och kravet på att tiden ska antecknas i tillståndsbeslutet, som gäller enligt övriga lagar framstår dessutom för hemlig dataavläsning som väl avvägd. Motsvarande bör därför gälla i lagen om hemlig dataavläsning som gäller för övriga hemliga tvångsmedel.

Mot bakgrund av den centrala plats som informationssystemet intar i bestämmelserna om hemlig dataavläsning bör det i beslutet också antecknas vilket informationssystem tillståndet avser. Det är i praktiken motsvarande krav som för närvarande gäller när tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation samt inhämtning enligt inhämtningslagen har beslutats, se 27 kap. 21 § tredje stycket rättegångsbalken, 8 § preventivlagen och 5 § inhämtningslagen.

Vi föreslår också att det ska antecknas vilken uppgiftstyp tillståndet avser. De olika uppgiftstyper som ett tillstånd kan avse framgår i avsnitt 10.3. Den här föreslagna bestämmelsen utgör den kanske allra viktigaste skyddsåtgärden för den personliga integriteten i tillståndet eftersom den begränsar möjligheten till avläsning av andra uppgiftstyper än den eller de som tillåts. Bestämmelsen utgör nämligen utgångspunkt för de anpassningsskyldigheter av verkställighetstekniken som vi föreslår ska gälla för den myndighet som ska verkställa hemlig dataavläsning(se avsnitt 10.10.2). I praktiken innebär det föreslagna kravet att domstolen i tillståndet ska anteckna vilken eller vilka uppgiftstyper som får läsas av eller tas upp genom hemlig dataavläsning. Det innebär också att den som ansöker om hemlig dataavläsning måste klargöra vilken uppgiftstyp det ansöks om tillstånd för att läsa av eller ta upp, vilket är viktigt eftersom olika regler kommer att aktualiseras beroende på vilken uppgiftstyp hemlig dataavläsning ska användas för.

När hemlig kameraövervakning eller hemlig rumsavlyssning har beslutats krävs enligt såväl 27 kap. 21 § fjärde stycket rättegångsbalken som 8 § preventivlagen (endast kameraövervakning) att platsen där åtgärderna får vidtas anges i beslutet. När hemlig dataavläsning avser kameraövervaknings- och rumsavlyssningsuppgifter har vi föreslagit att motsvarande platskrav ska gälla. Platsen bör därför även i dessa fall antecknas i tillståndsbeslutet. Likaså bör det, när det är fråga om hemlig dataavläsning som avser rumsavlyssningsuppgifter, på motsvarande vis som krävs vid hemlig rumsavlyssning (se 27 kap. 21 femte stycket rättegångsbalken) anges i beslutet vem som är misstänkt.

Vidare måste det också krävas att det i beslutet anges särskilt om ett tillträdestillstånd har meddelats och vilken plats det i så fall avser (jfr 27 kap. 21 § fjärde stycket rättegångsbalken).

Slutligen bör det också uppställas krav på att det i beslutet anges de särskilda villkor som domstolen ställt upp för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Sådana villkor kan ta sikte på i stort sett vilka omständigheter som helst som kan gagna den personliga integriteten för enskilda.

10.9.5 Möjlighet för åklagare att fatta interimistiska beslut

Utredningens förslag: Åklagaren får fatta interimistiska beslut om hemlig dataavläsning om det skulle medföra en fördröjning av väsentlig betydelse att inhämta rättens tillstånd. Det krävs att anmälan av beslutet sker till rätten utan dröjsmål och att rätten därefter skyndsamt prövar ärendet. Inhämtade uppgifter får inte användas i en brottsutredning till nackdel för en enskild om rätten anser att det saknats skäl för åtgärden.

Utredningens bedömning: Möjligheten att meddela interimistiska åklagarbeslut ska inte gälla när hemlig dataavläsning avser rumsavlyssningsuppgifter eller i LSU-fallen.

Nuvarande regler om interimistiska åklagarbeslut vid hemliga tvångsmedel

Domstolsprövningen är en viktig del av det system med rättssäkerhetsgarantier som omgärdar tillämpningen av de hemliga tvångsmedlen. En självklar utgångspunkt är därför att befogenheter för åklagare att fatta interimistiska beslut om tvångsmedlen endast bör förekomma om starka skäl talar för det (se prop. 2002/03:74 s. 42 f.).

Lagstiftaren har funnit att sådana starka skäl föreligger när det gäller hemlig avlyssning och övervakning av elektronisk kommunikation samt hemlig kameraövervakning, både såvitt avser förundersökningsverksamhet och underrättelseverksamhet (se 27 kap. 21 a § rättegångsbalken och 6 a § preventivlagen). Det som främst framhållits som skäl för en sådan möjlighet är att den tekniska utvecklingen lett till att hemliga tvångsmedelsbeslut kan behöva fattas med mycket kort varsel och att domstolarnas öppettider inte fullt ut motsvarar behovet.[31] Anledningen till att hemlig rumsavlyssning inte omfattas av bestämmelserna om interimistiska åklagarbeslut är enligt lagstiftaren att det, främst mot bakgrund av att åtgärden är det hemliga tvångsmedel som typiskt sett leder till det största intrånget i enskildas personliga integritet, är påkallat med särskild försiktighet när det gäller det tvångsmedlet.[32]

För att balansera den risk för rättssäkerheten som det innebär att domstol inte fattar beslutet som leder till tvångsmedelsanvändning har regler införts som innebär att beslutet efter ett interimistiskt åklagarbeslut utan dröjsmål ska anmälas till rätten. Vidare gäller att rätten därefter skyndsamt ska pröva ärendet på samma vis som vid en ansökan. Om rätten vid denna prövning finner att det inte finns skäl för åtgärden, ska den 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. (Se 27 kap. 21 a § andra och tredje styckena rättegångsbalken och 6 a § preventivlagen). Lagstiftaren framhöll att det genom dessa åtgärder saknades skäl att

[31] Prop. 2013/14:237 s. 138 f.
[32] Prop. 2013/14:237 s. 142.

anta att en möjlighet för åklagare att fatta interimistiska beslut om hemliga tvångsmedel skulle få negativa konsekvenser för enskildas rättssäkerhet.[33]

Interimistiska beslut vid hemlig dataavläsning

De rättssäkerhetsgarantier som uppställs i gällande regler om hemliga tvångsmedel vid interimistisk åklagarprövning är tillräckliga även för att tillåta sådana beslut beträffande hemlig dataavläsning. Det bör därför införas motsvarande ordning som gäller enligt rättegångsbalken och preventivlagen beträffande interimistisk tillståndsgivning till hemlig dataavläsning. Eftersom det inte finns någon rätt för åklagare att meddela interimistiska beslut vid hemlig rumsavlyssning bör det inte heller finnas någon sådan möjlighet beträffande hemlig dataavläsning avseende rumsavlyssningsuppgifter. Inte heller enligt LSU finns en sådan rätt. Det torde hänga samman med att åklagaren inte är involverad i de ärendena. Vid hemlig dataavläsning i LSU-fallen bör det därför inte heller finnas en rätt för åklagaren att meddela interimistiska beslut.

När det gäller inhämtningslagsfallen bör det föreligga möjlighet till interimistiska åklagarbeslut. Det är nämligen enligt vår mening svårt att se några avgörande skäl mot en interimistisk beslutanderätt i de fall då uppgifterna verkligen behövs omgående (t.ex. då det finns konkreta uppgifter om en nära förestående terroristattack), bedöms proportionerliga och inte är möjliga att hämta in på annat sätt. Vårt förslag blir därför att samma sak ska gälla när det är fråga hemlig dataavläsning i inhämtningslagsfallen som i övriga fall då åklagaren ges möjlighet att fatta interimistiska beslut om tillstånd.

10.9.6 Offentliga ombud, sammanträde och förfarandet

Utredningens förslag: Vid alla ärenden i domstol om hemlig dataavläsning ska det hållas sammanträde där ett offentligt ombud och den som gjort ansökan närvarar. I övrigt gäller den ordning

[33] Prop. 2013/14:237 s. 141.

som gäller enligt rättegångsbalken beträffande offentliga ombud eller 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.

Offentliga ombud m.m. enligt nuvarande hemliga tvångsmedelsregler

Offentliga ombud ska enligt nuvarande ordning 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. Bestämmelserna om offentliga ombud finns i 27 kap. 26–30 §§ rättegångsbalken och gäller genom hänvisningar även för tvångsmedelsanvändningen enligt preventivlagen och LSU.

Reglerna om offentliga ombud kom till för att stärka enskildas skydd i sådana ärenden om hemliga tvångsmedel. I förarbetena angavs att genom det offentliga ombudet tillkommer en person som har till särskild uppgift att bevaka enskildas intressen och att lyfta fram omständigheter till skydd för enskildas integritet. Vidare anfördes att det med offentliga ombud skapas ett slags kontradiktorisk process som ger bättre förutsättningar för en allsidig belysning av saken. Därtill, fann regeringen, skapas en reell möjlighet att få ett beslut att tillåta användning av hemliga tvångsmedel prövat av högre rätt.[34]

Som framgår av uppräkningen av vid vilka ärenden om hemliga tvångsmedel offentliga ombud ska delta i innebär dagens ordning således att det inte föreskrivs något om offentligt ombud i samband med prövning av ansökningar om hemlig övervakning av elektronisk kommunikation. Frågan om det offentliga ombudets närvaro även i dessa ärenden har utretts men inte föranlett någon förändring.

[34] Prop. 2002/03:74 s. 22 f.

Utredningen om vissa hemliga tvångsmedel anförde att det som kom fram vid den utredningens kartläggning gav stöd för att ombuden får sin främsta betydelse vid vissa särskilt integritetskränkande tvångsmedel (hemlig rumsavlyssning, hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning). De skäl som anfördes för att inte ställa krav på offentligt ombud vid hemlig övervakning av elektronisk kommunikation var dels att det integritetsintrång som tvångsmedlet medför typiskt sett är mindre än det från de övriga nämnda tvångsmedlen, dels att flera sådana frågor som de offentliga ombuden är särskilt ägnade att bevaka (t.ex. att ett beslut inte är förenligt med lag eller att rätten i fråga om hänsyn till ett motstående intresse har gjort en felaktig bedömning) mera sällan torde komma upp vid hemlig övervakning av elektronisk kommunikation. Därtill kom, enligt utredningen, att det finns ett värde i sig av att medverkan av offentliga ombud koncentreras till ärenden där behovet och funktionen av detta i praktiken visat sig vara starka eftersom det på så sätt undviks att ombudens roll vattnas ur eller att systemet uppfattas som ”ett spel för gallerierna”.[35] Utredningen kom således till slutsatsen att de övriga rättssäkerhetsgarantierna som den hemliga tvångsmedelslagstiftningen innehåller var tillräckliga och tillfredställande från rättssäkerhets- och integritetssynpunkt samt att ett krav på medverkan av ett offentligt ombud således inte borde införas.

Av naturliga skäl, eftersom den verkställande myndigheten själv fattar beslutet, finns inte heller krav på offentligt ombud när beslut om inhämtning enligt inhämtningslagen ska meddelas.

Offentliga ombud i frågor om hemlig dataavläsning

Av vad som framkommit i de utvärderingar som gjorts av systemet med offentliga ombud förefaller de regler som i dag finns vara ändamålsenliga utifrån de syften som föranlett dem. De har dessutom bedömts leva upp till regeringsformens och Europakonventionens krav på rättssäkerhetsgarantier vid hemliga tvångsmedel.[36] Motsvarande regler bör, mot bakgrund av de integritetsrisker och infor-

[35] SOU 2012:44 s. 672 f.
[36] Se t.ex. SOU 2012:44 s. 666.

mationssäkerhetsrisker som föreligger med hemlig dataavläsning oavsett vilken uppgiftstyp åtgärden avser, gälla för hemlig dataavläsning. Kravet på offentligt ombud i alla fall av hemlig dataavläsning innebär ett högre krav för den åtgärden avseende kommunikationsövervaknings- och lokaliseringsuppgifter än vad som gäller enligt de ”bakomliggande” tvångsmedlen hemlig övervakning av elektronisk kommunikation och inhämtning enligt inhämtningslagen. Det framstår som helt befogat med hänsyn till de integritetsrisker vi konstaterat i föregående kapitel.

Det är tillräckligt med en hänvisning till rättegångsbalkens bestämmelser om offentliga ombud och sammanträde. Eftersom det emellertid inte alla gånger kommer att vara åklagaren som gör ansökan, se avsnitt 10.9.3, bör det dock i stället för vad som anges i 27 kap. 28 § rättegångsbalken anges i bestämmelsen i lagen om hemlig dataavläsning att de som ska närvara vid sammanträdet är det offentliga ombudet och den som gjort ansökan.

Reglerna om sammanträde och offentligt ombud tar sikte på förfarandet. Det finns ytterligare delar av förfarandet som behöver regleras i den nya lagen eftersom dessa annars lämnas oreglerade. I preventivlagen har en hänvisning beträffande förfarandet gjorts till reglerna i rättegångsbalken om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor. Till bestämmelsen har fogats undantaget att det anförda gäller om inte annat anges i den lagen. Den i preventivlagen valda lösningen framstår som ändamålsenlig även för lagen om hemlig dataavläsning.

Det bör också särskilt föreskrivas ett skyndsamhetskrav i lagtexten.

10.9.7 Omedelbar verkställighet och omedelbart hävande

Utredningens förslag: 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.

Enligt 30 kap. 12 § rättegångsbalken gäller att beslut enligt vilket rätten utlåtit sig angående häktning eller åtgärd som avses i 25–28 kap. omedelbart kan verkställas. Eftersom samtliga hemliga tvångsmedel

finns i 27 kap. rättegångsbalken omfattas de av bestämmelsen. I de övriga lagarna som reglerar hemliga tvångsmedel finns särskilda regler som anger att beslut om hemliga tvångsmedel går i omedelbar verkställighet. Det saknas skäl att låta något annat gälla för hemlig dataavläsning. Eftersom åtgärden inte kommer att omfattas av 30 kap. 12 § rättegångsbalken bör detta framgå direkt av lagen.

Givetvis bör inte åtgärden fortsätta längre än vad som är absolut nödvändigt. 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 § rättegångsbalken. Det finns enligt vår mening skäl att införa en motsvarande och tydlig bestämmelse i lagen om hemlig dataavläsning. Mot bakgrund av att det dock finns ärenden då åklagaren inte är den som ansöker om tillståndet och därmed inte är involverad alls i ärendet (LSU-fallen, se avsnitt 10.9.3) bör dock ordalydelsen justeras något jämfört med vad som gäller enligt rättegångsbalken.

10.10 Genomförande av hemlig dataavläsning

10.10.1 Hur får hemlig dataavläsning verkställas

Utredningens förslag: När tillstånd till hemlig dataavläsning har lämnats får de tekniska hjälpmedel som behövs för avläsning och 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 sedan tillstånd till hemlig dataavläsning har lämnats.

Nuvarande regler om verkställighet av hemliga tvångsmedel

När det i nuvarande regler om hemliga tvångsmedel beskrivs hur åtgärderna får verkställas framgår detta delvis i de bestämmelser som definierar tvångsmedlen och delvis i särskilda bestämmelser som reglerar själva verkställigheten. För hemlig avlyssning och hemlig

övervakning av elektronisk kommunikation gäller enligt 27 kap. 25 § rättegångsbalken att de tekniska hjälpmedel som behövs för åtgärden får användas. Motsvarande uttryckssätt används i 9 § preventivlagen för de tvångsmedlen enligt den lagen. Det innebär att de myndigheterna kan verkställa åtgärden själva, med den avlyssnings- eller övervakningsutrustning som de finner lämplig. Dessutom finns möjligheten att ta hjälp av den som bedriver verksamhet enligt lagen om elektronisk kommunikation enligt vad som föreskrivs i dels 27 kap. 25 § andra stycket rättegångsbalken, dels 6 kap. 19 § lagen om elektronisk kommunikation. Med *tekniskt hjälpmedel* avses både hårdvaror och programvara.

För hemlig kameraövervakning och hemlig rumsavlyssning finns inte motsvarande bestämmelser beträffande verkställighet som finns för de nyss nämnda åtgärderna. Verkställighetsmetoden för hemlig kameraövervakning kan i stället sägas vara reglerad direkt i den bestämmelse (27 kap. 20 a § rättegångsbalken) som definierar åtgärden. Där anges att åtgärden innebär att fjärrstyrda TV-kameror, andra optisk-elektroniska instrument eller därmed jämförbara utrustningar används för optisk personövervakning. Den teknik som anges i regleringen är således sådan som får användas vid verkställighet. På motsvarande vis framgår av 27 kap. 20 d § rättegångsbalken att hemlig rumsavlyssning sker med hjälp av ett tekniskt hjälpmedel som är avsett att återge ljud.

Verkställighet av hemlig dataavläsning

Vi har i avsnitt 8.4.1 beskrivit hur verkställighet av hemlig dataavläsning kan gå till och de olika faserna som kan sägas ingå i den. Så som vi föreslagit att hemlig dataavläsning ska definieras är det egentligen bara avläsningsfasen, dvs. då själva avläsningen eller upptagningen av uppgifter sker, som innebär verkställande av ett beslut om hemlig dataavläsning. Icke desto mindre är också intrångsfasen, dvs. beredandet av tillgång till det informationssystem som tillståndet avser, av stor betydelse för en lyckad verkställighet. Viktig är även installationsfasen, dvs. installationen av hårdvaran eller programvaran när sådan ska användas för verkställighet. En verkställighetsregel bör mot bakgrund av det anförda sätta ramarna för vad

som ska vara tillåtet respektive inte tillåtet beträffande alla de tre nämnda faserna.

I enlighet med direktivens krav bör verkställighetsregeln utformas teknikneutralt för att stå sig över tid. Samtidigt bör, för att balansera de risker för tillämpningsglidningar som vi redovisat i föregående kapitel, viss specificering av vilken teknik som får användas ske. Att på samma gång utforma en regel både teknikneutralt och teknikspecifikt kan framstå som en paradox. Vår bedömning, såvitt avser själva avläsningsdelen, är emellertid att den bestämmelse som reglerar hur hemlig avlyssning och övervakning av elektronisk kommunikation får verkställas är utformad på ett neutralt vis samtidigt som den verkar avgränsande. Dessutom rymmer den de tekniker som vi kan se framför oss för själva avläsningen i dag. Det bör därför införas en regel som klargör att när tillstånd till hemlig dataavläsning har lämnats får de tekniska hjälpmedel som behövs för avläsningen eller upptagningen användas. Med tekniska hjälpmedel avses då både hårdvara och programvara. Dessa kan vara placerade i informationssystemet eller, när det är fråga om avläsning av uppgifter i informationssystem som är ett användarkonto, helt enkelt utgöras av datorer hos den brottsbekämpande myndigheten från vilka själva avläsningen kan ske efter t.ex. inloggning på kontot.

När det gäller åtgärder som inte är en del av själva verkställigheten av avläsningen men som ändå är nödvändiga för att verkställighet ska kunna ske bör alltså även dessa framgå av verkställighetsregeln. Det finns då anledning att utgå från de åtgärder som nämnts i avsnitt 8.4.1 eftersom uppgifterna där kommer från de tekniska experterna vid de brottsbekämpande myndigheterna med god insikt i vad som krävs för en lyckad verkställighet. Till att börja med bör det framgå att det ska vara möjligt för den brottsbekämpande myndigheten att genom inloggning bereda sig tillgång till informationssystem. Det bör således vara tillåtet för den brottsbekämpande myndigheten att använda sig av exempelvis den misstänktes inloggningsuppgifter om man har kännedom om dessa. Även andra sätt att bereda sig tillgång till informationssystem bör omfattas. Som ett sammanfattande uttryck kan motsvarande lydelse som gäller för dataavlesing i Norge användas, nämligen att den brottsbekämpande myndigheten får bryta eller kringgå systemskydd om det är nödvändigt för att kunna verkställa beslutet om hemlig dataavläsning. Vidare bör det framgå att det ska vara möjligt för den brotts-

bekämpande myndigheten att utnyttja sårbarheter på ett sådant sätt som förklarats i avsnitt 8.4.1, se särskilt under underrubrikerna Intrångsfasen och Installationsfasen. Även ett sådant utnyttjande bör endast få ske om det är nödvändigt för att kunna verkställa ett beslut om hemlig dataavläsning. Det bör slutligen också framgå att den brottsbekämpande myndigheten får använda tekniska hjälpmedel i det informationssystem som tillståndet avser. Det kan gälla t.ex. programvara eller funktioner som redan finns i informationssystemet, såsom GPS, kamera eller mikrofon för att kunna avläsa eller ta upp lokaliserings-, kameraövervaknings- eller rumsavlyssningsuppgifter, eller programvara som den brottsbekämpande myndigheten placerar i systemet för att hemlig dataavläsning ska kunna genomföras.

Ett krav för att få vidta sådana åtgärder som nu nämnts bör, utöver att de ska vara nödvändiga, vara att tillstånd till hemlig dataavläsning har beslutats. När så skett får åtgärderna vidtas och utgör då således, givetvis, inte straffbara dataintrång.

Mot bakgrund av de tämligen långtgående möjligheter som de brottsbekämpande myndigheterna ges genom den bestämmelse som här föreslås och de integritets- och informationssäkerhetsrisker som vi konstaterat i föregående kapitel redogör vi i avsnitt 10.10.2 och 10.10.3 för vissa inskränkningar som gäller i alla delar av verkställigheten. Dessutom förtjänar det här att påminna om att de grundläggande principerna om ändamål, behov och proportionalitet gäller även vid bedömningen av vilket tekniskt tillvägagångssätt som ska användas för att verkställa ett beslut om hemlig dataavläsning.

Verkställighetstekniken ingår inte i domstolsprövningen

I tidigare avsnitt har vi redogjort för bl.a. vad domstolen ska pröva inför tillstånd till hemlig dataavläsning. Själva teknikfrågan, dvs. hur hemlig dataavläsning ska genomföras i det enskilda fallet, omfattas dock inte av domstolens prövning utan lämnas till den brottsbekämpande myndigheten att avgöra. Vår bedömning är nämligen att det är lämpligast om den verkställande myndigheten själv avgör vilken teknik som passar bäst i det enskilda fallet. Denna ordning gäller i dag för övriga hemliga tvångsmedel.

Utredningen har tillskrivits av Dataskydd.net[37] och Föreningen för digitala fri- och rättigheter, DFRI[38]. I skrivelsen framförs bl.a. följande krav.

> Ingen åtgärd ska vidtas utan föregående prövning i en oberoende instans. Den oberoende instansen ska få tillräckligt med information för att göra en självständig bedömning av nödvändigheten och proportionaliteten i åtgärden. Informationen ska innefatta en *redovisning av hur myndigheterna tekniskt kommer att genomföra och avsluta* husrannsakan. (Utredningens kursivering)

Skälet bakom kravet är enligt föreningarna att det utan en prövning av tekniken som ska användas inte är möjligt att göra en fullständig nödvändighets- och proportionalitetsbedömning i det enskilda fallet. För andra hemliga tvångsmedel gäller att domstolen prövar om de lagliga förutsättningarna för åtgärden är uppfyllda och den verkställande myndigheten avgör hur verkställigheten ska gå till. Samma sak bör gälla för hemlig dataavläsning. Det bör erinras både om att den verkställande myndigheten är skyldig att iaktta de grundläggande principerna om ändamål, behov och proportionalitet även vid verkställigheten och att tillsynsmyndigheten i samband med sin kontroll kan anmärka mot åtgärderna och, om det behövs, vidta andra åtgärder om principerna inte följs i verkställighetsskedet. Till detta kommer att de krav som vi nedan ställer upp om anpassningsskyldighet för den brottsbekämpande myndigheten av verkställighetstekniken, aktsamhetskrav och att en särskild person ska ansvara för verkställigheten bör leda till att särskild försiktighet iakttas vid verkställighet, vilket i sin tur också torde kunna motverka de risker som föreningarna ser framför sig.

Det kan också påminnas om att det enligt 2 § polisdataförordningen åligger Polismyndigheten eller Säkerhetspolisen, när dessa planerar nya it-system av större omfattning eller nya it-system som kan innebära särskilda risker för intrång i den personliga integriteten, att samråda med Datainspektionen i god tid innan beslut i frågan

[37] Dataskydd.net är enligt uppgifter på webbsidan www.dataskydd.net/om en partipolitiskt oberoende ideell förening vars syfte är att verka för informerade beslut om lagstiftning och teknologi i enlighet med de grundläggande rättigheterna till dataskydd och personlig integritet.

[38] DFRI är enligt uppgifter på webbsidan www.dfri.se/dfri en ideell och partipolitiskt obunden förening som verkar för främjandet av digitala rättigheter, vars mål är ett samhälle med så lite övervakning, spårning och avlyssning som möjligt där yttrandefrihet, transparens och informationsfrihet, personlig integritet och människors rätt att själva bestämma över sin personliga information och digitala fotspår värnas.

fattas. Detsamma gäller myndigheterna, när de genomför betydande förändringar i sådana system. De ska, när sådant samråd som nyss nämnts krävs, även samråda med Säkerhets- och integritetsskyddsnämnden bl.a. i frågor som avser användning av hemliga tvångsmedel. Viss förhandskontroll av it-lösningar som kommer att användas vid hemlig dataavläsning kan således förväntas ske utanför de brottsbekämpande myndigheterna.[39] Vår samlade bedömning av vad som anförts är att det inte finns skäl att inom ramen för domstolsprövningen överväga frågan om hur själva verkställigheten ska ske.

Frågan om rapportering av säkerhetsbrister

En annan fråga som Dataskydd.net och DFRI tagit upp i sin skrivelse till utredningen handlar om att om hemlig dataavläsning införs bör det finnas en skyldighet för de brottsbekämpande myndigheterna att rapportera säkerhetsbrister. De två intresseföreningarna uttrycker sina krav enligt följande.

> De brottsbekämpande myndigheterna ska offentligt och lättillgängligt redovisa de metoder de har använt för att utnyttja sårbarheter i programvaror och andra elektroniska system. Oavsett om de brottsbekämpande myndigheterna har fått tag på metoderna för att utnyttja sårbarheter från andra myndigheter eller från näringslivet ska användningen omfattas av en redovisningsplikt som ska göras offentlig. Det ska alltså inte vara möjligt för myndigheterna att begagna sig av en metod för att utnyttja en sårbarhet i programvaror eller elektroniska system upprepade gånger utan att sårbarheten sedan kan åtgärdas.

Skälet till denna uppfattning är att ett krav på redovisningsskyldighet underlättar åtgärdande av sårbarheten för den stora majoriteten laglydiga användare av elektroniska verktyg. Ett annat sätt att uttrycka detta på, vilket gjorts i den allmänna debatten om riskerna med hemlig dataavläsning, är att man genom hemlig dataavläsning kan bidra till ”en osäkrare digitaliserad tillvaro för oss alla genom att säkerhetshål i de verktyg och tjänster vi använder inte täpps igen så snabbt som de kunde”.[40]

[39] Utredningen om 2016 års dataskyddsdirektiv har föreslagit vissa förändringar på området, se SOU 2017:29. Dock kommer det även med dessa förslag bli fråga om viss extern förhandskontroll.
[40] Citat från debattartikeln *Hemlig dataavläsning – statliga virus i frihetens och öppenhetens tjänst… eller?* av docenten i teknik och social förändring och doktorn i rättssociologi vid

Utredningen gör bedömningen att de skäl som anförs för en redovisningsskyldighet endast har viss giltighet. När sårbarheter eller säkerhetsbrister i informationssystem som redan är kända av den som utvecklar eller producerar informationssystemet utnyttjas vid hemlig dataavläsning så finns redan möjlighet för den både att åtgärda systemets svagheter och – i tiden till dess att så skett – upplysa användarna om bristen. Enligt utredningens mening kan därför brottsbekämpande myndigheters utnyttjande av sådana sårbarheter eller säkerhetsbrister varken anses öka riskerna för den breda massan eller upprätthålla vägar in i informationssystem (möjligen undantaget det enskilda informationssystem som tillståndet avser). I detta sammanhang bör påminnas om att hemlig dataavläsning är en riktad åtgärd som kräver särskilt tillstånd för varje informationssystem som ska avses.

När det däremot gäller utnyttjande av s.k. dag noll-sårbarheter, dvs. sådana sårbarheter eller säkerhetsbrister som inte är kända av den som utvecklar eller producerar informationssystemet, är situationen delvis en annan. Genom att inte underrätta tillverkaren om sårbarheten i dessa fall kommer denna stå öppen inte bara för den brottsbekämpande myndigheten utan också för andra, och därmed även illasinnade personer. På så vis kan det sägas att säkerhetshålen inte täpps igen så snart som de skulle kunna täppas igen. Det innebär i förlängningen att det finns risk för att kriminella skulle kunna utnyttja samma hål som den brottsbekämpande myndigheten. Detta kan i viss mån sägas tala för en rapporteringsskyldighet avseende den typen av sårbarheter och säkerhetsbrister. Emellertid kommer de säkerhetsbrister och sårbarheter som nu diskuteras att finnas oavsett om de brottsbekämpande myndigheterna får kännedom om dem eller inte. Därmed kommer de kunna utnyttjas av den som upptäcker eller får kännedom om dem (samt har tillräckliga kunskaper för ett sådant utnyttjande) oberoende av om brottsbekämpande myndigheter vet något om sårbarheterna. Dessutom kommer det endast vara en mycket begränsad mängd personer som har kännedom om de tekniker som används vid hemlig dataavläsning och därmed också om eventuella sårbarheter. Dessa personer kommer också att ha genomgått noggranna säkerhetskontroller varför risken för sprid-

Lunds universitets internetinstitut Stefan Larsson. Artikeln finns publicerad digitalt på Dagens juridiks webbsida www.dagensjuridik.se/2016/06/debatt-stefan-larsson-I.

ning utanför den skara personer som känner till sårbarheterna är synnerligen liten.

Vår sammanvägda bedömning är att det inte bör införas någon rapporteringsskyldighet avseende de tekniker som ska användas för verkställighet. Däremot kommer givetvis 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, vara oförhindrade att rapportera dessa. I vissa fall kan det till och med ligga i de brottsbekämpande myndigheternas eget intresse att rapportera sådant, t.ex. då den brottsbekämpande myndigheten bedömer att ett hål som upptäckts kan utnyttjas av kriminella personer på ett sätt som gör att det finns risk för allmän ordning och säkerhet eller allmänhetens skydd (jfr 1 § polislagen)

10.10.2 Teknikanpassning av verkställighetsteknik

Utredningens förslag: En särskild regel om att den teknik som används för verkställighet ska anpassas efter det tillstånd som meddelats införs så att det inte är möjligt att läsa av eller ta upp någon annan uppgiftstyp än den som tillståndet avser.

Om andra typer av uppgifter än tillståndet avser ändå lästs av eller tagits 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 användas i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser.

Tekniken måste i det enskilda fallet begränsas utifrån tillståndet

Teknik som får användas i samband med verkställighet av hemlig dataavläsning kan användas för att läsa av eller ta upp olika typer av uppgifter. Vi har föreslagit att det i lagen om hemlig dataavläsning ska tas in en förteckning avseende vilka uppgiftstyper metoden alls kan få användas för att läsa av eller ta upp och att det i tillståndet ska

anges vilken eller vilka uppgiftstyper tillståndet avser, se avsnitt 10.3 och 10.9.4. Det följer redan av ändamålsprincipen att endast uppgifter som tillståndet avser får läsas av eller tas upp. Om teknik används för att läsa av eller ta upp en annan uppgiftstyp än en som tillståndet avser är det således fråga om en olaglig åtgärd, vilken dessutom skulle kunna bedömas som ett straffbart dataintrång.

Även om det kan och bör förutsättas att de brottsbekämpande myndigheterna rättar sig efter de regler som gäller så att man inte, trots att det vore teoretiskt möjligt, utnyttjar tekniken för annat än det som tillståndet avser finns en risk för ryktesspridning och misstro mot åtgärden om inte också den faktiska möjligheten att utnyttja tekniken på ett icke avsett vis begränsas, se diskussion om detta i avsnitt 9.5.4. Det bör därför införas en bestämmelse som anger vilka anpassningar av tekniken den brottsbekämpande myndigheten måste göra i samband med verkställighet. En sådan regel bör lämpligen ange att den teknik som används i samband med verkställighet i ett enskilt fall ska utesluta avläsning eller upptagning av annan typ av uppgift än sådan som tillståndet avser. Utredningen har av tekniska experter vid de brottsbekämpande myndigheterna försäkrats om att det är möjligt att anpassa verkställighetstekniken på det sätt som vi föreslår. Vi har inte funnit anledning att ifrågasätta denna uppgift.

Behövs ett förbud mot att använda otillåten tilläggsinformation?

Det ska således inte vara praktiskt möjligt att läsa av eller ta upp annan typ av uppgift än sådan som tillståndet avser. Med annan typ av uppgift avses inte det som brukar kallas för överskottsinformation, dvs. uppgifter som i och för sig får hämtas in enligt ett tvångsmedelstillstånd men som inte har samband med skälen för tvångsmedelsbeslutet. De uppgifter som den brottsbekämpande myndigheten läser av eller tar upp som är av annan uppgiftstyp än den som avses i tillståndet kanske snarare kan kallas för *otillåten tilläggsinformation*. Detta eftersom tillståndet inte tillåter avläsning eller upptagning av uppgifterna. Frågan är om det behövs någon bestämmelse för att begränsa användning av otillåten tilläggsinformation. Med en regel som den som nyss föreslagits kan det tyckas överflödigt med en sådan bestämmelse, eftersom ju själva tanken är att begränsa den

praktiska möjligheten att läsa av eller ta upp andra uppgiftstyper än sådana som tillståndet avser. Om en korrekt anpassning av tekniken inte har skett kan det således komma i fråga med avläsning eller upptagning av otillåten tilläggsinformation. Har anpassning inte gjorts torde dessutom såväl straffrättsliga som disciplinära åtgärder kunna aktualiseras för den eller de som ansvarar för dataavläsningen.

Icke desto mindre råder, som en grundläggande regel, fri bevisprövning och fri bevisvärdering i Sverige, vilket bl.a. innebär att det är möjligt att inför domstol åberopa uppgifter utan begränsningar i bevismöjligheterna med hänsyn till en viss beviskällas art.[41] Det betyder således att även om personer vid den verkställande myndigheten kan ställas inför rätta på grund av sättet som viss bevisning åtkommits så hindras som utgångspunkt inte användningen av olagligt avlästa eller upptagna uppgifter i ett domstolsförfarande utan en särskild förbudsregel.

Enligt vår uppfattning innebär det anförda att det bör regleras särskilt vad som ska gälla för otillåten tilläggsinformation. Att inte reglera detta skulle, trots vårt förslag om anpassning, kunna uppfattas som att det i vissa fall vore möjligt eller rentav fördelaktigt att underlåta anpassning av tekniken för att kunna läsa av fler uppgiftstyper än tillståndet tillåter. Teknikerna för verkställighet i samband med hemlig dataavläsning uppvisar, när det gäller den teoretiska möjligheten till avläsning av otillåten tilläggsinformation, säregenhet jämfört med andra verkställighetstekniker. Det finns risk för misstro och ryktesspridning om det kan uppfattas som att brottsbekämpningen skulle gynnas av underlåten anpassning av tekniken. Detta leder oss till slutsatsen att frågan om otillåten tilläggsinformation bör regleras särskilt.

Eftersom det inte bara skulle stå i strid med sed och moral att utnyttja otillåten tilläggsinformation utan framförallt att avläsning eller upptagning av sådan kan innebära brott mot såväl regeringsformen som Europakonventionen finns skäl att inta ett strängt förhållningssätt beträffande användning av otillåten tilläggsinformation. Det ligger enligt vår mening närmast till hands att betrakta otillåten tilläggsinformation på motsvarande vis som annan förbjuden information, t.ex. uppgifter som omfattas av beslagsförbudet i 27 kap. 2 § rättegångsbalken eller uppgifter som omfattas av frågeförbudet i

[41] Se t.ex. prop. 2004/05:143 s. 36.

36 kap. 5 § rättegångsbalken. I analogi med vad som gäller för sådana uppgifter bör otillåten tilläggsinformation inte alls kunna komma till användning. Det bör därför föreskrivas att om det, trots den anpassning av tekniken som ska ske, kommer fram att fel typ av uppgifter har lästs av eller tagits upp så ska upptagningar av sådana uppgifter omedelbart förstöras.

Dessutom bör brottsbekämpande myndigheter åläggas att underrätta tillsynsmyndigheten om ett så allvarligt fel som avläsning eller upptagning av uppgifter i strid med vad som anges i tillståndet. Detta bör göras för att tydliggöra att ett sådant fel är allvarligt och för att tidigt ge tillsynsmyndigheten upplysning om ett potentiellt tillsynsärende.

I reglerna om interimistiska åklagarbeslut finns ett förbud mot att i en brottsutredning till nackdel för den som har omfattats av åtgärden, eller för någon annan som uppgifterna avser, använda uppgifter som hämtats in efter ett åklagarbeslut som sedan upphävts av rätten se avsnitt 10.9.5. När den regleringen infördes i rättegångsbalken konstaterade regeringen att inhämtningen i sig innebär ett intrång i den enskildes privatliv som kan uppfattas som integritetskränkande. Att använda uppgifterna i en brottsutredning mot en person kan sägas innebära att integritetsintrånget tillåts fortsätta. Lämpligheten av att fritt kunna använda uppgifter som framkommit vid ett interimistiskt beslut som upphävs av domstol kunde därför enligt regeringens mening ifrågasättas (prop. 2011/12:55 s. 80). Motsvarande resonemang gör sig gällande för uppgifter som den brottsbekämpande myndigheten läst av eller tagit upp i strid med ett tillstånd. Det bör därför införas en motsvarande reglering för sådana uppgifter i lagen om hemlig dataavläsning.

10.10.3 Aktsamhetskrav och informationssäkerhet i samband med verkställighet

Utredningens förslag: 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 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 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.

En allmän aktsamhetsregel införs vid verkställighet

Proportionalitetsprincipen gäller i alla stadier av tvångsmedelsanvändning, således även när verkställighet ska ske. Trots detta finns det bland tvångsmedelsreglerna särskilda regler som påminner om att det ska finnas ett proportionalitetstänkande också i samband med verkställighet. Sådana exempel finns i 28 kap. 6 § rättegångsbalken avseende husrannsakan och 27 kap. 25 a § femte stycket rättegångsbalken avseende hemlig kameraövervakning och rumsavlyssning och innebär att när sådana åtgärder verkställs får olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt. Vi gör bedömningen att motsvarande generella aktsamhetskrav uttryckligen bör anges i lagen om hemlig dataavläsning. Det ska sägas att det ligger i den verkställande myndighetens intresse att inte orsaka olägenhet eller skada i samband med verkställighet, eftersom detta kan riskera att röja åtgärden.

Särskilt om informationssäkerhet

I föregående kapitel har vi framhållit att det finns risker för informationssäkerheten som måste balanseras om hemlig dataavläsning ska kunna införas. Vi har också tidigare i detta kapitel nämnt att risker för informationssäkerheten bör föranleda vissa särskilda bestämmelser.

I mitten på 1990-talet avfärdade regeringen motsvarigheter till hemlig dataavläsning genom att (i anslutning till en diskussion om hemlig avlyssning och övervakning av elektronisk kommunikation) uttala att av ”hänsyn till informationssäkerheten och skyddet för den enskilde bör den som företar en verkställighetsåtgärd inte få göra några ingrepp via telenät i de datorer m.m. som används för att befordra telemeddelanden”.[42] Vad som mer i detalj avsågs med uttalandet utvecklades emellertid inte närmare, inte heller förklarades vad som innefattades i begreppet informationssäkerhet.

I den s.k. NISU-utredningens betänkande *Informations- och cybersäkerhet i Sverige* (SOU 2015:23) angavs informationssäkerhet vara en strävan att skydda information så att:

– Informationen alltid finns när den behövs (tillgänglighet)
– Det går att lita på att informationen är korrekt och inte manipulerad eller förstörd (riktighet)
– Endast behöriga personer får ta del av informationen (konfidentialitet)
– Det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet)

Utredningen anförde också att informationssäkerhet omfattar såväl administrativa åtgärder för att skydda information (såsom föreskrifter, behörighetsrutiner, etc.) som tekniska åtgärder (såsom it-säkerhet och fysisk inpasseringskontroll).[43]

Som antyds i det betänkandets titel diskuterades också frågor om cybersäkerhet i betänkandet. Beträffande detta begrepp anförde utredningen bl.a. att det omfattar de mekanismer och åtgärder som används för att skydda cyberdomänen, både civilt och militärt, mot de hot som är förknippade med eller som kan skada dess ömsesidigt beroende nätverk och informationsinfrastruktur. Cybersäkerhet strävar efter att bevara nätverkens och infrastrukturens tillgänglighet och integritet samt konfidentialiteten hos informationen däri. Utredningen framhöll emellertid också att begreppen informationssäkerhet och cybersäkerhet ofta används utan särskillnad och att det

[42] Prop. 1994/95:227 s. 25.
[43] SOU 2015:23 s. 42.

för svensk myndighetsintern verksamhet (och med den sammanhängande normgivning) utan tvekan går bra att även framdeles använda begreppet informationssäkerhet.[44] När vi i det följande diskuterar informationssäkerhet använder vi begreppet i vid mening, dvs. innefattande också cybersäkerhet. Vi inkluderar även, möjligen en aning oegentligt, nätsäkerhet, dvs. säkerheten i elektroniska kommunikationsnät, i begreppet.

Det har i olika sammanhang framförts att det finns risk för minskad informationssäkerhet om brottsbekämpande myndigheter tillåts använda tekniker för hemlig dataavläsning.[45] Riskerna som anförs i dessa sammanhang tar sikte på olika avseenden, t.ex. risker för teknisk spridning av programvara utanför 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. Det har varit svårt att under utredningsarbetet få närmare klarhet i hur stora och konkreta risker för informationssäkerheten som verkligen föreligger i olika sammanhang, i synnerhet när det gäller risker hänförliga till teknik som används. Klart är under alla förhållanden att en stark informationssäkerhet är ett så viktigt samhällsintresse att det inte utan vidare kan accepteras att nya åtgärder för att tillgodose brottsbekämpningsintresset får leda till risker för informationssäkerheten för andra än den vars uppgifter ska läsas av eller tas upp.[46] Sådana risker skulle ju för övrigt dessutom kunna verka kontraproduktivt, om de brottsbekämpande myndigheternas verksamhet leder till öppningar för ökad kriminalitet. Det behövs därför, vilket vi också framhållit i föregående kapitel, regler som klargör att risker för informationssäkerheten inte får öka på grund av hemlig dataavläsning.

---

[44] SOU 2015:23 s. 42 f.

[45] Se t.ex. rapporten *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparision of Practices*, tillgänglig via www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf. Se också Bellovin m.fl., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, tillgänglig via http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip

[46] I juni 2017 antogs t.ex. en *Nationell strategi för samhällets informations- och cybersäkerhet* (Skr. 2016/17:213). Dess syfte är bl.a. att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med, höja medvetenheten och kunskapen om samt stödja de insatser och det engagemang som redan finns i samhället för att stärka informations- och cybersäkerheten. Se också redan nämnda SOU 2015:23 och SOU 2016:41, särskilt kapitel 22.

Något om hur informationssäkerhetsfrågan hanterats i andra länders lagstiftning på området

Frågan om informationssäkerhet har om den alls hanterats i andra länders lagstiftning reglerats olika. I Norge krävs enligt den norska straffeprosessloven kap. 16 d. § 216 p andra stycket att dataavläsningen utförs så att det inte onödigtvis skapas fara för driftsstörning eller skada på utrustning eller data. Polisen ska enligt samma bestämmelse så vitt möjligt avvärja fara för att någon, som en följd av åtgärden, kan skaffa sig obehörig åtkomst till datasystemet eller skyddad information. Enligt kompletterande föreskrifter[47] ska det i samband med verkställighet av dataavlesing föras protokoll i vilket det antecknas bl.a. följande.

- Om polisen har brutit eller kringgått skydd i datasystemet.
- Vilka risker datasystemet varit utsatt för vid avläsningen.
- Information om vilka åtgärder som vidtagits för att avvärja fara för driftsstörning eller skada på utrustning eller data.
- Information om risk för att någon, som ett resultat av genomförandet, kan få obehörig åtkomst till datasystemet eller skyddade uppgifter.
- Eventuellt kända skador som dataavläsningen inneburit.
- Vilken personal som utfört dataavläsningen.

Även i andra länders lagstiftning (och förslag till lagstiftning) på området synes vissa regler beträffande informationssäkerhet finnas. Enligt ett italienskt lagförslag som behandlas ska exempelvis krävas att dataavläsningen genomförs av brottsbekämpande myndigheter och inte av privat kontrakterade företag. Vidare krävs enligt förslaget att det, vid varje tillfälle då programvara används för verkställighet, såväl loggas som dokumenteras på ett verifierbart vis. Dessutom får programvaran, när den har installerats, inte minska säkerheten i det informationssystem den riktas mot.

På liknande vis stadgas i tysk rätt att nyckelinformation relaterad till de tekniska metoder som används vid motsvarigheten till data-

[47] Forskrift om kommunikasjonskontroll, romavlytting og dataavlesing (FOR-2016-09-09-1047), vilken på normhierarkisk nivå motsvarar en svensk förordning.

avläsning ska loggas. Den information som avses är benämningen på tekniken som används, vilket datum den används, vilken brottsbekämpande organisation som genomför åtgärden samt identifikationsuppgifter avseende det informationssystem åtgärden riktas mot och inhämtade data.

Nödvändiga åtgärder måste vidtas för upprätthållande av en stark informationssäkerhet

Trots att det är svårt att tydligt redogöra för och kvantifiera de konkreta riskerna för informationssäkerheten med hemlig dataavläsning på ett generellt plan och att perspektivet helt saknas i utredningsdirektiven står det klart att lagen om hemlig dataavläsning måste förses med någon typ av reglering som balanserar informationssäkerhetsrisker. Frågan är då hur en sådan ska se ut.

Till en början kan sägas att vi i föregående kapitel bedömt att det kan accepteras en viss minskning av informationssäkerheten i det informationssystem hemlig dataavläsning enligt tillståndet ska avse under tillståndstiden, men inte utanför detta system, varken i andra informationssystem eller i de nät som informationssystemet är anslutet till. Detta är utgångspunkten för våra förslag här.

Vid avvägningen av hur en bestämmelse på området lämpligen bör utformas har vi beaktat att den antingen kan ha karaktären av förbud eller begränsning (t.ex. att informationssäkerheten i visst avseende inte får minska till följd av hemlig dataavläsning) eller instruktion (t.ex. att nödvändiga åtgärder ska vidtas för att undvika en minskad informationssäkerhet). Vi har stannat för att det senare alternativet är lämpligast eftersom det torde skapa bättre och mer dynamiska förutsättningar för de som har att verkställa åtgärden, utan att för den skull medföra några ökade risker. Dessutom bör en regel som ska balansera risker för informationssäkerheten utformas generellt och neutralt, för att fånga upp de olika typer av risker och situationer som kan uppstå.

Vidare har vi, med viss inspiration från den norska lagstiftningen, konstaterat att det endast bör vara vissa, särskilt kvalificerade, personer som kan komma i fråga för att ansvara för att verkställa hemlig dataavläsning. Denna slutsats hänger samman med att de olika tekniska metoder som kan aktualiseras i samband med verkställighet torde förutsätta särskilda kunskaper, bl.a. på informations-

säkerhetsområdet. Det finns därför, enligt vår mening, skäl att redan i lagtexten ange att det ska finnas en ansvarig för verkställigheten. Lämpligen kan detta ske genom att det uttrycks att *den som ansvarar* för verkställigheten ska vidta vissa åtgärder. Det bör ankomma på de brottsbekämpande myndigheterna att utse ansvariga personer för verkställigheten. Vi återkommer i avsnitt 10.12.4 till vilka kvalifikationskrav som lämpligen bör ställas på den ansvarige.

Den som ansvarar för verkställigheten ska se till att inga åtgärder vidtas som minskar informationssäkerheten utanför informationssystemet. Lämpligen kan detta uttryckas så att den ansvarige ska vidta nödvändiga och tillräckliga åtgärder för att informationssäkerheten utanför det informationssystem tillståndet avser inte åsidosätts, minskas eller skadas till följd av verkställigheten. Med en så generell utformning av bestämmelsen uppnås å ena sidan en neutralitet som möjliggör dynamiska lösningar av den som ansvarar men å andra sidan medför en sådan utformning ett mycket brett ansvarsfält för den ansvarige. Samtidigt kan, mot bakgrund av att det visat sig svårt att bringa klarhet i hur stora riskerna för informationssäkerheten faktiskt kan vara, inget annat än en bred men ändå skarp reglering komma i fråga eftersom informationssäkerheten är ett så väsentligt intresse.

När det gäller riskerna för informationssäkerheten i det informationssystem som tillståndet avser får det, som vi konstaterat i föregående kapitel, accepteras en viss minskning av denna under den tid som avläsningen ska pågå om det är nödvändigt. Redan av den generella aktsamhetsregeln som vi presenterat ovan följer att denna risk, liksom övriga olägenheter och skador, ska begränsas till vad som är absolut nödvändigt. Däremot kan det inte accepteras att informationssäkerheten förblir mindre än vid avläsningens början när åtgärden avslutas.

Åtgärder när verkställighet avslutas

Som vi nyss nämnde kan det inte anses acceptabelt om hemlig dataavläsning får som konsekvens att det informationssystem som tillståndet avser har ett sämre skydd efter att avläsningen avslutats. Detta gäller från både ett informationssäkerhets- och ett integritetsperspektiv. Det bör därför föreskrivas att den verkställande myndig-

heten i samband med att verkställighet avslutas ska vidta de åtgärder som behövs för att säkerheten i det informationssystem som tillståndet avser ska hålla åtminstone samma nivå som vid verkställighetens början. Mer detaljerad än så bör en lagreglering inte vara mot bakgrund av de olika tekniker som ska kunna användas i samband med verkställighet. Det bör dock påpekas att kravet bör gälla oavsett vilken teknik som använts i samband med verkställighet.

När tekniska hjälpmedel (programvara eller hårdvara) har använts i samband med verkställighet bör motsvarande regel som gäller i dag vid hemlig kameraövervakning och hemlig rumsavlyssning gälla, se 27 kap. 25 a § fjärde stycket rättegångsbalken. Den innebär att ett tekniskt hjälpmedel ska tas bort eller göras obrukbart när tvångsmedelsanvändningen avslutas (dvs. när tiden för tillståndet har gått ut eller tillståndet har upphävts). Eftersom det vid hemlig dataavläsning kan komma i fråga att använda programvara som installerats utan fysisk tillgång till det informationssystem som avses bör det av bestämmelsen framgå att det kan vara tillräckligt med avinstallation. Vårt förslag blir därför att ett tekniskt hjälpmedel ska tas bort, avinstalleras eller annars göras obrukbart så snart detta kan ske efter att tiden för tillståndet har gått ut eller tillståndet har upphävts. Det ska således inte vara möjligt för den brottsbekämpande myndigheten att efter tillståndstiden löpt ut (eller åtgärden i förtid avbrutits) kunna utnyttja samma verktyg igen. För att tillgodose kravet bör det exempelvis vara möjligt för den brottsbekämpande myndigheten att ”tidsinställa” ett tekniskt hjälpmedel som används.

10.11 Vissa andra rättssäkerhetsgarantier

10.11.1 Allmänt om rättssäkerhetsgarantier i lagstiftningen om hemliga tvångsmedel

När vi i kapitel 3 skisserade en översikt avseende de nuvarande hemliga tvångsmedlen delade vi in denna i dels materiella förutsättningar för nuvarande hemliga tvångsmedel (avsnitt 3.4), dels rättssäkerhetsgarantier och skyddet för den personliga integriteten i lagstiftningen om hemliga tvångsmedel (avsnitt 3.5). Anledningen till indelningen var pedagogisk men som angavs där utgör även de materiella förutsättningarna i någon mening integritetsskyddsregler och

rättssäkerhetsgarantier eftersom ju hemliga tvångsmedel inte tillåts om de materiella förutsättningarna inte föreligger.

Ett möjligen mer korrekt förhållningssätt är att utgångspunkten är att staten, genom de brottsbekämpande myndigheterna, inte får använda hemliga tvångsmedel mot enskilda. Endast om de särskilda förutsättningar som följer av regeringsformen och Europakonventionen är uppfyllda får undantag göras från denna utgångspunkt. Som vi redovisat i föregående kapitel är det vår bedömning att sådana förutsättningar finns när det gäller hemlig dataavläsning.

Enligt Europakonventionen krävs att reglerna om hemliga tvångsmedel är sådana att deras tillämpning är förutsebar samt att tillräckliga kontrollmekanismer finns för att se till att normer för förutsebarheten efterlevs. Vad avser reglernas utformning har Europadomstolen beträffande dolda spaningsåtgärder (främst avlyssning) utarbetat en minimistandard enligt vilken följande ska framgå.

- Arten av de brott som skulle kunna leda till en begäran om dolda spaningsåtgärder.
- En definition av de personkategorier som skulle kunna riskera att t.ex. få sin telefon avlyssnad.
- En begränsning av åtgärdens varaktighet.
- Förfaranderegler för undersökning, användning och lagring av de uppgifter som inhämtats.
- Försiktighetsåtgärder vid överföring av information till andra parter.
- Angivande av de omständigheter under vilka inspelningarna kan eller måste raderas eller förstöras.

Flera av de krav som enligt Europadomstolens minimistandard ska finnas med i lagstiftning om hemliga tvångsmedel har behandlats redan i det föregående, t.ex. arten av de brott eller den brottslighet som kan föranleda åtgärden och de personkategorier som kan träffas av bestämmelserna. Några av kraven har emellertid ännu inte diskuterats. I detta avsnitt analyseras därför i vad mån de rättssäkerhetsgarantier som gäller enligt nuvarande regler om hemliga tvångsmedel, vilka i många avseenden är ett utflöde av Europadomstolens praxis, ska gälla även för hemlig dataavläsning.

Den svenska regleringen av hemliga tvångsmedel – och dess rättssäkerhetsgarantier – utvärderades av en särskild utredare år 2012 och bedömdes då leva upp till både regeringsformens och Europakonventionens krav (bl.a. avseende den minimistandard som framgår ovan). Utredaren framhöll att det inte av rättssäkerhetsskäl fanns behov av några förändringar av de rättssäkerhetsgarantier som omgärdar tvångsmedelsanvändningen enligt de lagar som utvärderades.[48] Det finns skäl att låta de slutsatserna utgöra en utgångspunkt för våra bedömningar avseende de rättssäkerhetsgarantier som här ska diskuteras.[49]

10.11.2 Överskottsinformation

Utredningens förslag: 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.

Nuvarande regler om användning av överskottsinformation

Överskottsinformation är uppgifter som vid verkställande av tvångsmedel har kommit fram om annat än den brottslighet som har legat till grund för tillståndet. För annat än hemliga tvångsmedel finns i svensk rätt inte någon lagstadgad begränsning av hur överskottsinformation får användas utan där råder reglerna om fri bevis-

[48] Se SOU 2012:44 s. 666.

[49] Det ska anmärkas att regeringen gett Utredningen om datalagring och EU-rätten i uppdrag att se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten vid användning av hemliga tvångsmedel, se Dir. 2017:16. Till dess annat framkommer finns emellertid skäl att utgå från att de slutsatser som redovisades i SOU 2012:44 äger fortsatt giltighet.

prövning och fri bevisföring utan begränsningar, se t.ex. 35 kap. 1 § rättegångsbalken.

Regler om användning av överskottsinformation finns i 27 kap. 23 a § rättegångsbalken, 12 § preventivlagen, 21 a § LSU och 7 och 8 §§ inhämtningslagen. Enligt dessa får överskottsinformation alltid användas för att förhindra förestående brott. I övrigt finns vissa skillnader beroende på vilket tvångsmedel som avses och ändamålet med tvångsmedelsanvändningen.

Bestämmelserna i rättegångsbalken

Enligt rättegångsbalkens regler gäller för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning som huvudregel att överskottsinformation får användas för att utreda brott. Den begränsning som finns för dessa tvångsmedel är att förundersökning eller motsvarande utredning får 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 brott som anges i 27 kap. 20 d § rättegångsbalken (dvs. brott som kan föranleda hemlig rumsavlyssning), eller annat brott, om det är föreskrivet fängelse i tre år eller däröver för brottet.

Bestämmelserna om överskottsinformation i underrättelseverksamhet

Motsvarande bestämmelse som gäller för hemlig rumsavlyssning gäller beträffande användning av överskottsinformation enligt 12 § preventivlagen, dock med den skillnaden att det i stället för brott som kan föranleda hemlig rumsavlyssning ska vara fråga om brott (eller försök, förberedelse eller stämpling till sådant brott) som kan föranleda tvångsmedelsanvändning enligt den lagen. Enligt 21 a § LSU gäller samma förutsättningar för användande av överskotts-

information som gäller för hemlig avlyssning och övervakning av elektronisk kommunikation enligt rättegångsbalken.

Enligt 7 § inhämtningslagen gäller att om det vid inhämtning av uppgifter enligt den lagen har kommit fram uppgifter om annan brottslig verksamhet än sådan som omfattas av beslutet om inhämtning så får uppgifterna användas för att förhindra brott. Enligt 8 § inhämtningslagen 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.

Bakgrund till nuvarande bestämmelser om överskottsinformation

Regleringen i 27 kap. rättegångsbalken om överskottsinformation från hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning infördes den 1 juli 2005. Dessförinnan hade frågan diskuterats och utretts under flera årtionden. Diskussionen avsåg bl.a. om en sådan reglering var nödvändig på grund av de krav som ställs upp i regeringsformen och Europakonventionen. Regeringen bedömde i förarbetena till 2005 års lagändring dels att artikel 8 i Europakonventionen och Europadomstolens praxis tydligt talade för att användningen av överskottsinformation borde regleras, dels att det fick anses bäst överensstämma med integritetsskyddet i regeringsformen att grundläggande bestämmelser ges i lag om hur och i vilken omfattning överskottsinformation från telefonavlyssning får användas (prop. 2004/05:143 s. 30).

Frågan var då hur regleringen skulle utformas. Regeringen konstaterade att Europakonventionen inte innehåller något förbud mot att använda överskottsinformation från hemliga tvångsmedel för att utreda och bevisa brott. Vidare bedömde regeringen att varken integritetsintresset eller risken för missbruk av tvångsmedlen i sig utgjorde skäl att begränsa möjligheterna att använda överskottsinformation. När det gäller integritetsintresset motiverades det med att intresset hos den som begått ett brott att inte avslöjas som brottsling inte kunde räknas till ett skyddsvärt sådant intresse. Däremot konstaterades att de brottsbekämpande myndigheterna

inte verkade ha något generellt behov av att använda sådan information som bevis. Från myndighetshåll hade det framhållits bl.a. att det allmänt sett inte var rimligt att åberopa uppgifter från hemlig avlyssning av elektronisk kommunikation för att bevisa exempelvis ett snatteri eller en ringa misshandel. Regeringen ansåg därför att övervägande skäl talade för att begränsa användningen av överskottsinformation vid utredning om mindre allvarliga brott (prop. 2004/05:143 s. 32 f.)

När det gäller de strängare reglerna beträffande hemlig rumsavlyssning och tvångsmedelsanvändning enligt preventivlagen ska först sägas att dessa innebär ett lägre ställt krav än vad som gällde tidigare. Ändringarna, som gjordes år 2014, föranleddes bl.a. av att Utredningen om vissa hemliga tvångsmedel i sitt betänkande *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44) presenterade en utvärdering som visade att de strängare reglerna hade lett till att tydlig information om mycket allvarliga brott (bl.a. mord och människohandel) inte kunde användas. Dessutom visade utvärderingen att det inte fanns några omständigheter som talade för att hemliga tvångsmedel användes i det otillbörliga syftet att generera överskottsinformation. Regeringen fann, till skillnad från utredningen (som föreslog helt enhetliga överskottsinformationsregler), att det fanns skäl att ställa upp högre krav för att överskottsinformation från hemlig rumsavlyssning ska få användas jämfört med vad som gäller enligt 27 kap. rättegångsbalken eftersom hemlig rumsavlyssning ofta genererar betydande mängder kringinformation. Även beträffande de preventiva tvångsmedlen enligt preventivlagen fann regeringen att det fanns anledning att vara mer restriktiv eftersom dessa normalt används i ett skede innan något brott har begåtts. Någon ändring beträffande LSU gjordes dock inte.

Användning av överskottsinformation vid hemlig dataavläsning

Vi har redan förklarat att om uppgifter läses av eller tas upp som inte är av den uppgiftstyp som tillståndet avser, s.k. otillåten tilläggsinformation, så får dessa uppgifter inte användas, se avsnitt 10.10.2. Frågan om hur överskottsinformation ska få användas vid hemlig dataavläsning bör därför bedömas utifrån den uppgiftstyp tillståndet avser.

En naturlig första utgångspunkt är att låta reglerna om överskottsinformation i lagen om hemlig dataavläsning följa de regler som gäller för sådan information för ”bakomliggande” hemliga tvångsmedel. Reglerna om användning av överskottsinformation skiljer sig emellertid åt en aning beroende på om hemliga tvångsmedel används i förundersöknings- eller underrättelseverksamhet. Det framstår därför som rimligt att låta reglerna om användning av överskottsinformation i lagen om hemlig dataavläsning utformas olika beroende på ändamålet för åtgärden.

Vi har tidigare gjort bedömningen att hemlig dataavläsning för att läsa av eller ta upp lagrade uppgifter eller uppgifter som visar hur ett informationssystem används motsvarar hemlig avlyssning av elektronisk kommunikation såvitt avser integritetsrisker, se t.ex. avsnitt 10.5.1. Denna slutsats bör vara utgångspunkt även vid bedömningen av hur användning av överskottsinformation när hemlig dataavläsning avser sådana uppgifter ska göras.

I 27 kap. 23 a § rättegångsbalken görs skillnad mellan å ena sidan överskottsinformation vid hemlig avlyssning eller övervakning av elektronisk kommunikation och hemlig kameraövervakning och å andra sidan överskottsinformation vid hemlig rumsavlyssning. För att i lagen om hemlig dataavläsning uppnå överensstämmelse med denna reglering bör det göras motsvarande skillnad mellan å ena sidan överskottsinformation vid hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter och å andra sidan överskottsinformation vid hemlig dataavläsning när åtgärden används för att läsa av eller ta upp någon av de övriga uppgiftstyperna. I det förra fallet bör motsvarande gälla som gäller för hemlig rumsavlyssning enligt 27 kap. 23 a § andra stycket rättegångsbalken och i det senare fallet bör motsvarande gälla som gäller för övriga hemliga tvångsmedel enligt 27 kap. 23 a § första stycket rättegångsbalken.

När det gäller överskottsinformation i underrättelseverksamhet bör motsvarande gälla för hemlig dataavläsning i de olika underrättelsefallen som gäller enligt 12 § preventivlagen, 21 a § LSU och 7 och 8 §§ inhämtningslagen.

Lämpligen kan rättegångsbalkens, preventivlagens, LSU:s och inhämtningslagens regler om användning av överskottsinformation göras direkt tillämpliga genom hänvisningar i lagen om hemlig dataavläsning med de förtydliganden som krävs.

10.11.3 Granskning, bevarande och förstörande av upptagningar och upptecknin gar vid hemlig dataavläsning

Utredningens förslag: Under förundersökning ska det som gäller för hemlig avlyssning av elektronisk kommunikation beträffande granskning, bevarande och förstörande av upptagningar och upptecknin gar gälla för hemlig dataavläsning. I de fall särreglering av hemlig rumsavlyssning görs ska dock motsvarande gälla när hemlig dataavläsning avser eller har avsett rumsavlyssningsuppgifter.

I underrättelsefallen ska motsvarande det som gäller för granskning, bevarande och förstörande av upptagningar och upptecknin gar enligt preventivlagen, LSU och inhämtningslagen gälla även för hemlig dataavläsning.

Nuvarande regler om granskning, bevarande och förstörande av upptagningar eller upptecknin gar vid användning av hemliga tvångsmedel

Regler om granskning, bevarande och förstörande av upptagningar eller upptecknin gar vid användning av hemliga tvångsmedel finns i 27 kap. 24 § rättegångsbalken, 13 § preventivlagen, 22 § LSU och 9 § inhämtningslagen. Upptagningar eller upptecknin gar som har gjorts under förundersökning vid hemlig tvångsmedelsanvändning ska granskas snarast möjligt och ska, i de delar som är av betydelse från brottsutredningssynpunkt, som huvudregel, bevaras till dess förundersökningen lagts ned eller, om åtal väcks, målet har avgjorts slutligt. I de delar upptagningarna eller upptecknin garna är av betydelse för att förhindra förestående brott, ska de bevaras så länge det behövs för att förhindra brott. De ska därefter förstöras.

Som en specialregel gäller, trots kravet på förstörande, att brottsbekämpande myndigheter får behandla uppgifter från upptagningar och upptecknin gar i enlighet med vad som är särskilt föreskrivet i lag, vilket kan vara fallet om det har kommit fram uppgifter som får behandlas i register eller på annat sätt enligt de förutsättningar som ställs upp i exempelvis polisdatalagen. 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 däröver för brottet.

Vid tvångsmedelsanvändning enligt preventivlagen gäller i stort sett motsvarande regel som enligt rättegångsbalken såvitt avser granskning, bevarande och förstörande av upptagningar eller uppteckningar. Dock gäller, såvitt avser bevarandeskyldigheten, att det endast är i de delar upptagningarna och uppteckningarna innehåller uppgifter om brott som enligt 12 § preventivlagen får användas för att utreda brott som upptagningarna eller uppteckningarna ska bevaras till dess att förundersökningen har lagts ned eller avslutats eller, om åtal har väckts, målet har avgjorts slutligt. Enligt preventivlagen får också uppgifter från upptagningar och uppteckningar behandlas i enlighet med vad som är särskilt föreskrivet i lag om uppgifterna rör förestående brott eller brott som kan föranleda tvångsmedelanvändning enligt preventivlagen, eller försök, förberedelse eller stämpling till ett sådant brott, om en sådan gärning är belagd med straff, eller ett annat brott för vilket det är föreskrivet fängelse i tre år eller däröver.

Såvitt avser LSU gäller i allt väsentligt motsvarande regler som i rättegångsbalken genom hänvisning dit (22 §). Dock föreskrivs särskilt att om upptagningen eller uppteckningen innehåller något som inte är av betydelse för ändamålet med tvångsmedelsanvändningen så ska den i denna del omedelbart förstöras efter granskningen.

Enligt 9 § inhämtningslagen ska uppteckningar av uppgifter granskas snarast möjligt. Uppteckningar ska, i de delar de är av betydelse för att förebygga, förhindra eller upptäcka brottslig verksamhet som omfattas av beslutet om inhämtning eller för att förhindra annat brott, bevaras så länge det behövs för något av dessa syften. De ska därefter förstöras. Detta hindrar dock inte att brottsbekämpande myndigheter behandlar uppgifter från uppteckningar i enlighet med vad som är särskilt föreskrivet i lag.

Vår bedömning avseende granskning, bevarande och förstörande av upptagningar och uppteckningar vid hemlig dataavläsning

Liksom beträffande överskottsinformation är det en naturlig första utgångspunkt att låta reglerna om granskning, bevarande och förstörande av upptagningar och uppteckningar i lagen om hemlig

dataavläsning följa de regler som gäller för sådan information för ”bakomliggande” hemliga tvångsmedel. Även i detta sammanhang bör då hemlig dataavläsning avseende lagrade uppgifter och uppgifter som visar hur ett informationssystem används motsvara vad som gäller för hemlig avlyssning av elektronisk kommunikation. Eftersom reglerna skiljer sig åt en aning beroende på om hemliga tvångsmedel används i förundersöknings- eller underrättelseverksamhet är det också i detta sammanhang rimligt att låta bestämmelser om granskning, bevarande och förstörande av upptagningar och uppteckningar i lagen om hemlig dataavläsning utformas olika beroende på ändamålet för åtgärden.

I förundersökningsfallen bör lämpligen det som enligt 27 kap. 24 § rättegångsbalken gäller för hemlig avlyssning av elektronisk kommunikation gälla även för hemlig dataavläsning. Eftersom emellertid hemlig rumsavlyssning enligt 27 kap. 24 § rättegångsbalken i viss mån särregleras bör när hemlig dataavläsning används för rumsavlyssningsuppgifter motsvarande det som gäller för hemlig rumsavlyssning i stället gälla.

Såvitt avser granskning, bevarande och förstörande av upptagningar och uppteckningar i de olika underrättelsefallen bör det gälla för hemlig dataavläsning som gäller enligt 13 § preventivlagen, 22 § LSU och 9 § inhämtningslagen.

Lämpligen kan rättegångsbalkens, preventivlagens, LSU:s och inhämtningslagens regler om granskning, bevarande och förstörande av upptagningar och uppteckningar göras direkt tillämpliga genom hänvisningar i lagen om hemlig dataavläsning med de förtydliganden som krävs.

Det bör påpekas att vi gör bedömningen att det omfattande arbete som för närvarande pågår beträffande behandling av personuppgifter som samlas in i brottsbekämpande myndigheters verksamhet inom ramen för EU:s dataskyddsreform inte direkt påverkar våra förslag i denna del. I den mån ny lagstiftning om skydd för personuppgifter antas kan sådan emellertid, i vart fall indirekt, påverka våra förslag här, t.ex. om det i lag föreskrivs om andra förutsättningar för behandling av uppgifterna. Sådana ändringar bör uppmärksammas i det fortsatta beredningsarbetet.[50]

[50] Se t.ex. förslag i SOU 2017:29 och 2017:74, vilka för närvarande bereds. Såvitt vi kan bedöma bör dock inte de regler som där föreslås påverka våra förslag.

10.11.4 Underrättelse till enskild om hemlig dataavläsning

Utredningens förslag: 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 preventivlagsfallen. De särskilda regler som gäller för hemlig kameraövervakning och hemlig rumsavlyssning ska tillämpas även för hemlig dataavläsning avseende kameraövervakningsuppgifter och rumsavlyssningsuppgifter.

Nuvarande regler om underrättelse till enskild om att denne varit utsatt för hemliga tvångsmedel

Regler om i vilka fall underrättelse ska lämnas till enskild om hemliga tvångsmedel under förundersökning finns i 27 kap. 31–33 §§ rättegångsbalken. Huvudregeln är att den som är eller har varit misstänkt för ett brott ska underrättats om tvångsmedelsanvändningen i efterhand. Även vissa innehavare av platser (när hemlig kameraövervakning och rumsavlyssning har avsett en plats som innehas av någon annan än den misstänkte) och innehavarare av telefonnummer, adresser och utrustningar (när hemlig avlyssning eller övervakning av elektronisk kommunikation avsett sådana som innehas av annan än misstänkt) ska underrättas om tvångsmedelsanvändningen i efterhand. Underrättelseskyldigheten omfattar bl.a. vilka tvångsmedel som använts, vilken plats, adress eller utrustning som övervakats eller avlyssnats samt när detta har skett.

Flera undantag finns från underrättelseskyldigheten. Bl.a. undantas fall där uppgifterna omfattas av utrikessekretess, försvarssekretess, förundersökningssekretess eller sekretess i underrättelseverksamhet. Har det på grund av sekretess inte kunnat lämnas någon underrättelse inom ett år från det att förundersökningen avslutades, behöver det inte lämnas någon underrättelse. Då ska dock Säkerhets- och integritetsskyddsnämnden underrättas, se 14 b § förundersökningskungörelsen. Förundersökningar angående ett antal brott som normalt handläggs av Säkerhetspolisen undantas också helt från underrättelseskyldighet.

I preventivlagen regleras frågan om underrättelse till enskild i 16–18 §§. För preventivlagen kan motsatt huvudregel sägas gälla för de flesta av de brottskategorier som upptas i brottskatalogen i den lagen, nämligen att underrättelse inte ska ske om tvångsmedelsanvändningen. Det hänger samman med att de brott som undantas från underrättelseskyldigheten är brott som faller inom Säkerhetspolisens verksamhetsområde, vilket alltså utgör en stor del av brotten som kan föranleda preventiv tvångsmedelsanvändning enligt lagen. När det däremot är fråga om brott som faller inom Polismyndighetens verksamhetsområde, dvs. mord, dråp, grov misshandel, synnerligen grov misshandel, människorov och olaga frihetsberövande i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd, gäller som huvudregel att underrättelse till den som utsatts för hemliga tvångsmedel ska ske. I dessa fall motsvarar bestämmelserna om underrättelseskyldighet, och undantag från denna, i allt väsentligt reglerna enligt rättegångsbalken, dock givetvis med de skillnader som följer av att det inte pågår någon förundersökning och att det därmed inte finns någon skäligen misstänkt för brott.

När det gäller LSU finns ingen underrättelseskyldighet. Detta har motiverats av att lagen angår terroristbrott och att därför samma skäl gör sig gällande för att undanta tvångsmedelsanvändningen enligt denna lag från underrättelseskyldigheten som motiverat att sådana brott bör undantas från underrättelseskyldigheten vid förundersökningar i brottmål.[51] Inte heller enligt inhämtningslagen gäller någon underrättelseskyldighet.

Vår bedömning beträffande underrättelse till enskild om att denne varit föremål för hemlig dataavläsning

De regler som gäller för underrättelse till enskilda om att de varit föremål för hemlig tvångsmedelsanvändning framstår som väl avvägda, se om skälen bakom regleringen bl.a. i prop. 2006/07:133. Reglerna kan också, tillsammans med andra rättssäkerhetsgarantier, förväntas bidra till uppfyllnaden av kraven i artikel 13 i Europa-

[51] Prop. 2006/07:133 s. 52.

konventionen om rätten till effektiva rättsmedel, vilka för hemliga tvångsmedel är särpräglade mot bakgrund av att den som utsätts inte är medveten om eventuella rättighetskränkningar.[52]

Vår sammantagna bedömning är att underrättelseskyldighet ska gälla för hemlig dataavläsning på motsvarande vis som sådan föreligger för andra hemliga tvångsmedel i dag. Som utgångspunkt bör gälla att det som anges beträffande underrättelseskyldighet vid hemlig avlyssning av elektronisk kommunikation i rättegångsbalken (när hemlig dataavläsning används i förundersökningsfallen) eller preventivlagen (när hemlig dataavläsning används i preventivlagsfallen) ska gälla även vid hemlig dataavläsning. När det är fråga om hemlig dataavläsning avseende kameraövervakningsuppgifter eller rumsavlyssningsuppgifter bör de tillkommande skyldigheter som gäller för hemlig kameraövervakning eller hemlig rumsavlyssning gälla.

Lämpligen kan rättegångsbalkens och preventivlagens regler om underrättelse till enskild göras tillämpliga genom hänvisningar i lagen om hemlig dataavläsning med de förtydliganden som krävs.

10.12 Några särskilda frågor

10.12.1 Tillsynsfrågor

Utredningens förslag: När domstol har meddelat beslut att tillåta hemlig dataavläsning ska Säkerhets- och integritetsskyddsnämnden underrättas om beslutet.

Utredningens bedömning: 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.

[52] Se t.ex. Danelius, *Mänskliga rättigheter i europeisk praxis*, femte uppl., s. 547 f.

Säkerhets- och integritetsskyddsnämndens uppdrag och arbete

Säkerhets- och integritetsskyddsnämnden (nämnden) inrättades den 1 januari 2008. Syftet med myndigheten är att den ska bidra till att värna rättssäkerheten och skyddet för den personliga integriteten i förhållande till den brottsbekämpande verksamheten.

Nämnden har enligt 1 och 2 §§ lagen om tillsyn över viss brottsbekämpande verksamhet (tillsynslagen) till uppgift att med inspektioner och andra undersökningar utöva tillsyn över de brottsbekämpande myndigheternas användning av bl.a. hemliga tvångsmedel. Tillsynen ska särskilt syfta till att säkerställa att de brottsbekämpande myndigheternas verksamhet bedrivs i enlighet med lag och andra författningar. Tillsynen omfattar inte domstolarna.

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 efter sin utredning kan konstatera att ingen tvångsmedelsanvändning har förekommit eller att sådan användning visserligen förekommit men skett lagenligt, får den enskilde normalt besked av nämnden att den inte funnit någon olaglig tvångsmedelsanvändning. Skulle den emellertid vid sin kontroll finna att någon brottsbekämpande myndighet i strid med gällande författningar har använt hemliga tvångsmedel ska den person som har begärt kontrollen underrättas även om detta. Nämnden är då också skyldig att efter omständigheterna anmäla den författningsstridiga verksamhet den funnit till Justitiekanslern, Åklagarmyndigheten, Datainspektionen eller någon annan behörig myndighet för åtgärd. Det sista följer av 20 § förordningen med instruktion för Säkerhets- och integritetsskyddsnämnden (nämndinstruktionen). I nämndinstruktionen finns också en del förfaranderegler när det gäller handläggningen av tillsynsärenden. Av särskild betydelse här är 18 § som anger att nämnden vid handläggningen av ett ärende som kräver särskild kompetens får förordna en sakkunnig person till att biträda nämnden.

När Utredningen om vissa hemliga tvångsmedel gjorde en omfattande utvärdering av den hemliga tvångsmedelsanvändningen i Sverige gjordes vissa uttalanden om nämnden. Utredningen framhöll bl.a. följande.

> De uppgifter som kommit fram om Säkerhets- och integritetsskyddsnämndens verksamhet ger goda indikationer på att tvångsmedelsregleringens tillämpning hos de aktuella myndigheterna skett enligt gällande regler och varit i hög grad förutsebar. Nämndens granskning synes också ha varit en väl fungerande kontrollmekanism som i de fall där brister ändå kommit fram lett till att åtgärder vidtagits med anledning av dessa.[53]

Även Riksrevisionen har granskat nämnden. Resultatet av granskningen redovisades i rapporten Tillsyn över brottsbekämpande myndigheter – En granskning av Säkerhets- och integritetsskyddsnämnden.[54] Även enligt den rapporten framstår det som att nämnden bedriver sin verksamhet på ett ändamålsenligt sätt och att dess tillsyn leder till åtgärder hos de brottsbekämpande myndigheterna när det gäller regelefterlevnad.[55]

Kan Säkerhets- och integritetsskyddsnämnden utöva tillsyn även beträffande hemlig dataavläsning?

Säkerhets- och integritetsskyddsnämnden har nu nästan tio års arbete bakom sig med att utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel. Såvitt framkommit av de granskningar som gjorts av nämndens arbete synes tillsynen fungera väl och dessutom förefaller de brottsbekämpande myndigheterna följa nämndens uttalanden på ett ändamålsenligt vis. Redan dessa omständigheter talar med styrka för att låta nämnden utöva tillsyn också över användningen av hemlig dataavläsning. Vad som i än högre utsträckning talar för att låta så ske är att åtgärden i flera avseenden kan anses vara en förlängning av nuvarande hemliga tvångsmedel. När det gäller den del av hemlig dataavläsning som i praktiken innebär det nya, dvs. avläsning eller upptagning av lagrade uppgifter eller uppgifter som visar hur ett informationssystem används, gör vi bedömningen att denna åtgärd inte i något avgörande avseende skiljer ut sig från övriga hemliga tvångsmedel på ett sätt som ger anledning att ifrågasätta att Säkerhets- och integritetsskyddsnämnden ska vara den myndighet som bör utöva tillsyn. Det

[53] SOU 2012:44 s. 667.
[54] RiR 2016:12.
[55] Se RiR 2016:12 s. 8 och 10 f.

anförda leder sammantaget till att Säkerhets- och integritetsskyddsnämnden kan och bör vara den myndighet som utövar tillsyn även över användningen av hemlig dataavläsning.

Krävs det några författningsändringar om hemlig dataavläsning införs?

Nästa fråga att ställa sig är då om det finns behov av ändringar i det nuvarande regelverket för att det ska finnas laglig grund för nämndens tillsyn över användningen av hemlig dataavläsning. Det kan konstateras att de regler som styr nämndens verksamhet är neutralt utformade på ett sätt som gör att den ska utöva tillsyn över all hemlig tvångsmedelsanvändning. Det innebär att en ny lag om hemlig dataavläsning automatiskt kommer att falla in under nämndens tillsyn om inte annat anges. Vi gör därför bedömningen att det inte krävs några författningsändringar i det avseendet. Reglerna beträffande nu aktuell tillsyn lämnar också stor frihet till nämnden att själv bestämma hur tillsynsarbetet ska genomföras. Detta är enligt vår mening något positivt även såvitt avser tillsyn över användning av hemlig dataavläsning. Det finns därför inte heller några skäl att göra ändringar i detta avseende.

Det kommer att behövas teknisk kompetens vid tillsynsmyndigheten

När det gäller tillsynen över användningen av hemlig dataavläsning är det dock mycket som talar för att nämnden kan behöva komplettera sin tekniska kompetens. I synnerhet gäller detta i tillsynen av verkställighetsfasen där vi ju föreslagit regler som, av hänsyn till den personliga integriteten och intresset av en stark informationssäkerhet, är mycket viktiga. Att det sker en reell, effektiv och aktiv tillsyn av att reglerna om hemlig dataavläsning följs kan vara avgörande för tvångsmedlets legitimitet.

För att våra förslag om att åtgärder ska vidtas av den verkställande myndigheten för att se till att andra uppgiftstyper än de som tillståndet avser inte kan läsas av eller tas upp och för att säkerställa informationssäkerheten utanför informationssystemet som tillståndet avser krävs personer med särskild teknisk kompetens för att till-

synen ska kunna bli tillräcklig. Det är för övrigt inte bara våra förslag i de nu nämnda delarna som kan fordra sådan kompetens utan redan tvångsmedlets synnerligen tekniska karaktär torde innebära att den som har att granska användningen av åtgärden, för att helt förstå det som granskas, behöver mycket god kännedom om tekniken som används.

En särskild bestämmelse om underrättelse till Säkerhets- och integritetsskyddsnämnden bör införas

Nämnden har stor frihet att själv välja hur och när tillsyn av hemliga tvångsmedel ska genomföras. Så bör gälla även när tillsyn avseende hemlig dataavläsning ska utövas. Vår bedömning är emellertid att det kan behövas en mer aktiv tillsyn vid hemlig dataavläsning än vad som är fallet vid tillsynen avseende övriga hemliga tvångsmedel. Det hänger särskilt samman med riskerna för informationssäkerheten som kan uppstå om de förhållningsregler som vi föreslagit inte följs av de brottsbekämpande myndigheterna. Det bör därför kunna förekomma att tillsynsmyndigheten utövar sin tillsyn redan under pågående verkställighet för att bilda sig en uppfattning av om de brottsbekämpande myndigheterna följer de lagstadgade reglerna om vad som ska vidtas i genomförandefasen, se avsnitt 10.10. Vid utredningens studiebesök i utlandet har det visat sig att det inte är ovanligt att tillsynsfunktioner ibland helt övervakar verkställighet eller i vart fall gör enskilda nedslag under pågående verkställighet. Så bör alltså enligt vår mening även kunna förekomma i Sverige.

För att ge nämnden en fingervisning om när det kan vara aktuellt att påbörja ett tillsynsärende bör en regel införas som ålägger domstolen som har meddelat ett tillståndsbeslut att underrätta tillsynsmyndigheten om beslutet. Det blir således en slags upplysning som kan initiera en tidigare tillsyn än vad som torde vara det vanliga i dag. Det står dock naturligtvis nämnden helt fritt att själv välja vilka åtgärder, om några, den ska vidta med anledning av en sådan upplysning.

10.12.2 Medverkan vid verkställighet

Utredningens förslag: 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.

Bakgrund

Från experterna vid de brottsbekämpande myndigheterna har det framhållits att en framgångsfaktor avseende effektiviteten hos hemlig dataavläsning, i meningen att åtgärden blir möjlig att genomföra, i vissa fall kommer att vara en aktiv medverkan från operatörer. Med operatörer avses här de som tillhandahåller allmänt tillgängliga elektroniska kommunikationsnät och kommunikationstjänster (se 2 kap. 1 § lagen om elektronisk kommunikation). En sådan medverkan kan handla om att operatören bistår de brottsbekämpande myndigheterna med att identifiera vilka tjänster en specifik användare har, identifiera vilka förbindelser som används, rådgivning avseende vilka tekniska hjälpmedel som kan användas, tillhandahållande av möjlighet att installera brottsbekämpande myndigheters tekniska hjälpmedel i operatörens nät för verkställighet eller hjälp med andra liknande stödåtgärder. Som ett exempel har nämnts att brottsbekämpande myndigheter, med operatörens aktiva medverkan, kan installera utrustning som aktivt påverkar trafikflödet mellan den som ska vara föremål för hemlig dataavläsning och annan utrustning som denne kommunicerar med. Det kan i praktiken exempelvis handla om förändring av trafik och kvarhållande eller borttagning av datapaket från att nå fram till denne.

Från de brottsbekämpande myndigheternas håll har det också framhållits att en operatörs aktiva medverkan i vissa fall kommer att vara en förutsättning för att de tekniska hjälpmedel som ska användas kan installeras på ett så effektivt, snabbt och säkert sätt som möjligt. En aktiv medverkan från operatörer innebär enligt de brottsbekämpande myndigheterna att verkställighet kan effektueras snab-

bare då utrustning kan finnas installerad i operatörens utrymmen och endast behöva anslutas när hemlig dataavläsning ska verkställas. Åtgärden kan enligt de brottsbekämpande myndigheterna också bli mer säker när installation av tekniska hjälpmedel sker med en mer kirurgisk precision i de förbindelser och den kommunikation som tillståndet avser.

Saknas operatörens medverkan, när sådan behövs, kommer enligt de brottsbekämpande myndigheterna verkställande av hemlig dataavläsning i vissa fall inte att kunna ske eller kräva tillstånd under betydligt längre tid. Dessutom har framhållits att mer komplicerade metoder kan behöva användas, vilket kan innebära att de tekniska hjälpmedel som föranleder minst risker i verkställighetsfasen inte kan användas.

Enligt de brottsbekämpande myndigheterna är det 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 brottsbekämpande myndigheterna emellertid för närvarande inte bedömt att det är nödvändigt med en anpassningsskyldighet för operatörerna, liknande den som föreligger enligt lagen om elektronisk kommunikation (se t.ex. 6 kap. 19 § den lagen).

Det ska för fullständighetens skull också nämnas att det i diskussionerna avseende operatörers medverkan har framkommit att hemlig dataavläsning i många fall kommer att kunna verkställas helt utan att åtgärder från operatören är nödvändiga.

Mot den angivna bakgrunden har utredningen funnit skäl att överväga om det ska vara möjligt för de brottsbekämpande myndigheterna att ta hjälp av externa aktörer i samband med verkställighet av hemlig dataavläsning. Utredningen har i det arbetet, utöver diskussioner med tekniska experter vid de brottsbekämpande myndigheterna, också sammanträffat med företrädare för vissa operatörer, intresseorganisationen IT- och telekomföretagen samt Post- och telestyrelsen (PTS). I diskussioner med operatörerna har främst frågor om risker för nät- och informationssäkerheten vid en medverkan från operatörer och kostnader med anledning av medverkan aktualiserats.

En regel om medverkansmöjlighet införs

Det är givetvis av största intresse att hemlig dataavläsning blir ett så effektivt tvångsmedel som möjligt. De skäl som framhållits av de brottsbekämpande myndigheterna talar med styrka för att det i vissa fall är nödvändigt med en aktiv medverkan från operatörer när hemlig dataavläsning ska verkställas. Det saknas skäl att ifrågasätta att effektiviteten av hemlig dataavläsning kan påverkas av om operatörer inte medverkar när den brottsbekämpande myndigheten har ett behov av sådan medverkan. Att medverkan också i praktiken ska ske av en operatör på begäran av den brottsbekämpande myndigheten ligger helt i linje med det samhällsansvar som följer med den bedrivna verksamheten, jfr prop. 1995/96:180 s. 29 f. och 2010/11:46 s. 66 ff.

Mot bakgrund av de regler som vi föreslår ska gälla till skydd för den personliga integriteten och informationssäkerheten (se särskilt avsnitt 10.10.3) finns inte skäl för operatörer att vägra att medverka eller hjälpa den brottsbekämpande myndigheten. Det ansvar som vilar på den verkställande myndigheten innebär ju att det inte får uppstå risker för informationssäkerheten, i vilken innefattas även nätsäkerhet, i något annat informationssystem än det som tillståndet till hemlig dataavläsning avser.

Sammantaget finns det starka skäl för en aktiv medverkan från operatörer i samband med verkställighet av hemlig dataavläsning. Frågan är närmast om en sådan medverkan ska tvingas fram genom en skyldighet för operatörer att medverka på den verkställande myndighetens begäran, som de brottsbekämpande myndigheterna har föreslagit, eller om det ska vara en medverkan baserad på frivillighet, dock inom ramen för det samhällsansvar det innebär att bedriva sådan verksamhet.

En skyldighet att medverka skulle utgöra ett sådant ingrepp i operatörernas verksamhet som enligt 8 kap. 2 § första stycket 2 regeringsformen kräver lagstöd. Det talar enligt vår mening för att det måste finnas starka skäl att tro att operatörerna inte skulle bistå de brottsbekämpande myndigheterna med den hjälp som behövs om det inte föreligger en skyldighet för operatörer att medverka. Den uppfattning som de brottsbekämpande myndigheterna i detta sammanhang framfört är att erfarenheter visat att det, när en skyldighet inte föreligger, är svårt att få hjälp från operatörer.

När det gäller frågan om det ska införas en regel om tvång att medverka bör till en början återigen framhållas det samhällsansvar som följer med den verksamhet operatörerna bedriver. Den operatör som tar sitt samhällsansvar på allvar kommer således att bistå den brottsbekämpande myndigheten som begär operatörens medverkan, oavsett om det föreligger en skyldighet att göra så eller inte. I den mån ekonomiska skäl ligger bakom en operatörs överväganden att inte medverka torde en lösning som innebär att operatörens kostnader för det bistånd man lämnar ska ersättas avhjälpa en bristande vilja att bistå, se vidare om ersättning nedan.

I den diskussion som uppstått efter EU-domstolens dom i fråga om den svenska lagringsskyldigheten i slutet av 2016 har det ibland framstått som att det alltid är operatörerna på den ena sidan och de brottsbekämpande myndigheterna på den andra sidan och att de två sidorna har helt olika intressen för ögonen. I somliga fall kanske det förhåller sig på det sättet men underhandsinformation som utredningen fått ger samtidigt vid handen att det finns upparbetade och goda relationer mellan brottsbekämpande myndigheter och flera operatörer samt att de senare inte sällan är behjälpliga när det är fråga om allvarlig brottslighet som ska utredas eller förhindras, vilket alltid kommer att vara fallet vid hemlig dataavläsning.

Det är svårt att med säkerhet veta om det är tillräckligt med en lösning som bygger på frihet under ansvar för operatörerna, dvs. att de inom ramen för det samhällsansvar som följer med den bedrivna verksamheten ges möjlighet att på frivillig grund bistå de brottsbekämpande myndigheterna när dessa behöver hjälp i verkställighetsfasen. Med hänsyn till det ingrepp det skulle innebära för operatörens verksamhet med en sådan skyldighet som diskuterats bör dock rimligen den osäkerhet som råder falla ut så att ingen skyldighet införs. Visar det sig när lagen om hemlig dataavläsning har införts att operatörerna inte bistår i den utsträckning som de borde göra eller att effektiviteten av hemlig dataavläsning av annan anledning minskar på grund av avsaknad av en medverkansskyldighet bör en sådan skyldighet införas i lagen. Vid den utvärdering som vi föreslår ska göras, se avsnitt 10.1.2, bör frågan om hur operatörernas medverkan har fungerat särskilt uppmärksammas. Med viss tvekan föreslår vi alltså inte någon lagfäst skyldighet för operatörerna att medverka.

En möjlighet för operatörer att bistå vid verkställighet finns rimligen alldeles oavsett stöd i lag eller inte. Eftersom det emellertid i fråga om sådana nät och tjänster som operatörerna tillhandahåller finns särskilda regler om nät- och informationssäkerhet och skydd för de uppgifter som behandlas (se t.ex. 6 kap. lagen om elektronisk kommunikation) bör det i lagen om hemlig dataavläsning tas in en bestämmelse om operatörers medverkan. Den kan lämpligen uttryckas som att 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. En fråga om medverkan vid verkställighet väcks rimligen av den verkställande myndigheten när denne konstaterat att operatörens medverkan i något avseende behövs för att kunna verkställa åtgärden.

Till regeln om medverkansmöjlighet bör kopplas dels bestämmelser om rätt till ersättning för den som bistår den verkställande myndigheten i samband med verkställighet, dels bestämmelser om tystnadsplikt. Den senare av dessa frågor diskuteras i nästa avsnitt.

När det gäller frågan om ersättning bör gälla att den verkställande myndigheten ska betala ersättning till operatören för de faktiska kostnader som uppstår vid medverkan. Typiskt sett torde sådana kostnader avse ianspråktagande av tid för operatörens anställda men även andra faktiska kostnader som uppstår för operatören bör ersättas.

Ersättningsfrågan bör kunna lösas av den brottsbekämpande myndigheten och den operatör som medverkar. Därför föreslår vi inte någon reglering avseende t.ex. nivåer för ersättningen. Visar det sig att denna ordning inte fungerar bör ersättningsfrågan, liksom frågan om skyldighet att medverka, bli föremål för en särskild utredning.

Regeln om medverkan och ersättning för medverkan bör införas i lagen om hemlig dataavläsning i anslutning till reglerna om genomförande av åtgärden.

10.12.3 Sekretess-, tystnadsplikts-, och partsinsynsfrågor

Utredningens förslag: 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. I tredje stycket föreslås också en ändring så att hemlig rumsavlyssning läggs till i katalogen över tvångsmedel.

En särskild sekretessregel införs för 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. Tystnadsplikten enligt den bestämmelsen ska ha företräde framför rätten att meddela och offentliggöra uppgifter. För att så ska bli fallet införs ett tillägg om detta i 44 kap. 5 § offentlighets- och sekretesslagen.

I offentlighets- och sekretessförordningen bör tillägg göras för att hemlig dataavläsning ska följa samma struktur som övriga hemliga tvångsmedel.

Utredningens bedömning: Nuvarande sekretessregler till skydd för både intresset av att förebygga eller beivra brott och enskildas personliga och ekonomiska förhållanden ger adekvat skydd för de uppgifter om hemlig dataavläsning som kan behöva hemlighållas. Någon ändring av dessa behöver således inte göras. Inte heller behövs någon ändring av reglerna om kollision mellan rätten till partsinsyn och sekretessbestämmelserna.

Regler om sekretess och rätten att meddela och offentliggöra uppgifter när det gäller hemliga tvångsmedel

Enligt 18 kap. 1 § offentlighets- och sekretesslagen gäller sekretess 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. Sekretess gäller också enligt bestämmelsen bl.a. för uppgift som hänför sig till annan verksamhet än sådan som syftar till att förebygga, uppdaga, utreda eller beivra brott och som bedrivs av en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen.

Frågor om sekretess i de brottsbekämpande myndigheternas underrättelseverksamhet regleras i stället i 18 kap. 2 § offentlighets- och sekretesslagen. Enligt den bestämmelsen gäller sekretess bl.a. för uppgift som hänför sig till sådan verksamhet, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Enligt 18 kap. 3 § offentlighets- och sekretesslagen gäller sekretessen enligt nu nämnda bestämmelser i annan verksamhet än som där avses hos en myndighet för att biträda en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott.

Bestämmelserna är generella och tar inte särskilt sikte på användningen av hemliga tvångsmedel, även om sådan användning givetvis innefattas. Det finns också regler i 18 kap. 17 § offentlighets- och sekretesslagen som talar om vad som ska gälla beträffande sekretess för uppgift i verksamhet som avser rättsligt samarbete på begäran av en annan stat eller en mellanfolklig domstol, för uppgift som hänför sig till en utredning enligt bestämmelserna om förundersökning i brottmål eller en angelägenhet som angår tvångsmedel. I dessa fall ska sekretess gälla om det kan antas att det varit en förutsättning för den andra statens eller den mellanfolkliga domstolens begäran att uppgiften inte skulle röjas.

I 18 kap. 19 § offentlighets- och sekretesslagen anges att tystnadsplikten som följer av 18 kap. 1–3 §§ och 17 § inskränker rätten att meddela och offentliggöra uppgifter, bl.a. när det är fråga om uppgifter som gäller användning av hemliga tvångsmedel. I bestämmelsen anges de hemliga tvångsmedel, för vilket detta gäller, uttryckligen. Att tystnadsplikten har getts företräde framför rätten att meddela och offentliggöra uppgifter har motiverats bl.a. av att syftet med åtgärderna skulle kunna omintetgöras om uppgifterna kommer ut och den utgör således ett undantag till den generella huvudregeln om

att rätten att meddela och offentliggöra uppgifter har företräde framför tystnadsplikten.[56]

Den sekretess som regleras i 18 kap. offentlighets- och sekretesslagen gäller enligt kapitelrubriken till skydd främst för intresset av att förebygga eller beivra brott. Det finns också sekretessregler till skydd för enskild i verksamhet som syftar till att förebygga eller beivra brott i lagens 35 kap. Enligt 35 kap. 1 § gäller sekretess 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. Till skillnad från vad som gäller enligt 18 kap. offentlighets- och sekretesslagen har rätten att meddela och offentliggöra uppgifter företräde framför tystnadsplikten enligt 35 kap. 1 §.

Regler om partsinsyn

En särskild fråga av betydelse är den om misstänktas rätt till insyn i den utredning som bedrivs mot dem och kollisionen som kan uppstå med de ovan nämnda sekretessbestämmelserna. Den som är misstänkt för brott har rätt att ta del av vad som förekommit vid förundersökningen – den s.k. insynsrätten. 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 göra sina synpunkter gällande och påverka utredningen. Den misstänktes rätt till insyn inträder i och med att hen i samband med förhör underrättas enligt 23 kap. 18 § första stycket rättegångsbalken om skälig misstanke om brott. Före det förhöret finns ingen rätt till insyn enligt rättegångsbalkens regler. Enligt samma paragrafs andra stycke gäller insynsrätten med de begränsningar som följer av 10 kap. 3 § offentlighets- och sekretesslagen.

[56] Se t.ex. prop. 2005/06:178 s. 81.

Sedan slutdelgivning skett, dvs. när undersökningsledaren har slutfört den utredning som hen anser är nödvändig och underrättat den misstänkte och försvararen om detta, har den misstänkte och försvararen rätt att ta del av det som har förekommit vid förundersökningen. Detta följer av 23 kap. 18 a § rättegångsbalken och gäller även efter det att åtalet har väckts och fram till dess att åtalet slutligt har prövats eller saken annars slutligt har avgjorts. Rätten begränsas dock enligt samma bestämmelse av vad som följer av 10 kap. 3 och 3 a §§ offentlighets- och sekretesslagen.

I 10 kap. 3 § offentlighets- och sekretesslagen anges att sekretess inte hindrar att en enskild eller en myndighet som är part i ett mål eller ärende hos domstol eller annan myndighet och som på grund av sin partsställning har rätt till insyn i handläggningen, tar del av en handling eller annat material i målet eller ärendet. En sådan handling eller ett sådant material får dock inte 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. I sådana fall ska myndigheten på 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.

Bestämmelsen i 10 kap. 3 § offentlighets- och sekretesslagen kompletteras av 3 a § i samma kapitel. Där anges att när en misstänkt och försvararen enligt 23 kap. 18 a § första stycket rättegångsbalken har underrättats om rätten att ta del av det som har förekommit vid en förundersökning, gäller begränsningarna enligt 3 § första stycket i fråga om rätten att ta del av en handling eller något annat material endast om det är fråga om en uppgift som inte har betydelse för beslutet i åtalsfrågan, och det står klart att det intresse som sekretessen ska skydda har företräde framför den misstänktes intresse av att ta del av uppgiften.[57]

[57] Insynsreglerna i rättegångsbalken och kollisionsreglerna i offentlighets- och sekretesslagen sågs över och förtydligades nyligen (se prop. 2016/17:68).

Krävs några förändringar i sekretessregleringen till följd av förslaget om hemlig dataavläsning?

Situationer där vi bedömer att inga förändringar behövs

Som framhållits ovan är 18 kap. 1–3 och 17 §§ och 35 kap. 1 § offentlighets- och sekretesslagen generellt formulerade. De täcker således upp samtliga hemliga tvångsmedel. De kommer alltså gälla även för hemlig dataavläsning enligt vårt förslag. Det är därför inte nödvändigt med några förändringar i denna del.

Också bestämmelserna i 10 kap. 3 och 3 a §§ offentlighets- och sekretesslagen, som reglerar vad som ska gälla vid kollision mellan den misstänktes insynsrätt och sekretess, är generellt utformade. Även dessa kommer således enligt sin nuvarande lydelse att gälla när hemlig dataavläsning används. Inte heller här föreslår vi därför några förändringar.

Tystnadsplikten och rätten att meddela och offentliggöra uppgifter – svenska förhållanden

En fråga som däremot behöver övervägas är om tystnadsplikten bör ha företräde framför rätten att meddela och offentliggöra uppgifter som hänför sig till användning av det nya tvångsmedlet. Som redovisats ovan gäller enligt 18 kap. 19 § andra stycket offentlighets- och sekretesslagen tystnadsplikten framför rätten att meddela och offentliggöra uppgifter för uppgifter om hemliga tvångsmedel. I bestämmelsen anges vart och ett av de nuvarande tvångsmedlen uttryckligen, varför hemlig dataavläsning inte finns med i förteckningen. Utan ändringar i 18 kap. 19 § andra stycket offentlighets- och sekretesslagen kommer därför rätten att meddela och offentliggöra uppgifter ha företräde framför tystnadsplikten för uppgifter om hemlig dataavläsning.

De skäl som har gjorts gällande tidigare när tystnadsplikt för uppgifter om hemliga tvångsmedel har fått försteg framför rätten att meddela och offentliggöra uppgifter, särskilt att syftet med åtgärderna skulle kunna omintetgöras om uppgifterna kommer ut, har skäl för sig även beträffande hemlig dataavläsning. Eftersom beslut att tillåta hemlig dataavläsning enligt vårt förslag alltid kommer att fattas av domstol, framstår det kontrollbehov som rätten att meddela

och offentliggöra uppgifter kan tillgodose för utomstående också som relativt sett mindre. För uppgifter från hemlig dataavläsning bör därför, liksom för uppgifter från övriga hemliga tvångsmedel, tystnadsplikten ges företräde framför rätten att meddela och offentliggöra uppgifter genom att tillägg om detta görs i 18 kap. 19 § andra stycket offentlighets- och sekretesslagen.

Tystnadsplikten och rätten att meddela och offentliggöra uppgifter – internationell rättslig hjälp

Eftersom vi i kapitel 11 föreslår att hemlig dataavläsning ska tas upp i katalogen av tvångsmedel som kan användas enligt lagen om internationell rättslig hjälp i brottmål och i den föreslagna lagen om europeisk utredningsorder finns skäl att göra en ändring i 18 kap. 19 § tredje stycket offentlighets- och sekretesslagen. Detta för att hemlig dataavläsning även i de fall åtgärden används med grund i det internationella rättsliga samarbetet ska följa strukturen för övriga hemliga tvångsmedel. I bestämmelsen regleras i vilka fall rätten att meddela och offentliggöra uppgifter får ge vika för tystnadsplikten när det gäller uppgifter hänförliga till det internationella rättsliga samarbetet.

När det gäller just den bestämmelsen har utredningen noterat att samtliga hemliga tvångsmedel inte regleras likadant. Hemlig rumsavlyssning regleras nämligen annorlunda än övriga hemliga tvångsmedel. Till skillnad från vad som gäller enligt 18 kap. 19 § andra stycket offentlighets- och sekretesslagen tas inte i tredje stycket uppgift om hemlig rumsavlyssning upp. Det innebär att rätten att meddela och offentliggöra uppgifter enligt bestämmelsens nuvarande ordalydelse har företräde framför tystnadsplikten när det är fråga om uppgifter om hemlig rumsavlyssning men inte när det gäller övriga hemliga tvångsmedel. Dock gäller ändå i vissa fall att rätten att meddela och offentliggöra uppgifter inskränks av andra regler, jfr 18 kap. 19 § fjärde stycket offentlighets- och sekretesslagen och hänvisningarna däri till tryckfrihetsförordningen och yttrandefrihetsgrundlagen.

Nämnda skillnad framstår som svårförklarlig, i synnerhet eftersom tystnadsplikten för uppgifter om hemlig rumsavlyssning har företräde framför rätten att meddela och offentliggöra uppgifter enligt 18 kap. 19 § andra stycket offentlighets- och sekretesslagen.

Anledningen till skillnaden har inte motiverats i förarbetena vid införandet av hemlig rumsavlyssning (se prop. 2005/06:178 avsnitt 9.12 jämfört med kapitel 11) och inte heller vid senare ändringar av bestämmelsen i 18 kap. 19 § (se prop. 2008/09:150 och prop. 2011/12:55). Med anledning av att utredningen noterat den beskrivna diskrepansen har kontakt tagits med Justitiedepartementet utan att några klargörande anledningar till den har kommit fram. Något sakligt skäl för att reglera hemlig rumsavlyssning annorlunda än övriga hemliga tvångsmedel vid det internationella rättsliga samarbetet såvitt avser avvägningen mellan tystnadsplikten och rätten att meddela och offentliggöra uppgifter synes inte heller finnas. Vår bedömning är därför att skillnaden i reglering är följden av ett förbiseende i samband med införandet av reglerna om hemlig rumsavlyssning.

De skäl som vi redovisat ovan beträffande att låta tystnadsplikten för uppgifter om hemlig dataavläsning ha företräde framför rätten att meddela och offentliggöra uppgifter vid svenska förundersökningar och underrättelseärenden gör sig gällande även när det är fråga om internationella förhållanden. Därför bör hemlig dataavläsning regleras på motsvarande vis i dessa fall, dvs. tystnadsplikten bör alltid ha företräde framför rätten att meddela och offentliggöra uppgifter om hemlig dataavläsning. Mot bakgrund av den bedömning vi nyss redovisat om hemlig rumsavlyssning finns skäl att också föreslå en justering av den nuvarande regleringen så att tystnadsplikten även för uppgifter om hemlig rumsavlyssning har företräde framför rätten att meddela och offentliggöra uppgifter. Vi gör bedömningen att ett sådant förslag ryms inom våra direktiv.

En särskild sekretessregel införs i lagen om hemlig dataavläsning

Vi har föreslagit att en regel införs om att operatörer får medverka i samband med verkställighet av hemlig dataavläsning. Operatörerna omfattas inte av regleringarna i 18 kap. 1–3 eller 17 § offentlighets- och sekretesslagen. När det gäller hemlig alvyssning och övervakning av elektronisk kommunikation finns särskilda bestämmelser i 6 kap. 21 § lagen om elektronisk kommunikation som ålägger privaträttsliga subjekt som, i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, har fått del av uppgifter som hänför sig till åtgärderna tystnadsplikt. En

liknande bestämmelse bör införas i lagen om hemlig dataavläsning. Den bör ta sikte på alla situationer då personer verksamma vid de företag som kan medverka i samband med verkställighet av hemlig dataavläsning får kännedom om uppgifter som hänför sig till åtgärden.

Bestämmelsen kan lämpligen utformas med ledning av hur 6 kap. 21 § lagen om elektronisk kommunikation har utformats. En koppling bör först göras till vem som träffas av bestämmelsen. I lagen om elektronisk kommunikation uttrycks detta med *den som*, vilket framstår som ändamålsenligt även här. Vi föreslår därför att en bestämmelse om tystnadsplikt bör omfatta 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. För att bestämmelsen ska motsvara den sekretess som gäller enligt 18 kap. 1–3 och 17 §§ offentlighets- och sekretesslagen bör det vara uppgifter som hänför sig till *användningen av* hemlig dataavläsning som tystnadsplikten ska omfatta. När det gäller vad tystnadsplikten ska innebära framstår uttryckssättet enligt 6 kap. 21 § lagen om elektronisk kommunikation (genom hänvisningen till 20 § samma lag och kapitel) som lämplig. Där anges att den som tystnadsplikten gäller inte obehörigen får föra vidare eller utnyttja det han fått del av eller tillgång till. Motsvarande uttryckssätt bör användas i den bestämmelse vi föreslår i lagen om hemlig dataavläsning. I 20 kap. brottsbalken finns bestämmelser om straff för den som bryter mot tystnadsplikten. I 7 kap. 15 § tredje stycket lagen om elektronisk kommunikation erinras om dessa straffbestämmelser för den som bryter mot tystnadsplikten. Motsvarande påminnelse bör enligt vår bedömning göras även i lagen om hemlig dataavläsning.

Tystnadsplikten och rätten att meddela och offentliggöra uppgifter – den nya sekretessregeln i lagen om hemlig dataavläsning

Vi har föreslagit att rätten att meddela och offentliggöra uppgifter ska ge vika för tystnadsplikten när det gäller uppgifter om hemlig dataavläsning. Detta bör gälla även när operatörer medverkar i samband med verkställighet. Därför bör en motsvarande bestämmelse för dessa subjekt föras in i offentlighets- och sekretesslagen. I 44 kap. den lagen finns bestämmelser om andra situationer då tystnadsplikten

har företräde framför rätten att meddela och offentliggöra uppgifter. Bland annat regleras där (4 § 3) att tystnadsplikten för användningen av hemliga tvångsmedel som följer av 6 kap. 21 § lagen om elektronisk kommunikation inskränker rätten att meddela och offentliggöra uppgifter. Den bestämmelsen tar dock endast sikte på just lagen om elektronisk kommunikation. I 44 kap. 5 § offentlighets- och sekretesslagen finns emellertid en uppsamlande bestämmelse för vissa andra lagar (under rubriken Annan lagstiftning). Lämpligen kan därför en bestämmelse som inskränker rätten att meddela och offentliggöra uppgifter för de uppgifter som omfattas av tystnadsplikten enligt vårt förslag ovan föras in som en sista punkt i 44 kap. 5 § offentlighets- och sekretesslagen.

Ändring i sekretessförordningen

Avslutningsvis bör också, av praktiska skäl, en ändring göras i 3 § offentlighets- och sekretessförordningen så att hemlig dataavläsning, liksom övriga hemliga tvångsmedel, tas upp i de förteckningar som anger för vilka register allmänna domstolar, Polismyndigheten, Säkerhetspolisen, Tullverket och åklagarmyndigheter inte ska tillämpa 5 kap. 2 § andra stycket offentlighets- och sekretesslagen.

10.12.4 Kvalifikationskrav på den som ansvarar för verkställighet

Utredningens förslag: Myndighetschefen vid den verkställande myndigheten 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.

Vi har föreslagit att det ska vara en särskild person som ansvarar för verkställighet av hemlig dataavläsning, se avsnitt 10.10.3. Verkställighet av hemlig dataavläsning är av en teknisk särart jämfört med verkställighet av övriga hemliga tvångsmedel. Dessutom kan risker för den personliga integriteten och informationssäkerheten uppstå

om åtgärden verkställs på sätt som inte står i överensstämmelse med våra förslag. Därför bör särskilda kvalifikationskrav uppställas i lag för den som ska ansvara för verkställighet.

För att understryka vikten av beslutet att utse personer som får ansvara för verkställighet bör beslutanderätten ligga på myndighetschefen. Denne bör dock få delegera beslutanderätten.

Vad sedan avser själva kvalifikationskraven på den som ska utses bör för det första krävas särskilda kunskaper om informationssäkerhet. Kravet på sådana kunskaper hänger samman med det vi nämnt tidigare om risker för informationssäkerheten och åtgärdens tekniska natur samt de anpassningar som den verkställande myndigheten ska vidta beträffande verkställighetstekniken, se avsnitt 10.10.2. Ett krav på särskilda kunskaper om informationssäkerhet för den som ansvarar för verkställighet kan således minska riskerna vid verkställighet. Även i övriga avseenden, t.ex. beträffande utbildning, erfarenhet och allmän lämplighet, måste det ställas höga krav på den som ska ansvara för verkställighet.

10.12.5 Ändringar i andra författningar

Utredningens förslag: I 28 § lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. görs ett tillägg som innebär att när hemlig dataavläsning avser rumsavlyssningsuppgifter i sådana situationer som den lagen avser får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.

I lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. finns särskilda bestämmelser som ska gälla om Sverige är i krig. Bestämmelserna kan också bli tillämpliga om Sverige är i krigsfara eller det råder sådana utomordentliga förhållanden som är föranledda av krig eller av krigsfara som Sverige har befunnit sig i, se 2 §. Enligt lagens 28 § gäller, när lagen är tillämplig, 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 § rättegångsbalken, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut. Tidigare gällde detta även för andra hem-

liga tvångsmedel men regeln ändrades i samband med att möjligheten till interimistisk åklagarprövning infördes i rättegångsbalken 2015, se prop. 2013/14:237 s. 146 f. och 191.

De skäl som ligger bakom att det ska vara möjligt för åklagaren att fatta interimistiska beslut beträffande hemlig rumsavlyssning i sådana tider som aktualiserar tillämpning av lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. gör sig gällande även för hemlig dataavläsning avseende rumsavlyssningsuppgifter. Enligt vårt förslag till lag om hemlig dataavläsning ska det vara möjligt för åklagaren att fatta interimistiska beslut i samtliga fall åtgärden ska användas utom när den ska användas för att läsa av eller ta upp sådana uppgifter. Det är således endast beträffande det användningsområdet för åtgärden som en reglering i lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. behövs. Vi föreslår av denna anledning ett tillägg i den lagens 28 § som innebär att när det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig dataavläsning avseende rumsavlyssningsuppgifter får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.

I nästa kapitel kommer frågor om internationella förhållanden att behandlas. Där redovisas förslag till ändringar i några författningar som reglerar sådana frågor. Utöver vad som nu anförts och det vi föreslår i nästa kapitel har vi inte funnit skäl att göra några ändringar i andra författningar.

11 Jurisdiktionsfrågor och internationella förhållanden

11.1 Allmänt om exekutiv jurisdiktion

Ordet jurisdiktion används först och främst för att hänvisa till en stats maktutövning över personer och egendom inom dess eget territorium. En stats jurisdiktion kan utövas genom rätten att stifta lagar och andra regler (legislativ jurisdiktion), rätten att tillämpa lagstiftningen eller skipa rätt (judiciell jurisdiktion) och rätten att verkställa åtgärder eller förverkliga beslut som fattats inom ramen för lagstiftning och rättskipning (exekutiv jurisdiktion).

I Lotus-målet mellan Frankrike och Turkiet som avgjordes av den Fasta mellanfolkliga domstolen 1927 (Permanent Court of International Justice, PCIJ Ser. A, no. 10) fastslogs att den viktigaste inskränkningen som folkrätten ålägger en stat är att inte utöva makt inom en annan stats territorium. Samtidigt konstaterade domstolen att det inte finns något hinder för en stat att utöva jurisdiktion inom sitt eget territorium över något som har inträffat utomlands, om det inte finns ett uttryckligt folkrättsligt förbud mot det. Vad domstolen menade var att en stat har obegränsad makt att utöva lagstiftande och dömande makt (legislativ och judiciell jurisdiktion) över personer och egendom som befinner sig utomlands och över händelser som äger rum utanför statens territorium, så länge det inte finns något folkrättsligt förbud. Däremot kan verkställighet av nationella lagar och domar (den exekutiva jurisdiktionen) äga rum endast inom det egna territoriet.[1]

När det gäller exekutiv jurisdiktion är utgångspunkten i folkrätten att det råder ett förbud för stater att vidta verkställighetsåtgär-

[1] Se Mahmoudi m.fl., *Sverige och folkrätten*, 5 uppl. s. 100.

der inom andra staters territorier, t.ex. använda hemliga tvångsmedel där. Detta är ett utflöde av den s.k. territorialitetsprincipen, vilken används som grund för jurisdiktion. Tanken med territorialitetsprincipen är att ingen stat ska kränka en annan stats territoriella integritet (suveränitet). Om ett visst föremål av betydelse som bevisning i en utredning i Sverige t.ex. finns i en lokal i USA är de svenska brottsbekämpande myndigheterna därför, trots att det i Sverige finns regler om husrannsakan och beslag för brottsbekämpande myndigheter här, förhindrade att åka till lokalen och hämta föremålet. I stället är myndigheterna som utgångspunkt hänvisade till att begära hjälp av amerikanska brottsbekämpande myndigheter med hänvisning till territorialitetsprincipen.

De förutsättningar som gäller för exekutiv jurisdiktion har vuxit fram i den traditionellt fysiska världen. I den är det tämligen enkelt att klarlägga var fysiska ting finns förvarade. Åtminstone är det i teorin alltid möjligt. Därmed är det också förhållandevis enkelt att identifiera i vilken stat verkställighet ska ske och således även att veta vilken stat en begäran om rättslig hjälp ska ställas till.

I den digitala eller virtuella världen ser förhållandena annorlunda ut. 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. Trots detta tillämpar Sverige, och vissa andra länder, territorialitetsprincipen på samma sätt för elektroniskt lagrade uppgifter som för information som manifesterats på t.ex. papper. Det innebär exempelvis att det inte är tillåtet för svenska brottsbekämpande myndigheter att under en förundersökning, där man känner till den misstänktes inloggningsuppgifter, logga in på dennes internetbaserade kommunikations- eller lagringstjänster om tjänstetföretagets servrar kan finnas utanför Sverige.

Brottsbekämpande myndigheter är i stället hänvisade till att begära in uppgifterna från tjänstetillhandahållaren eller i många fall, särskilt när det är fråga om innehållsuppgifter (eng. content), begära rättslig hjälp från det land där tjänstetillhandahållaren har sitt säte eller där uppgifterna finns eller lagras. Det innebär, när det inte är fråga om innehållsuppgifter, att svenska brottsbekämpande myndigheter är utlämnade till den goda viljan hos tjänstetillhandahållaren

och vid innehållsuppgifter till att den stat som rättslig hjälp begärs från kan tillgodose begäran inom rimlig tid. Som kommer att framgå nedan finns problem med detta förfarande.

Den svenska hållningen är således att territorialitetsprincipen innebär 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. Denna tolkning av territorialitetsprincipen delas inte av alla andra länder. Mot bakgrund av den snabba utveckling som skett på främst molntjänstområdet har flera länder funnit skäl att lämna tolkningen bakom sig för att i stället låta andra territoriella anknytningsfaktorer påverka jurisdiktionsfrågan, i synnerhet när det är fråga om situationer då det inte är klarlagt var uppgifter lagras. I brottsutredningar används bl.a. den misstänktes hemvist, platsen där brottet begåtts och informationsinnehavarens (t.ex. den som förfogar över/äger/disponerar/har kontrollen över ett användarkonto) hemvist som jurisdiktionsgrundande omständigheter. Vi ska senare återkomma till olika tolkningar av territorialitetsprincipen och föra en diskussion om för- respektive nackdelar med dessa och den svenska hållningen. Dessförinnan ska vi dock utveckla hur vi, utifrån det svenska synsättet, ser på vårt förslag till hemlig dataavläsning.

11.1.1 Exekutiv jurisdiktion vid hemlig dataavläsning

När det gäller hemlig dataavläsning uppstår, såvitt vi kan bedöma, inga svårigheter med den exekutiva jurisdiktionen enligt den nuvarande svenska tolkningen av territorialitetsprincipen så länge som informationssystemet och personen som åtgärden avser finns i Sverige och de brottsbekämpande myndigheterna dels förvissar sig om att själva intrånget i informationssystemet sker på svenskt territorium, dels agerar passivt i avläsningen. Med passivt avses att det enda som sker är en observation av vad som försiggår på den utrustning åtgärden avser.

Annorlunda kan det emellertid förhålla sig om den brottsbekämpande myndigheten är aktiv i åtgärden och inte endast observerar vad som sker på utrustningen utan t.ex. öppnar eller kör program eller appar, eller på annat sätt tar del av uppgifter som lagras utanför utrustningen men som kan göras tillgängliga genom den. Med modern

teknik är det inte ovanligt att uppgifter som traditionellt har hanterats direkt i den tekniska utrustningen, t.ex. lagring av data och körning av tillämpningsprogram (exempelvis appar) i stället sköts på annat håll än i utrustningen genom s.k. molntjänster.

I vårt förslag till lag om hemlig dataavläsning möjliggörs för brottsbekämpande myndigheter att ansöka om tillstånd för hemlig dataavläsning riktad mot t.ex. ett virtuellt avgränsat användarkonto till en kommunikations- eller lagringstjänst. Även vid hemlig dataavläsning av det slaget kommer frågor om Sverige har exekutiv jurisdiktion att uppstå eftersom de uppgifter som eftersöks kan vara, och ofta är, lagrade i servrar som finns på annan plats än i Sverige.

De beskrivna svårigheterna avseende exekutiv jurisdiktion vid hemlig dataavläsning har således det gemensamt att problem som behöver adresseras kan uppstå på grund av att intressanta eller nödvändiga uppgifter lagras utanför Sverige eller att det inte är känt var de lagras. Vi har därför valt att gemensamt benämna dessa svårigheter för *lagringsfallen*. En särskild del av lagringsfallen benämner vi *loss of location.* Det begreppet har använts i internationella sammanhang sedan viss tid tillbaka för de problem som uppstår när det inte är möjligt för brottsbekämpande myndigheter att ta reda på var elektroniskt lagrade uppgifter finns.

Det finns för hemlig dataavläsning dessutom andra faktorer än de som vi tagit upp nu som kan påverka Sveriges exekutiva jurisdiktion. Liksom vid hemlig avlyssning och övervakning av elektronisk kommunikation finns det vid hemlig dataavläsning risk för att en person eller ett informationssystem som tillståndet avser flyttas utanför Sveriges gränser. Om så sker kan det innebära att Sverige inte längre har exekutiv jurisdiktion. Typfallet torde vara att en misstänkt person reser utomlands och då tar med sig den telefon eller dator som åtgärden avser. Det kan också finnas situationer där personer eller teknisk utrustning av intresse för den svenska utredningen redan innan fråga om att vidta åtgärder enligt lagen uppkommer befinner sig utanför Sverige. De situationer som nu nämnts och som påverkar Sveriges exekutiva jurisdiktion har vi valt att kalla *person- och utrustningsfallen.*

Det finns en skiljelinje mellan person- och utrustningsfallen och lagringsfallen i det att de förra redan i dag kan uppstå vid hemlig tvångsmedelsanvändning och därför, om än inte specifikt för hemlig dataavläsning, är reglerade i både inhemsk lag och i olika inter-

nationella överenskommelser. Det framstår därför som mest ändamålsenligt att utgå från befintlig reglering när de svårigheter som uppstår vid person- och utrustningsfallen ska adresseras beträffande hemlig dataavläsning.

När det däremot gäller lagringsfallen saknas i praktiken motsvarande lagstiftning och överenskommelser. Svårigheterna som ryms i begreppet har i stället uppstått som en direkt följd av tolkningen av territorialitetsprincipen i förening med den tekniska utvecklingen. De lösningar som finns för lagringsfallen är inte heller sådana att de utan vidare passar in i de gällande nationella regelverken om internationellt samarbete eftersom reglerna, såvitt avser hemliga tvångsmedel, närmast uteslutande tar sikte på var en person eller viss fysisk utrustning finns, men inte var uppgifter lagras.

Mot den bakgrund som nu anförts behandlas i det följande först i avsnitt 11.2 person- och utrustningsfallen, varefter lagringsfallen behandlas i avsnitt 11.3.

11.2 Exekutiv jurisdiktion vid hemlig dataavläsning; person- och utrustningsfallen

11.2.1 Bakgrund

De svårigheter som adresseras här tar sikte på frågor som behöver besvaras när en enskild som är föremål för hemlig dataavläsning eller ett fysiskt avgränsat informationssystem som tillståndet avser finns utanför Sveriges gränser. I de fallen påverkas Sveriges exekutiva jurisdiktion. Självfallet påverkas på motsvarande vis andra staters exekutiva jurisdiktion när en person eller viss fysisk utrustning som den andra staten riktar åtgärder mot finns här i Sverige eller annars utanför den staten. Sådana frågor adresseras också i detta avsnitt.

Det förekommer sådana svårigheter som avses i *person- och utrustningsfallen* redan vid verkställighet av de gällande hemliga tvångsmedlen. Därför finns det som nämnts redan regler i svensk rätt på området. Lagen om internationell rättslig hjälp i brottmål reglerar främst vilka åtgärder Sverige kan bistå andra stater med och vilka förutsättningar som gäller för sådan hjälp. I lagstiftningen finns dock också regler om vad som gäller för svenska domstolars och åklagares möjligheter att ansöka om rättslig hjälp utomlands.

Sverige kan som huvudregel lämna och ta emot hjälp enligt lagen även om Sverige inte har ett avtal om rättslig hjälp i brottmål med den andra staten, dvs. inget krav på reciprocitet (ömsesidighet) ställs upp. En del länder kräver dock avtal för att kunna samarbeta med Sverige. Vi har i avsnitt 3.7.1 redovisat vad som gäller för hemliga tvångsmedel enligt lagen om internationell rättslig hjälp i brottmål. För en bakgrund avseende dessa regler hänvisas dit.

I det följande ska i stället redogöras för det lagförslag avseende europeisk utredningsorder som träder i kraft den 1 december 2017, dvs. efter att detta betänkande har lämnats.[2] Även detta (föreslagna) regelkomplex är nämligen av betydelse för vårt arbete.

Förslaget till lag om europeisk utredningsorder

Lagförslaget är ett led i att genomföra Europaparlamentets och rådets direktiv om en europeisk utredningsorder[3], som bygger på ett initiativ från bl.a. Sverige. Det är fråga om en tämligen omfattande lag som involverar en hel rad olika åtgärder som är av mindre betydelse för slutsatserna i detta betänkande. Vi har därför begränsat den fortsatta framställningen i detta avsnitt till bestämmelser i lagförslaget av särskild betydelse för de frågor som vi ska behandla i avsnitt 11.2.2 och 11.2.4; nämligen om det finns skäl att låta hemlig dataavläsning ingå bland de hemliga tvångsmedel som räknas upp i den föreslagna lagen och i så fall hur sådan reglering bör utformas. För en mer fullständig genomgång av lagförslaget hänvisas till prop. 2016/17:218, se särskilt dess kapitel 6–9 och avsnitt 13.1. I propositionen finns också det bakomliggande EU-direktivet som bilaga.

När hänvisningar i det följande görs till enskilda paragrafer avses, om annat inte anges särskilt, reglerna i den föreslagna lagen.

[2] Lagförslaget, som behandlas i prop. 2016/17:218 har mot bakgrund av att det inte trätt i kraft vid betänkandets lämnande inte tagits upp i kapitel 3, som ju behandlar gällande rätt.
[3] Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området.

Allmänna bestämmelser

Enligt 1 kap. 3 § avses med en europeisk utredningsorder antingen

1. ett beslut i Sverige som innebär att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning och som har meddelats av en åklagare eller domstol under en förundersökning eller rättegång i brottmål, eller
2. ett rättsligt avgörande i en annan medlemsstat som innebär att en utredningsåtgärd ska vidtas i Sverige i syfte att inhämta bevisning och som har utfärdats eller godkänts av en domare, domstol, undersökningsdomare eller allmän åklagare i ett straffrättsligt förfarande eller i ett annat förfarande avseende straffbara gärningar som inleds vid en administrativ eller rättslig myndighet, när ett beslut i ett sådant annat förfarande kan leda till ett förfarande inför en domstol som är behörig att handlägga brottmål.

I 1 kap. 4 § anges vad en utredningsåtgärd enligt lagen ska avse eller motsvara. Där framgår att bl.a. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning är utredningsåtgärder som avses i lagen.

Utredningsorder som utfärdas i Sverige

En europeisk utredningsorder får enligt 2 kap. 1 och 3–4 §§ utfärdas i Sverige av åklagare om de förutsättningar som gäller för att vidta utredningsåtgärden under en svensk förundersökning är uppfyllda och åtgärden är proportionerlig. Dessutom krävs, när det är fråga om hemliga tvångsmedel, enligt 2 kap. 5 § att domstol har lämnat tillstånd att utfärda ordern. I avvaktan på domstolens beslut får åklagaren fatta interimistiskt beslut under de förutsättningar som gäller enligt 27 kap. 21 a § rättegångsbalken för hemlig avlyssning eller övervakning av elektronisk kommunikation eller hemlig kameraövervakning. Åklagaren ska utan dröjsmål anmäla detta till domstolen. För domstolens handläggning gäller vad som är föreskrivet i rättegångsbalken eller annan författning för den åtgärd som avses. Det föreskrivs också särskilt i 2 kap. 17–19 §§ lagförslaget vilka

regler i 27 kap. rättegångsbalken som ska tillämpas när utredningsordern avser hemliga tvångsmedel.

I 2 kap. 6 § anges att det i utredningsordern ska anges om några särskilda formkrav eller förfaranden ska iakttas av den behöriga myndigheten i den andra medlemsstaten vid verkställighet av utredningsordern.

Erkännande och verkställighet i Sverige av utländsk utredningsorder

När det gäller erkännande och verkställighet i Sverige av en europeisk utredningsorder gäller enligt 3 kap. 1 § att en utredningsorder som sänds över från en annan medlemsstat ska erkännas och verkställas i Sverige om vissa särskilda förutsättningar enligt lagen är uppfyllda och inte annat följer av lagen. För hemliga tvångsmedel ställs i 3 kap. 4 § som en särskild förutsättning upp att en utredningsorder får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning är uppfyllda. Bland de obligatoriska vägransgrunderna i 3 kap. 5 § nämns att utredningsordern skulle medföra fara för Sveriges säkerhet. Även att utredningsåtgärden inte motsvarar en åtgärd som anges i 1 kap. 4 § utgör en obligatorisk vägransgrund, dock inte om en annan utredningsåtgärd kan vidtas som ger motsvarande resultat som den åtgärd som utredningsordern avser.

Beträffande handläggningen av ett ärende om erkännande och verkställighet av en utredningsorder gäller bl.a. enligt 3 kap. 9 § att om utredningsordern avser en utredningsåtgärd som i en svensk förundersökning endast kan vidtas efter tillstånd från domstol, ska åklagaren, om han eller hon vid sin prövning inte vägrar att erkänna och verkställa utredningsordern, överlämna ärendet till domstol för prövning av om utredningsordern ska erkännas och verkställas. Åklagaren får dock enligt 3 kap. 10 §, i avvaktan på domstolens beslut, enligt de förutsättningar som anges i 27 kap. 21 a § rättegångsbalken, besluta att erkänna och verkställa en utredningsorder för hemlig avlyssning eller övervakning av elektronisk kommunikation eller hemlig kameraövervakning.

Om utredningsordern kan erkännas och verkställas i Sverige, ska enligt 3 kap. 19 § lagförslaget beslut meddelas om att verkställighet

ska äga rum, en s.k. verkställbarhetsförklaring. Vad sedan avser själva verkställigheten av utredningsordern är bestämmelserna i 3 kap. 34–37 §§ av särskild betydelse när åtgärden som ska genomföras är ett hemligt tvångsmedel. 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 uppteckning i Sverige av meddelanden eller uppgifter om meddelanden. Dessa överlämnas sedan enligt vad som föreskrivs i särskilda bestämmelser (3 kap. 38 och 39 §§)

När omedelbar överföring används får upptagning eller uppteckning inte göras i Sverige och bestämmelserna i rättegångsbalken om underrättelse till enskild ska inte heller tillämpas. När däremot upptagning eller uppteckning enligt beslut ska ske i Sverige gäller ett undantag avseende granskningsskyldigheten i 27 kap. 24 § rättegångsbalken som innebär att upptagningarna eller uppteckningarna inte behöver granskas i Sverige. Upptagningar och uppteckningar som finns kvar i Sverige efter det att ärendet har avslutats hos åklagaren och bevismaterialet har överlämnats till den andra staten, får bevaras endast om detta är tillåtet enligt 27 kap. 24 § rättegångsbalken. Särskilda bestämmelser för underrättelse till enskild, med utgångspunkt i rättegångsbalkens bestämmelser, gäller enligt 3 kap. 36 § när upptagning eller uppteckning enligt beslut ska ske i Sverige. Vid verkställighet av en utredningsorder för hemlig kameraövervakning och hemlig rumsavlyssning ska de nyss nämnda reglerna om hemlig avlyssning eller övervakning av elektronisk kommunikation när upptagningar eller uppteckningar sker i Sverige gälla.

Särskilt om underrättelse till annan medlemsstat

Det finns också särskilda regler i lagförslaget (4 kap. 12–15 §§) 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. Typfallet torde vara när den som är föremål för åtgärd rör sig över gränsen och då använder samma mobiltelefon under sin resa. I sådana fall finns enligt lagför-

slaget möjlighet för det land i vars territorium åtgärden ska utföras att motsätta sig att så sker.

11.2.2 Behövs regler om hemlig dataavläsning i lagen om internationell rättslig hjälp i brottmål och i den föreslagna lagen om europeisk utredningsorder?

Utredningens bedömning: Regler bör införas om hemlig dataavläsning både i lagen om internationell rättslig hjälp i brottmål och i den föreslagna lagen om europeisk utredningsorder.

Vårt förslag till lag om hemlig dataavläsning innebär att ett nytt hemligt tvångsmedel införs. Eftersom det är ett nytt tvångsmedel saknas uttryckliga regler om det både i lagen om internationell rättslig hjälp i brottmål och i den föreslagna lagen om europeisk utredningsorder.

Den brottslighet som enligt vårt förslag ska omfattas av reglerna om hemlig dataavläsning är inte sällan av gränsöverskridande natur. Det kan därför på goda grunder antas att utredningar om sådana brott kommer att bli föremål för internationellt rättsligt samarbete. Det kan gälla t.ex. grov narkotikabrottslighet, människohandel, grova övergrepp mot barn och terroristbrottslighet. Det är självfallet viktigt att Sverige – utöver att införa möjligheter att använda sig av hemlig dataavläsning på nationell nivå – även medverkar i det internationella samarbetet för att bekämpa brott av detta slag, oavsett om det är fråga om brottslighet i Sverige eller utomlands. Det bör inte vara lättare att planera, förbereda eller medverka i allvarlig brottslighet här i landet än i andra länder i vårt närområde. Redan det nu anförda talar för ett behov av särskilda regler beträffande hemlig dataavläsning i de lagar som reglerar det internationella samarbetet.

Till det angivna kommer att även om det saknas internationella överenskommelser som särskilt reglerar vad som ska gälla samarbete beträffande hemlig dataavläsning, eller dess motsvarighet i andra länder, ger direktivet som ligger till grund för lagförslaget om europeisk utredningsorder stöd för att införa regler även om det tvångsmedel som vi utreder. Direktivet förutsätter nämligen att Sverige, när det kommer en utredningsorder från ett annat land, kan tillhandahålla samtliga åtgärder som en svensk åklagare eller domstol

kan använda sig av, se t.ex. skäl 8 och artikel 3. Detta var ett av skälen till att regeringen inte ansåg att det fanns några skäl till att låta vissa åtgärder uteslutas från lagens tillämpningsområde.[4] Det finns således mycket starka skäl att låta hemlig dataavläsning ingå bland de åtgärder som en europeisk utredningsorder kan omfatta och att föreslå andra nödvändiga lagändringar i det lagförslaget.

Enligt1 kap. 2 § lagförslaget om europeisk utredningsorder ska den lagen inte gälla i förhållande till Danmark och Irland. Dessutom ska den inte gälla i förhållande till annan EU-medlemsstat som inte genomfört direktivet och icke EU-medlemsstater, däribland Norge. I dessa fall ska lagen om internationell rättslig hjälp i brottmål även fortsättningsvis tillämpas.[5] Detta talar för att också införa regler om hemlig dataavläsning i lagen om internationell rättslig hjälp i brottmål.

Vår sammantagna bedömning är således att det bör införas regler om hemlig dataavläsning i både lagen om internationell rättslig hjälp i brottmål och i den föreslagna lagen om europeisk utredningsorder.

11.2.3 Lagen om internationell rättslig hjälp i brottmål

Hemlig dataavläsning blir en åtgärd som rättslig hjälp enligt lagen omfattar

Utredningens förslag: Hemlig dataavläsning tas upp som en åtgärd som rättslig hjälp omfattar i lagen om internationell rättslig hjälp i brottmål. Nödvändiga redaktionella följdändringar på grund av detta genomförs.

I förteckningen avseende vilka åtgärder som rättslig hjälp enligt lagen om internationell rättslig hjälp i brottmål omfattar anges inte hemlig dataavläsning. För att tydliggöra att hemlig dataavläsning ska omfattas behöver åtgärden föras in i förteckningen i 1 kap. 2 § första stycket.[6] Av tydlighetsskäl bör åtgärden placeras i en egen punkt,

[4] Se prop. 2016/17:218 s. 86.
[5] Enligt en föreslagen regel i 1 kap. 9 § lagen om internationell rättslig hjälp i brottmål ska den lagen inte gälla när lagen om europeisk utredningsorder är tillämplig.
[6] Lagrumshänvisningar i avsnittet som inte anger den lag det hänvisas till avser lagen om internationell rättslig hjälp i brottmål.

lämpligen i anslutning till de andra hemliga tvångsmedlen som anges i förteckningen. Vårt förslag blir därför att placera hemlig dataavläsning i punkt 11 i förteckningen i 1 kap. 2 § första stycket lagen om internationell rättslig hjälp i brottmål. Förslaget leder till redaktionella följdändringar i 2 kap. 1 och 2 §§ som hänvisar till 1 kap. 2 §.

Hemlig dataavläsning avseende någon i Sverige

Utredningens förslag: Nya bestämmelser införs för rättslig hjälp med hemlig dataavläsning avseende någon i Sverige.

Ansökan handläggs av åklagare. Åklagaren prövar om det finns förutsättningar för åtgärden och ansöker i så fall genast om rättens tillstånd. Åklagaren får själv pröva ansökan om det är tillåtet enligt lagen om hemlig dataavläsning. Om åklagaren fattat beslut får återredovisning ske först när rätten fattat beslut.

Upptagningar och uppteckningar behöver inte granskas. De får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning skett endast om detta är tillåtet enligt vad som föreskrivs i lagen om hemlig dataavläsning.

I fråga om underrättelse till en enskild ska det gälla som gäller vid rättslig hjälp med hemlig avlyssning av elektronisk kommunikation.

När hemlig dataavläsning ska användas för att läsa av eller ta upp uppgifter som får hämtas in genom hemlig avlyssning eller övervakning av elektronisk kommunikation ska motsvarande gälla beträffande omedelbar överföring, tekniskt bistånd och gränsöverskridande åtgärder som gäller för de tvångsmedlen enligt lagen om internationell rättslig hjälp i brottmål.

Utgångspunkter

Rent generellt kan sägas att det i andra kapitlet i lagen om internationell rättslig hjälp i brottmål finns allmänna bestämmelser om rättslig hjälp i Sverige (2 kap.). Dessa regler kommer att tillämpas även för hemlig dataavläsning och innebär bl.a. att rättslig hjälp i Sverige kan lämnas under de förutsättningar som gäller för åtgärden

under en svensk förundersökning enligt reglerna i den nya lagen om hemlig dataavläsning (2 kap. 1 §).

I lagens fjärde kapitel finns särskilda bestämmelser om olika former av rättslig hjälp. De hemliga tvångsmedlen behandlas i 4 kap. 25–28 b §§. Det framstår som naturligt att införa nya bestämmelser om hemlig dataavläsning i direkt anslutning till den sista regeln som behandlar hemliga tvångsmedel. De nya bestämmelserna bör följa samma struktur som övriga tvångsmedel enligt lagen, dvs. att det först anges vad som gäller för tvångsmedlet avseende någon i Sverige och därefter vad som gäller avseende någon i utlandet.

Hur ska reglerna utformas?

Det finns skäl att i så stor utsträckning som möjligt ta ledning av de gällande bestämmelserna om rättslig hjälp i Sverige med hemliga tvångsmedel vid utformningen av reglerna om hjälp med hemlig dataavläsning. Enligt samtliga dessa gäller att ansökan om rättslig hjälp avseende någon som befinner sig i Sverige handläggs av åklagare. Det finns ingen anledning att avvika från detta vid hemlig dataavläsning. Samma skyndsamhetskrav som finns beträffande åklagarens prövning och överlämnande till rätten som gäller för de övriga tvångsmedlen bör också 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 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.

För samtliga hemliga tvångsmedel enligt lagen om internationell rättslig hjälp i brottmål 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 prop. 2004/05:144 s. 170. Samma bör gälla vid rättslig hjälp med hemlig dataavläsning. För tydlighetens skull bör det då framgå att undantaget görs från vad som föreskrivs om granskningsskyldigheten i lagen om hemlig dataavläsning. Sådan granskning som krävs för att uppfylla bestämmelsen om avlyssningsförbud påverkas dock inte av bestämmelsen och ska alltså göras.

Det bör vidare, liksom enligt 4 kap. 25 och 27 §§, framgå att om åklagaren har fattat beslut om hemlig dataavläsning så får återredovisning till det ansökande landet inte ske förrän domstol fattat beslut att tillåta åtgärden. Dessutom bör det av bestämmelsen, också det i enlighet med förlagorna, framgå att upptagningar och uppteckningar endast får bevaras när ärendet avslutats och återredovisning skett om det är tillåtet enligt de bestämmelser som reglerar detta.

När det gäller underrättelse till enskild bör samma sak gälla vid rättslig hjälp med hemlig dataavläsning som gäller vid rättslig hjälp med samtliga övriga hemliga tvångsmedel enligt lagen. Det kan enklast ske på samma vis som det är reglerat för hemlig kameraövervakning och hemlig rumsavlyssning, dvs. genom en direkt hänvisning till vad som gäller enligt 4 kap. 25 § tredje stycket. För de bakomliggande skälen till denna reglering hänvisas till prop. 2006/07:133 s. 55 ff.

För hemlig avlyssning och övervakning av elektronisk kommunikation gäller vissa särskilda regler. Dessa tar sikte på omedelbar överföring, tekniskt bistånd med omedelbar överföring och gränsöverskridande hemlig avlyssning och övervakning av elektronisk kommunikation av någon i Sverige. Reglerna grundar sig ursprungligen på 2000 års EU-konvention[7] och dess tilläggsprotokoll och innebär bl.a. att den stat där verkställighet ska ske under vissa förutsättningar kan vidta verkställighetsåtgärder själv i stället för att ta hjälp. Konventionen tar sikte på telemeddelanden och är i flera avseenden neutralt utformad såvitt avser hur dessa eller uppgifter om dessa hämtas in. Eftersom hemlig dataavläsning i vissa fall i praktiken kommer att vara ett nytt sätt att verkställa dessa åtgärder, dvs. vara ett nytt sätt att samla in motsvarande uppgifter som får hämtas in med de tvångsmedlen, bör motsvarande gälla för hemlig dataavläsning i de fallen som gäller för hemlig avlyssning och övervakning av

[7] 2000 års konvention om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater.

elektronisk kommunikation. I stället för hänvisningar till rättegångsbalken bör dock hänvisningar göras till motsvarande bestämmelser i lagen om hemlig dataavläsning.

Hemlig dataavläsning avseende någon i utlandet

Utredningens förslag: Svenska åklagare ska kunna begära rättslig hjälp med hemlig dataavläsning från en annan stat.

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 i frågan om avläsningen ska tillåtas.

Underrättelse enligt vad som föreskrivs i lagen om hemlig dataavläsning ska inte lämnas.

När hemlig dataavläsning ska användas för att läsa av eller ta upp uppgifter som får hämtas in genom hemlig avlyssning eller övervakning av elektronisk kommunikation ska motsvarande gälla beträffande tekniskt bistånd och gränsöverskridande åtgärder som gäller för de tvångsmedlen enligt lagen om internationell rättslig hjälp i brottmål.

En svensk åklagare bör också kunna begära rättslig hjälp med hemlig dataavläsning från en annan stat. Av 1 kap. 7 § framgår att en svensk åklagare utan särskilt stöd i lagen får begära rättslig hjälp utomlands i den utsträckning som den andra staten tillåter det. I enlighet med vad som gäller för nuvarande former av rättslig hjälp krävs det alltså inte någon särskild bestämmelse om rättslig hjälp med hemlig dataavläsning utomlands. Efter ansökan prövar den anmodade staten om det finns förutsättningar för åtgärden med stöd av den statens nationella rätt. Det kan förekomma att den anmodade staten för att bevilja rättslig hjälp med åtgärden ställer upp krav på att svensk domstolsprövning har skett. På motsvarande sätt som i fråga om rättslig hjälp i utlandet med övriga hemliga tvångsmedel enligt lagen (4 kap. 26, 27 och 28 §§) bör därför en svensk domstol, på åklagarens begäran, kunna pröva om hemlig dataavläsning ska äga rum utomlands. En särskild bestämmelse behövs således och den bör utformas i enlighet med bestämmelserna om hemlig kameraövervakning och rums-

avlyssning eftersom dessa har införts i lagen utan att det funnits särskilda regler i internationella överenskommelser, vilket ju också är fallet för hemlig dataavläsning.

I bestämmelsen om hemlig rumsavlyssning anges också att underrättelse till enskild inte ska lämnas. Det hänger samman med att hemlig kameraövervakning och hemlig rumsavlyssning i dessa fall genomförs enligt den andra statens lag, se prop. 2006/07:133 s. 59. Motsvarande bör enligt vår uppfattning gälla även för hemlig dataavläsning när avläsning eller upptagning inte sker i Sverige.

För hemlig avlyssning och övervakning av elektronisk kommunikation gäller särskilda bestämmelser (4 kap. 26 och 26 c §§). Liksom framhölls ovan beträffande hemlig dataavläsning avseende någon i Sverige bör, när hemlig dataavläsning ska användas för att läsa av eller ta upp kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter, motsvarande som gäller för hemlig avlyssning och övervakning av elektronisk kommunikation gälla. Bestämmelser som klargör detta bör därför införas.

11.2.4 Förslaget till lag om europeisk utredningsorder

Tillägg i befintliga bestämmelser för hemlig dataavläsning

Utredningens förslag: Hemlig dataavläsning tas upp i förteckningen som anger vad en utredningsåtgärd avser eller motsvarar. Det klargörs också genom ändringar i befintliga regler att åtgärden ingår bland de utredningsåtgärder som kräver domstolsprövning innan utfärdande av utredningsordern. Det införs vidare hänvisningar på två ställen till åklagarens möjlighet att fatta interimistiskt beslut innan domstolsprövning enligt lagen om hemlig dataavläsning.

Regeringen har inte ansett att det finns några skäl att låta vissa åtgärder som är möjliga att använda nationellt uteslutas från den föreslagna lagens tillämpningsområde. När hemlig dataavläsning införs i svensk rätt framstår det därför som helt följdenligt att föra in bestämmelser om åtgärden i lagen om europeisk utredningsorder. Så kan enklast ske genom vissa ändringar och tillägg i den föreslagna lagen om europeisk utredningsorder.

Till en början bör hemlig dataavläsning tas in i förteckningen i 1 kap. 4 §, vilken definierar utredningsåtgärder som en europeisk utredningsorder ska avse eller motsvara. I bestämmelsens sjätte punkt tas de gällande hemliga tvångsmedlen (utom kvarhållande av försändelse) upp och det är därför lämpligt att placera hemlig dataavläsning sist i uppräkningen som sker där.

Som en följd av att hemlig dataavläsning tas in som en utredningsåtgärd i lagen behöver vissa följdändringar också göras. En sådan följdändring är att hemlig dataavläsning ska kräva domstolsprövning innan åklagaren utfärdar en utredningsorder. Detta gäller enligt lagförslaget för övriga hemliga tvångsmedel. I 2 kap. 5 § första stycket 2 tas därför hemlig dataavläsning in i förteckningen. I den bestämmelsens andra stycke föreskrivs möjlighet för åklagaren att i avvaktan på domstolens beslut, under de förutsättningar som anges i rättegångsbalken, fatta interimistiskt beslut om utredningsorder (dock inte avseende hemlig rumsavlyssning). För att åklagaren ska ha möjlighet att fatta interimistiska beslut även avseende hemlig dataavläsning behövs en hänvisning till att sådana beslut får fattas i avvaktan på domstolens beslut under de förutsättningar som gäller enligt lagen om hemlig dataavläsning.

Motsvarande justering bör göras när det är fråga om erkännande och verkställande av utredningsorder. Även i de fallen gäller enligt 3 kap. 9 § att domstolsprövning ska ske men att åklagaren enligt 3 kap. 10 § i avvaktan på domstolens beslut, under de förutsättningar som gäller enligt rättegångsbalken, får besluta att erkänna och verkställa en utredningsorder avseende hemliga tvångsmedel (dock inte hemlig rumsavlyssning). Åklagaren bör också ges möjlighet att interimistiskt fatta beslut om att erkänna eller verkställa utredningsorder avseende hemlig dataavläsning. För att det ska vara möjligt behövs även här hänvisningen till lagen om hemlig dataavläsning.

Utfärdande av utredningsorder i Sverige

Utredningens förslag: En bestämmelse införs som klargör att när en utredningsorder för hemlig dataavläsning har utfärdats i Sverige så ska reglerna om att rätten eller åklagaren omedelbart ska häva beslut om det inte finns skäl för det, om avlyssnings-

förbud, om överskottsinformation och om granskning och bevarande av upptagning eller uppteckning i lagen om hemlig dataavläsning tillämpas.

I bestämmelsen klargörs också att när en utredningsorder för hemlig dataavläsning som avser avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter har utfärdats i Sverige gäller motsvarande som när en utredningsorder har utfärdats för hemlig avlyssning eller övervakning av elektronisk kommunikation.

För samtliga hemliga tvångsmedel finns särskilda bestämmelser i lagen om europeisk utredningsorder beträffande vad som gäller när en sådan utfärdats i Sverige (se 2 kap. 18 och 19 §§). När upptagningar och uppteckningar sker i utlandet är reglerna desamma, nämligen att reglerna i 27 kap. 22–24 §§ rättegångsbalken ska tillämpas. För hemlig avlyssning och övervakning av elektronisk kommunikation gäller också att i de fall upptagningen eller uppteckningen av avlyssningen eller övervakningen sker i Sverige så ska även 27 kap. 31–33 §§ rättegångsbalken tillämpas. Den särskilda bestämmelsen hänger samman med att det vid hemlig avlyssning eller övervakning av elektronisk kommunikation är möjligt med omedelbar överföring av meddelanden eller uppgifter om meddelanden till det land som utfärdat ordern.

De bestämmelser som alltid ska tillämpas vid utfärdande i Sverige av utredningsorder för hemliga tvångsmedel bör tillämpas även vid hemlig dataavläsning. Hänvisningen bör dock, i stället för till rättegångsbalkens bestämmelser, göras till motsvarande bestämmelser i lagen om hemlig dataavläsning. Den första av dessa är 16 § andra stycket lagen om hemlig dataavläsning (som motsvarar 27 kap. 23 rättegångsbalken). I den föreskrivs att om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning så ska den som ansökt om åtgärden eller rätten omedelbart upphäva beslutet. Nästa bestämmelse som det bör hänvisas till är 22 § lagen om hemlig dataavläsning (som motsvarar 27 kap. 22 § rättegångsbalken), i vilken motsvarande avlyssningsförbud som gäller enligt rättegångsbalken föreskrivs. Det bör avslutningsvis också hänvisas till 23 § första stycket lagen om hemlig dataavläsning (som genom hänvisningar tillbaka till rättegångsbalken motsvarar 27 kap. 23 a och 24 §§ i balken), vilken regle-

rar frågor om överskottsinformation och granskning av upptagningar och uppteckningar.

Enligt vårt förslag till lag om hemlig dataavläsning kommer åtgärden att kunna användas för att läsa av eller ta upp uppgifter som får hämtas in med befintliga hemliga tvångsmedel. För en utredningsorder för hemlig avlyssning och övervakning av elektronisk kommunikation som utfärdas i Sverige finns en särskild paragraf i lagen om europeisk utredningsorder (2 kap. 17 §). Motsvarande som gäller enligt den bör, av samma skäl som vi anfört ovan om de särskilda reglerna i lagen om internationell rättslig hjälp i brottmål, gälla för utfärdande av en utredningsorder för hemlig dataavläsning som avser avläsning eller upptagning av sådana uppgifter som får samlas in med dessa tvångsmedel. Dock bör hänvisningar ske till lagen om hemlig dataavläsning i stället för till rättegångsbalkens regler.

Verkställighet i Sverige av en europeisk utredningsorder

Utredningens förslag: När en utredningsorder för hemlig dataavläsning verkställs i Sverige ska bestämmelser gälla som motsvarar det som gäller när en utredningsorder om annat hemligt tvångsmedel innebär att upptagningar eller uppteckningar sker i Sverige. En ny regel införs om detta, i vilken det sker nödvändiga hänvisningar till bestämmelserna i lagen om hemlig dataavläsning.

När en utredningsorder för hemlig dataavläsning som avser avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter verkställs i Sverige ska det som gäller för hemlig avlyssning eller övervakning av elektronisk kommunikation gälla.

Reglerna i 3 kap. gäller erkännande och verkställighet i Sverige av en europeisk utredningsorder. De grundläggande reglerna i kapitlet som behandlar vad som ska gälla för erkännande av utredningsorder för hemliga tvångsmedel är generellt utformade och kräver enligt vår bedömning inga justeringar för att hemlig dataavläsning ska omfattas av dem. Samma sak gäller såvitt avser handläggningen av frågor om erkännande och verkställighet (se dock vad som sagts ovan beträffande justering i 3 kap. 10 §).

När det däremot gäller de särskilda reglerna om verkställighet av en utredningsorder finns vissa behov av justeringar för att hemlig dataavläsning ska omfattas av regleringen. Reglerna om verkställighet av utredningsorder för hemliga tvångsmedel finns i 3 kap. 34–37 §§. Den sista av dessa reglerar vad som ska gälla vid hemlig kameraövervakning och rumsavlyssning och hänvisar helt kort till att 36 § ska tillämpas vid verkställighet av en utredningsorder beträffande dessa åtgärder.

3 kap. 34–36 §§ reglerar vad som ska gälla vid verkställighet av en utredningsorder om hemlig avlyssning eller övervakning av elektronisk kommunikation. Reglerna är uppbyggda så att 34 § förklarar att åtgärderna kan verkställas antingen genom omedelbar överföring till den andra medlemsstaten eller genom upptagning eller uppteckning i Sverige (för senare befordran till den andra medlemsstaten). I det förra fallet tillämpas 35 §, som klargör 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 verkställbarhetsförklaring får verkställighet genom omedelbar överföring till den andra medlemsstaten av meddelanden eller uppgifter om meddelanden inte ske förrän domstolen har fastställt förklaringen. I övriga fall, dvs. när verkställighet av hemlig avlyssning och övervakning av elektronisk kommunikation inte sker genom omedelbar överföring och när det är fråga om verkställighet av övriga hemliga tvångsmedel, tillämpas 36 §. Dess innebörd är att upptagningar och uppteckningar inte behöver granskas enligt 27 kap. 24 § rättegångsbalken och att upptagningar som finns kvar i Sverige när ärendet avslutats får bevaras endast om det är tillåtet enligt 27 kap. 24 § rättegångsbalken. Dessutom gäller enligt bestämmelsen särskilda regler beträffande underrättelse till enskild, för att anpassa regleringen till att det i dessa fall inte är en svensk förundersökning som pågår. I förarbetena till bestämmelsen sägs bl.a. följande om de särskilda reglerna om underrättelse.

> Med hänsyn till att åtgärden vidtas i en utländsk brottsutredning ska, i fråga om tidpunkten för underrättelse, bestämmelserna i 27 kap. 31 § fjärde stycket rättegångsbalken inte tillämpas. I stället knyts underrättelseskyldigheten till den tidpunkt då avlyssningen eller övervakningen avslutades. Vad underrättelsen ska innehålla framgår av bestämmelserna i 27 kap. 32 § rättegångsbalken. De undantag från underrättelseskyldigheten som gäller enligt 27 kap. 31 § femte stycket och

> 33 § första stycket rättegångsbalken ska tillämpas. Utöver de sekretessbestämmelser som nämns i det sistnämnda lagrummet ska även sekretess enligt 18 kap. 17 § offentlighets- och sekretesslagen (2009:400) medföra att underrättelsen skjuts upp. Tidsfristen om ett år, som gäller i sekretessfallen, ska dock räknas från det att avlyssningen eller övervakningen avslutades, vilket ersätter bestämmelserna i 27 kap. 33 § andra stycket rättegångsbalken. Det är inte möjligt för svenska myndigheter att göra en sekretessprövning utan att kontakta den behöriga myndigheten i den andra medlemsstaten som har utfärdat utredningsordern. En sådan sekretessprövning bör göras dels i samband med att åtgärden avslutas, dels i samband med att ettårsfristen löper ut. Därutöver bör svenska myndigheter företa en ny prövning när de får sådan information från den utländska myndigheten som ger anledning till omprövning av sekretessfrågan. Underrättelse ska inte lämnas om den utländska brottsutredningen avser en gärning som motsvarar brott som anges i 27 kap. 33 § tredje stycket rättegångsbalken.[8]

Enligt vår bedömning bör verkställighet av en utredningsorder för hemlig dataavläsning som utgångspunkt regleras i enlighet med vad som gäller enligt 36 §, dvs. på motsvarande vis som gäller för övriga hemliga tvångsmedel när upptagning eller uppteckning skett i Sverige. Eftersom lagen om hemlig dataavläsning emellertid innehåller särskilda bestämmelser av motsvarande innebörd som de det hänvisas till i 36 § bör hänvisningarna göras till dessa bestämmelser. Av tydlighetsskäl bör detta skrivas ut i en ny bestämmelse.

Av den nya bestämmelsen bör således först framgå att granskning inte behöver ske. Hänvisningen bör göras till 23 § första stycket lagen om hemlig dataavläsning som sedan hänvisar till rättegångsbalkens bestämmelse om detta. Vidare bör det upplysas om att upptagningar och uppteckningar som finns kvar i Sverige efter det att ärendet har avslutats hos åklagaren och bevismaterialet har överlämnats till den andra staten endast får bevaras om det är tillåtet enligt 23 § lagen om hemlig dataavläsning.

När det gäller underrättelse till enskild är det tillräckligt med en hänvisning till 36 § andra stycket tillsammans med ett påpekande om att det som där anges gäller för hemlig dataavläsning enligt vad som framgår av 23 § andra stycket lagen om hemlig dataavläsning, som anger att 27 kap. 31–33 §§ rättegångsbalken gäller även vid hemlig dataavläsning. Det bör också anges att 25 § lagen om hemlig dataavläsning ska tillämpas eftersom det där görs ett förtydligande av

[8] Prop. 2016/17:218 s. 287.

betydelse för underrättelsereglerna när de tillämpas vid hemlig dataavläsning.

Det bör också införas en bestämmelse som klargör att när en utredningsorder för hemlig dataavläsning som avser kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter ska verkställas i Sverige så bör det, på motsvarande vis som gäller för hemlig avlyssning och övervakning av elektronisk kommunikation, finnas möjlighet till omedelbar överföring. Den bestämmelsen kan lämpligen utformas genom hänvisningar till 34 och 35 §§, dock med angivande av reglerna i lagen om hemlig dataavläsning i stället för rättegångsbalkens regler i förekommande fall. Den nya bestämmelsen bör placeras efter den regel som klargör vad som ska gälla vid verkställighet av utredningsorder om hemlig kameraövervakning eller rumsavlyssning.

Underrättelse om hemlig dataavläsning

Utredningens förslag: En särskild bestämmelse införs om att det som gäller för hemlig avlyssning och övervakning av elektronisk kommunikation såvitt avser underrättelse från Sverige till annan stat och från 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 lokaliseringsuppgifter.

I 4 kap. 12–15 §§ finns bestämmelser om underrättelse till annan medlemsstat och om förfarandet när annan medlemsstat underrättar Sverige beträffande hemlig avlyssning eller övervakning av elektronisk kommunikation som avses att genomföras, genomförs eller har genomförts beträffande ett telefonnummer, en annan adress eller elektronisk kommunikationsutrustning som används på den andra statens territorium. Bestämmelserna grundar sig på artikel 31 direktivet om en europeisk utredningsorder, se vidare prop. 2016/17:218 s. 226 ff. Eftersom hemlig dataavläsning vid avläsning av kommunikationsavlyssnings-, kommunikationsövervaknings- och lokaliseringsuppgifter i praktiken kommer att vara ett sätt att komma åt samma uppgifter som får hämtas in genom hemlig avlyssning eller övervakning av elektronisk kommunikation bör motsvarande gälla

beträffande underrättelse och prövning av annan stats underrättelse som gäller för dessa tvångsmedel, för att Sverige ska fullgöra sina förpliktelser enligt direktivet. Lämpligen bör därför en bestämmelse som, när hemlig dataavläsning används i dessa fall, hänvisar till reglerna om hemlig avlyssning av elektronisk kommunikation tas in i lagen om europeisk utredningsorder.

11.3 Exekutiv jurisdiktion vid hemlig dataavläsning; lagringsfallen

11.3.1 Bakgrund

Sveriges hållning när det gäller exekutiv jurisdiktion vid tvångsmedelsanvändning är att svenska brottsbekämpande myndigheter inte har rätt att ta del av elektroniska uppgifter som 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 den. Detta är ett utflöde av den svenska tolkningen av territorialitetsprincipen vid exekutiv jurisdiktion.

Det kan redan här sägas att när hemlig dataavläsning ska avse uppgifter i informationssystem som är användarkonton till kommunikations- eller lagringstjänster så innebär den svenska hållningen att hemlig dataavläsning kan förväntas bli begränsat effektiv. Det hänger samman med att de allra flesta stora kommunikations- och lagringstjänsteföretagen kan antas lagra de uppgifter som deras användare förser dem med på annan plats än i Sverige. I vart fall är sannolikheten stor att det, även om tjänsteleverantören har servrar i Sverige, inte går att klarlägga att just de aktuella uppgifterna lagras här i det ögonblick verkställighet sker.

Den svenska tolkningen av territorialitetsprincipen står emellertid inte oemotsagd. Många andra länder gör nämligen en annan tolkning, vilket kommer att framgå i de följande avsnitten.

De folkrättsliga principerna om exekutiv jurisdiktion har vuxit fram i tider då information inte var rörlig på det sätt som elektronisk information av dagens snitt är. Därför utgår principerna från fysiska snarare än virtuella eller faktiska förhållanden. Det kan mot den bakgrunden ifrågasättas om Sveriges strikta tolkning är rimlig och

kommer att stå sig över tid. Inte minst det arbete som för närvarande sker på bred global front till följd av unilaterala lösningar talar för att någonting måste göras. Kapitlet avslutas därför med en diskussion om för- och nackdelar med att i vissa avseenden göra avsteg från den hittillsvarande svenska hållningen avseende exekutiv jurisdiktion.

11.3.2 Europarådets arbete med it-brottskonventionen och frågan om exekutiv jurisdiktion på internet

Inom Europarådet pågår ett internationellt arbete som handlar om det vi beskrivit som lagringsfallen och andra liknande frågor. Diskussionerna där tar sin utgångspunkt i Europarådets konvention om it-relaterad brottslighet (ETS nr 185, nedan kallad it-brottskonventionen) och några särskilda bestämmelser i den konventionen. För att sätta de diskussioner som förs i ett sammanhang har vi därför funnit det lämpligt att först redovisa något om it-brottskonventionen och de aktuella bestämmelserna innan vi behandlar de nutida diskussionerna.

Bakgrund till it-brottskonventionen

Tillkomsten av it-brottskonventionen ska ses mot bakgrund av de genomgripande förändringar i samhället som datoriseringen och de globala datornätverken har fört med sig och att en effektiv kamp mot it-relaterad brottslighet kräver ett utvidgat, snabbt och väl fungerande internationellt samarbete. I november 1996 beslutade Europarådets styrkommitté för brottsfrågor (CDPC) att uppdra åt en expertkommitté att utreda frågor rörande it-relaterad brottslighet med sikte på en konvention eller annan bindande internationell överenskommelse. Efter beslut i ministerrådet påbörjades arbetet på en konvention om it-relaterad brottslighet i april 1997. Den slutliga versionen av konventionen förelades ministerrådet i juni 2001. Konventionen antogs av ministerrådet den 8 november 2001 och öppnades för undertecknande den 23 november 2001 samt trädde i kraft den 1 juli 2004. Hittills (per den 3 november 2017) har 56 stater ratificerat konventionen.[9] En överväldigande majoritet av EU:s med-

[9] Https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

lemsstater har ratificerat konventionen. Det har också de övriga nordiska länderna. Även stater som inte är medlemmar i Europarådet har anslutit sig till och ratificerat konventionen, t.ex. Australien, Japan, Kanada och USA.

Sverige undertecknade konventionen samma dag som den upprättades, men har, i likhet med fyra andra länder som undertecknat den, ännu inte ratificerat den. Frågan om Sverige bör tillträda konventionen och tilläggsprotokollet samt vilka lagändringar som krävs för ett tillträde har behandlats i dels promemorian *Brott och brottsutredning i it-miljö* (Ds 2005:6), dels betänkandet *Europarådets konvention om it-relaterad brottslighet* (SOU 2013:39). I promemorian gjordes bedömningen att Sverige bör tillträda konventionen och i betänkandet, där direktiven förutsatte att konventionen skulle tillträdas, lämnades förslag på författningsändringar som behövs för att Sverige ska kunna leva upp till kraven i konventionen och dess tilläggsprotokoll. Beredningsarbete pågår för närvarande inom Regeringskansliet. Den omständigheten att Sverige inte har anslutit sig till konventionen innebär bland annat att Sverige inte deltar i de diskussioner som förs om ändringar av och tillägg till konventionen till följd av t.ex. de problem som uppstår vid loss of location.

It-brottskonventionens innehåll avseende möjligheten att bereda sig tillgång till elektroniskt lagrade uppgifter i annan stat

I it-brottskonventionens artikel 32 finns bestämmelser som gäller staters möjlighet att bereda sig tillgång till uppgifter som lagrats inom andra fördragsslutande staters territorium. Enligt artikel 32 får en fördragsslutande stat

– utan tillstånd av en annan sådan stat bereda sig åtkomst till lagrade datorbehandlingsbara uppgifter som är allmänt tillgängliga, oavsett var uppgifterna befinner sig geografiskt, eller
– genom ett datorsystem inom sitt territorium bereda sig åtkomst till eller ta emot lagrade datorbehandlingsbara uppgifter som finns hos annan fördragsslutande stat, om den förstnämnda staten erhåller lagligt och frivilligt samtycke av den person som har laglig rätt att röja uppgifterna för staten via det datorsystemet.

Artikeln medför i sig inte några egentliga förpliktelser utan är att betrakta som en överenskommelse om att tillåta en annan fördragsslutande stat att utan underrättelse eller tillstånd ta del av datorbehandlingsbara uppgifter som tekniskt sett finns på det egna territoriet. De två situationer då en stat ska kunna få åtkomst till uppgifter på en annan stats territorium, utan underrättelse eller tillstånd, som räknas upp i artikeln är situationer som alla de stater som var med och utarbetade konventionen var eniga om redan vid dess tillkomst var folkrättsligt tillåtna. (SOU 2013:39 s. 196). Det kan nämnas att det i den förklarande rapporten till konventionen anges bl.a. följande beträffande artikel 32.

> The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules.[10]

Man bör när man läser citatet komma ihåg att uttalandena om att det bl.a. på grund av bristande konkret erfarenhet av situationerna ännu inte var möjligt att reglera frågorna på ett bindande sätt gjordes i början av 2000-talet och att diskussionerna fördes under 1990-talet.

Det ska också sägas att artikel 39.3 i it-brottskonventionen anger att ingenting i konventionen ska inverka på en parts övriga rättigheter, begränsningar, skyldigheter eller ansvar. Enligt den nyss citerade förklarande rapporten innebär detta att konventionen varken tillåter eller utesluter gränsöverskridande åtkomst till elektroniskt lagrade uppgifter utan tillstånd från den andra staten i andra situationer än de som anges i artikel 32.[11]

[10] *Explanatory Report to the Convention on Cybercrime* s. 53 p. 293. Rapporten finns tillgänglig på https://rm.coe.int/16800cce5b
[11] Se föregående not, samma ställe.

Europarådets arbete på området efter it-brottskonventionens upprättande

Transbordergruppens kartläggning

Inom Europarådet har det inrättats en särskild kommitté för it-brottskonventionen (T-CY) vars uppdrag bl.a. är att underlätta tillämpningen och genomförandet av konventionen, vara en plattform för utbytande av information mellan konventionens parter och överväga eventuella ändringar av konventionen. När det gäller här relevanta frågor har olika arbetsgrupper knutits till kommittén. Tidigare arbetade den s.k. Transbordergruppen[12] med frågorna. Av särskilt intresse här är att den gruppen i en rapport 2012 kartlade och redovisade tillämpningen (avseende åren 2009–2010) i ett antal olika länder beträffande gränsöverskridande tillgång till elektroniskt lagrade uppgifter samt kom med rekommendationer till T-CY.[13]

I den nämnda kartläggningen utgick man från olika exempel vilka redovisas i det följande.[14]

> Exempel 1) Gränsöverskridande tillgång till uppgifter vid rannsakan
>
> Vid en rannsakan mot en misstänkt person påträffas en påslagen dator. Den brottsbekämpande myndigheten får, av den misstänkte, nödvändiga inloggningsuppgifter för att komma åt uppgifter som lagras elektroniskt på annan plats än lokalt i datorn men som kan tillgängliggöras från datorn.

I de flesta stater som ingick i kartläggningen var det tillåtet för den brottsbekämpande myndigheten att från den misstänktes dator direkt bereda sig tillgång till uppgifter som lagras på annan plats om det inte var uppenbart i vilken stat uppgifterna lagrades. De flesta stater tillät också användning av inloggningsuppgifter erhållna från den misstänkte för sådan direkt tillgång. Om det däremot stod klart att uppgifterna lagras i annan stat än den egna kunde brottsbekämpande myndigheter i sju länder[15] bereda sig tillgång till uppgifterna

[12] Enligt Europarådets webbsida var The Transborder Group en ”Ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows”, se www.coe.int/en/web/cybercrime/tb

[13] Se *Transborder access and jurisdiction: What are the options?*, tillgänglig på https://rm.coe.int/16802e79e8

[14] Uppgifterna i det följande är hämtade från rapportens avsnitt 4. Översättningar från engelska till svenska är gjorda av utredningen.

[15] Finland, Portugal, Polen Chile, Montenegro, Japan och USA.

medan detta i tio länder[16] då inte var tillåtet, såvida inte den misstänkte själv frivilligt samarbetar i enlighet med vad som gäller enligt artikel 32. I nästan alla stater gjorde det ingen skillnad för frågan om rätten till gränsöverskridande tillgång till uppgifterna om det var brådskande eller förelåg en risk för att informationen skulle kunna försvinna. I vissa stater fanns krav på underrättelse till annan stat.

> Exempel 2) Gränsöverskridande tillgång till uppgifter med lagligt erhållna inloggningsuppgifter
>
> Den brottsbekämpande myndigheten har på ett lagligt sätt erhållit inloggningsuppgifter till en tjänst med påstått olagligt innehåll eller graverande (eng. incriminating) bevisning.

De flesta svarande staterna kunde i detta fall bereda sig tillgång till uppgifterna från de brottsbekämpande myndigheternas egna datorer om det inte var uppenbart var uppgifterna lagrades. Även om det stod klart att uppgifterna lagrades utanför den egna staten kunde fortfarande de flesta[17] stater bereda sig sådan tillgång från de egna datorerna.

> Exempel 3) Gränsöverskridande tillgång till uppgifter med särskild mjukvara eller tekniska metoder
>
> Under en brottsutredning har den brottsbekämpande myndigheten fått kännedom om ett datorsystem med påstått olagligt innehåll eller graverande bevisning.

Brottsbekämpande myndigheter i vissa stater var, enligt den inhemska lagstiftningen, med hjälp av mjukvara eller andra tekniska metoder tillåtna att skaffa sig tillgång på distans till information om uppgifterna om det inte var uppenbart i vilken stat uppgifterna lagrades. I majoriteten av dessa stater var det dock endast tillåtet under mycket speciella förhållanden. Om det stod klart att det informationssystem som åtgärden skulle riktas mot fanns i en annan stat än den egna var sådana åtgärder endast tillåtna i några få svarande länder.[18]

[16] Tjeckien, Litauen, Tyskland, Sverige, Turkiet, Bosnien och Hercegovina, Japan, Ungern, Estland och Nederländerna.
[17] De enda undantagen utgjordes av Tjeckien, Litauen, Sverige, Ungern, Estland och Nederländerna.
[18] Bosnien och Hercegovina, Japan och (kanske) Chile.

Exempel 4) Gränsöverskridande tillgång till uppgifter med samtycke

Under en brottsutredning får den brottsbekämpande myndigheten lagligen och frivilligt samtycke från en person att bereda sig tillgång till elektroniska uppgifter som tillhör denne och kan utgöra viktig bevisning men som lagras i en annan stat än den egna.

Brottsbekämpande myndigheter i nästan alla svarande stater kunde i detta fall bereda sig tillgång till och genom nedladdning (eng. download) säkra bevisningen om den person som lämnat sitt samtycke fysiskt fanns i den egna staten. Om personen fanns i staten där uppgifterna lagrades var det fortfarande tillåtet i de flesta svarande stater, medan det i några var otillåtet alternativt tveksamt eller krävde ytterligare förutsättningar eller inte var tydligt reglerat. I de flesta stater var det i detta fall också av betydelse att den som erbjöd tillgången hade rätt att avslöja uppgifterna i den stat där dessa lagrades.

Exempel 5) Information erhållen från tjänsteleverantör

Under en brottsutredning måste den brottsbekämpande myndigheten komma åt teknisk information som rör en misstänkt från en internetbaserad tjänstetillhandahållare.

I alla svarande stater gällde att tjänsteleverantören, om uppgifterna avsåg en person i den egna staten samt lagrades och administrerades där, var skyldig att förse den brottsbekämpande myndigheten med uppgifterna. Om uppgifterna däremot avsåg en person i den egna staten men fanns lagrade och administrerades i en annan stat krävdes i de flesta fall internationell rättslig hjälp (mutual legal assistance, MLA). Det gällde också om informationen gällde en person i en annan stat som hade gjort sig skyldig till brott i den egna staten om uppgifterna lagrades och administrerades i en annan stat. Det konstaterades också att många stater upplevde stora problem, både tekniska och juridiska, med att samla in uppgifter som lagrades i en annan stat.

Molnbevisgruppens arbete

Sedan Transbordergruppens mandat löpt ut inrättades en ny grupp som knöts till T-CY, Cloud Evidence Group (nedan kallad Molnbevisgruppen). Dess huvudsakliga fokus är, som namnet antyder,

frågor som rör bevisning i molnet. Gruppen fick i uppdrag att avge en slutrapport senast i slutet av 2016 med alternativ och rekommendationer till hur man kan gå vidare med frågor som gäller tillgång till molnlagrad bevisning.

I Molnbevisgruppens rapport[19] diskuteras bl.a. frågor som här är av intresse, bl.a. exekutiv jurisdiktion vid frågor om loss of location. Där anges att det är långtifrån klart vilka regler som gäller i fråga om möjligheten för brottsbekämpande myndigheter att bereda sig tillgång till uppgifter som lagrats i molnet. Enligt rapporten är det möjligt att vid molnlagring och loss of location, till skillnad från vad som är fallet i den fysiska världen där ju fysiska ting endast kan finnas på ett ställe samtidigt, argumentera för andra relevanta anknytningspunkter än platsen där lagring sker för att avgöra vilket land som har exekutiv jurisdiktion. Förutom den stat där uppgifterna finns lagrade eller servern finns skulle exekutiv jurisdiktion enligt rapporten kunna tillkomma exempelvis en stat där tjänsteleverantören har sitt säte, en stat där tjänsteleverantören har en filial, en stat där den misstänkte har träffat avtal om molntjänsten, en stat där den misstänkte finns eller en stat där den misstänkte är medborgare.

I rapporten konstateras vidare, bl.a. med hänvisning till Transbordergruppens arbeten, att avsaknaden av ett tydligt, effektivt och fungerande (”feasible”) internationellt regelverk har lett till att stater i allt högre grad väljer att tillgripa unilaterala lösningar för att få tillgång till elektroniskt lagrade uppgifter i molnet. Det tycks således enligt rapporten vara utbrett att de brottbekämpande myndigheterna inom ramen för sina ärenden skaffar sig tillgång inte bara till sådana elektroniska uppgifter som är lagrade i en misstänkts elektroniska informationsbärare utan också till information på exempelvis ett webbmejlkonto eller molntjänstkonton, om informationsbäraren är olåst under undersökningen eller man på lagligt sätt fått tag i inloggningsuppgifter. Detta sker, såvitt framgår av rapporten, även när myndigheterna vet att uppgifterna finns i ett annat, känt, land.[20]

En av slutsatserna i rapporten är att det behövs ett gemensamt internationellt ramverk som minskar risker för mellanstatliga konflikter och stärker skyddet för enskilda, inklusive deras säkerhet.

[19] *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*, tillgänglig på https://rm.coe.int/16806a495e
[20] Se Molnbevisgruppens rapport s. 16.

En sådan lösning skulle enligt Molnbevisgruppen t.ex. kunna fokusera mindre på var elektroniskt lagrade uppgifter finns och i stället mer på var personen som innehar informationen och en eventuell målsägande finns. Enligt Molnbevisgruppen skulle de brottsbekämpande myndigheterna med en sådan lösning lagligen och gränsöverskridande kunna bereda sig tillgång till elektroniskt lagrade uppgifter oavsett var de är lagrade så länge det finns förutbestämda begränsningar av när så får ske.[21]

Inom ramen för sitt arbete granskade Molnbevisgruppen också den s.k. ”long-arm”-doktrinen som tillämpas i fråga om EU:s regelverk på antitrustområdet. EU-kommissionen har bl.a. rekommenderat[22] att de nationella konkurrensmyndigheterna i EU:s medlemsstater ska kunna bereda sig tillgång till uppgifter i servrar var som helst i världen i syfte att samla bevis i antitrustförfaranden. Rätten att samla elektronisk bevisning, borde enligt rekommendationen omfatta en rätt att få del av uppgifter som det inspekterade objektet har tillgång till och som har koppling till den undersökta verksamheten.[23]

Molnbevisgruppen gjorde mot bakgrund av det som nu anförts bedömningen att ett ramverk som behandlar vad som ska gälla för gränsöverskridande tillgång till elektroniskt lagrade uppgifter måste definiera vilka förutsättningar och rättssäkerhetsgarantier som ska gälla för att både skydda enskildas rättigheter och förhindra att andra staters eller dessas myndigheters rättigheter inskränks eller påverkas (ömsesidigt erkännande).[24]

Inför de rekommendationer som Molnbevisgruppen lämnade konstaterade den inledningsvis att internationell rättslig hjälp (eng. mutual legal assistance) är den primära vägen för stater att få del av elektronisk bevisning som lagras i andra stater än den egna. Samtidigt konstaterades att detta instrument sällan är en möjlig väg framåt när det är fråga om molnlagrade uppgifter, dels på grund av tidsaspekten (bl.a. risken att information försvinner), dels på grund av att det är svårt eller omöjligt att veta var uppgifterna finns. Trots

[21] Se Molnbevisgruppens rapport s. 16 (p. 46–47).
[22] European Competition Network, *Recommendation on the power to collect digital evidence, including by forensic means*, tillgänglig på http://ec.europa.eu/competition/ecn/ecn_recommendation_09122013_digital_evidence_en.pdf
[23] Se Molnbevisgruppens rapport s. 16 och 17 (p. 48).
[24] Se Molnbevisgruppens rapport s. 17 (p. 49).

detta anförde Molnbevisgruppen att möjligheterna till internationell rättslig hjälp måste uttömmas för att nya och innovativa förslag till lösningar avseende jurisdiktionsfrågorna ska kunna få bred acceptans.[25]

När det sedan gäller rekommendationerna, vilka tog sikte inte bara på loss of location-problematiken utan även på andra frågor om insamling av molnlagrad bevisning, anförde Molnbevisgruppen bl.a. att konventionsparterna skulle överväga att vidta generella åtgärder beträffande utbildning, statistik och uppföljning avseende internationell rättslig hjälp för att denna skulle bli mer effektiv. Därtill föreslogs ett antal mer direkta åtgärder för att väsentligt förbättra det internationella rättsliga samarbetet på området, såsom att förstärka möjligheterna till dygnetruntkontakter mellan stater och strömlinjeformning av processer vid ansökningar om rättslig hjälp.[26] Enligt Molnbevisgruppen finns skäl att inom ramen för utarbetandet av ett tilläggsprotokoll till it-brottskonventionen behandla bl.a. de nämnda förslagen.

I arbetet med ett sådant tilläggsprotokoll finns enligt Molnbevisgruppen också skäl att överväga frågor som mer direkt tar sikte på de här relevanta svårigheterna och möjligheten för stater att bereda sig tillgång till fjärrlagrade uppgifter genom gränsöverskridande direktåtkomst till dessa. Det rekommenderades att några av de förslag som tidigare lagts fram av Transbordergruppen, efter den ovan presenterade kartläggningen, tas upp till förnyad behandling. De förslag som enligt Molnbevisgruppen bör tas upp till förnyat övervägande är följande.[27]

– *Gränsöverskridande direktåtkomst till uppgifter utan samtycke då de brottsutredande myndigheterna på laglig väg fått fram inloggningsuppgifter till en molntjänst*. En sådan bestämmelse skulle kunna ge en konventionspart rätt att utan tillstånd av en annan part, under en brottsutredning eller rättegång och från ett informationssystem på sitt territorium, bereda sig tillgång till och samla in uppgifter som lagras elektroniskt i en annan stat. Det skulle förutsätta att den informationssökande konventionsparten fått inloggningsuppgifterna genom lagliga utredningsåtgärder.

[25] Se Molnbevisgruppens rapport s. 35 (p. 90 och 91).
[26] Se Molnbevisgruppens rapport s. 35–36.
[27] Se Molnbevisgruppens rapport s. 45 f. Exemplen är översatta av utredningen.

Den informationssökande parten skulle också vara skyldig att underrätta den andra parten före, under eller efter att uppgifterna samlats in. Ytterligare villkor och skyddsåtgärder skulle också behövas.

– *Gränsöverskridande direktåtkomst till uppgifter utan samtycke i god tro eller i nödsituationer eller under liknande omständigheter*. En sådan bestämmelse skulle kunna tillåta gränsöverskridande tillgång till uppgifter i specifika situationer för att förhindra överhängande fara, fysisk skada, en misstänkts flykt eller liknande. Bestämmelsen skulle också kunna innefatta situationer där det finns risk för att relevant bevisning förstörs eller går förlorad. Bestämmelsen kan också behöva täcka in ”godtrossituationer”, dvs. där en brottsbekämpande myndighet vid en utredning inte vet (säkert) om uppgifterna lagras på ett främmande territorium, inte vet på vilket territorium uppgifterna lagras eller där uppgifterna av misstag samlats in från ett främmande territorium. Särskilda villkor och skyddsåtgärder skulle liksom i föregående förslag behöva definieras och bestämmas och det bör krävas underrättelse till den andra staten.

– *Tillmätande av andra anknytningsfaktorers betydelse vid bedömningen av territorialitetsprincipen och därmed också av jurisdiktionsfrågan*. Detta förslag tar sikte på den specifika loss of location-problematiken och den traditionella tolkningen av territorialitetsprincipen. Sådana omständigheter som att elektroniskt lagrade uppgifter samtidigt kan finnas på olika platser (i olika territorier), vara dynamiskt sammansatta från olika geografiska områden eller, genom s.k. cachning (lokalt sparande) eller spegling finnas tillgängliga samtidigt på flera ställen innebär att det kan vara svårt att förlita sig på den hävdvunna tolkningen av territorialitetsprincipen (som grundar sig på platsen där uppgifterna lagras eller informationssystem finns) för att avgöra vilken stat som har jurisdiktion. Det har därför hävdats att nya sätt att tolka och tillämpa territorialitetsprincipen är nödvändiga. I sammanhanget har föreslagits att andra anknytningsfaktorer än uppgifternas eller informationssystemets lokalisering kan vara möjliga att tillmäta betydelse. Exempelvis skulle sådana relevanta anknytningsfaktorer kunna vara platsen där personen som har möjlighet att ta bort uppgifterna finns eller platsen där den som äger eller

kontrollerar uppgifterna finns. Även om lagringsplatsen inte kan bestämmas tydligt kan uppgifterna (och därmed jurisdiktionen) kopplas till en person som t.ex. har befogenhet att ändra, ta bort, undertrycka eller göra informationen oanvändbar för andra samt har rätt och möjlighet att utesluta andra från åtkomst, tillgång eller användning av informationen. Även vid en ändrad tolkning och tillämpning av territorialitetsprincipen kommer det krävas att särskilda villkor och skyddsåtgärder utarbetas.

Sedan Molnbevisgruppen lämnade sin rapport, vilken T-CY principiellt ställde sig bakom, har ett förslag presenterats med villkor för utarbetande av ett andra tilläggsprotokoll till it-brottskonventionen.[28] Förslaget antogs av T-CY i juni 2017. Vid samma tid beslutade T-CY också att inrätta en förslagsgrupp till vilken samtliga stater som tillträtt it-brottskonventionen får utse egna experter.[29] Därmed pågår för närvarande inom Europarådet ett arbete för att få till stånd lösningar avseende bl.a. loss of location-problematiken. De nyss presenterade förslagen kommer således att inom relativ närtid bli föremål för fortsatta diskussioner. Eftersom Sverige inte har tillträtt it-brottskonventionen deltar Sverige inte med representanter i dessa diskussioner.

11.3.3 EU:s arbete på motsvarande område

Även inom EU pågår, som nämnts, arbete med motsvarande frågor som de frågor Europarådet diskuterar. Där har fokus möjligen varit ännu mer inriktat på själva insamlingen av elektroniskt lagrad bevisning och metoder för sådan, mot bakgrund av att det ansetts att dagens metoder ger för otillfredsställande resultat.[30]

I april 2015 åtog sig kommissionen att ta itu med de utmaningar som finns på området för it-relaterad brottslighet. Rådet ställde sig i juni 2016 bakom kommissionen och uttalade bl.a. att samarbetet med tjänsteföretagen på området ska förbättras, att processerna för

[28] Se https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b
[29] Se https://rm.coe.int/t-cy-17-meeting-report-/168072366d
[30] Se https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en

det internationella rättsliga samarbetet måste effektiviseras och att reglerna om exekutiv jurisdiktion i cyberspace ska ses över.[31] Rådet begärde att kommissionen skulle lämna en delrapport i slutet av 2016 för att sedan, i juni 2017, presentera resultatet av sina undersökningar.

Kommissionen har i arbetet med frågorna vidtagit olika åtgärder; bl.a. har man konsulterat experter och berörda aktörer, inkluderande t.ex. privat sektor, brottsbekämpande myndigheter och organisationer från det civila samhället, för att söka lösningar på problemen. Man har också hållit såväl bilaterala som multilaterala möten. I december 2016 redovisade kommissionen för rådet hur arbetet dittills förflutit och pekade i rapporten bl.a. på de problem som uppstår när det inte är möjligt att lokalisera var vissa uppgifter finns (loss of location) och de risker som uppstår när medlemsstaterna hanterar detta på olika sätt.[32]

I juni 2017 presenterade kommissionen, i ett s.k. nonpaper[33], olika tänkbara lösningar i arbetet med e-bevisning och jurisdiktion i cyberspace. När det gäller frågan om loss of location angavs bl.a. följande.

> In some situations the location of data, infrastructure or a service provider cannot be established ("loss of knowledge of location situations") or there is a risk of losing data. In such cases, a number of Member States already today provide for possibilities to access and in some cases copy the data directly from a computer system. The experts suggest that at EU level common conditions and minimum safeguards for such direct access in potential crossborder situations could be defined, as well as mitigating measures such as notifications to other possibly affected countries. Such common conditions and safeguards would aim to reinforce mutual trust and loyal cooperation between the Member States while preserving national measures where they exist. Alternatively, this could also be limited to providing a common framework for notification of another (Member) State affected, while not touching the domestic regime for direct access.[34]

[31] Se rådets slutsatser på https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/council_conclusions_on_improving_criminal_justice_in_cyberspace_en.pdf
[32] Se http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf
[33] En rapport med förbehållet "This document is prepared by the Commission services and cannot be considered as stating an official position of the Commission."
[34] Se https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

Vid rådets sammanträde i juni 2017 begärde ministrarna att kommissionen skulle fortsätta sitt arbete med att föreslå praktiska åtgärder och lägga fram konkreta lagstiftningsförslag. Kommissionären Jourová har därefter meddelat att det är hennes intention att lägga fram lagstiftningsförslag som kan antas av kommissionen i början av 2018. Under hösten 2017 har en s.k. inception impact assessment på temat ”Legislative proposal on access to electronic evidence in criminal investigations” publicerats för att få in synpunkter från berörda parter. Därtill har seminarier för intressenter hållits och ett frågeformulär för att fånga upp allmänhetens synpunkter funnits tillgängligt. Även inom EU kan således fortsatta diskussioner (och kanske också lagförslag) på området förväntas.

11.3.4 Kort om rättspraxis

Det saknas såvitt utredningen känner till avgöranden i överrätterna som tar sikte på hur territorialitetsprincipen vid exekutiv jurisdiktion ska tolkas i Sverige. Utredningen har däremot kännedom om två underrättsavgöranden (tingsrätt) som har gällt s.k. intrångsundersökningar i upphovsrättsliga mål. I de fallen har domstolarna tillåtit sådana undersökningar även beträffande molnlagrade uppgifter.

I Danmark har den högsta domstolen (Højesteret) i ett mål år 2012 avseende s.k. hemliga upprepade rannsakningar slagit fast att sådana kan avse uppgifter på ett användarkonto (i det fallet en persons Facebook- och Messengerprofil till vilka den brottsbekämpande myndigheten hade lösenorden). Højesteret godkände åtgärden och angav beträffande territorialitetsfrågan följande.

> Da den kriminalitet, T er sigtet for, er undergivet dansk straffemyndighed, da sagen efterforskes af danske myndigheder, og da indgrebene kan foretages uden at involvere udenlandske myndigheder, kan det ikke føre til et andet resultat, at T fra februar 2010 til februar 2011 befandt sig i udlandet, og at oplysningerne på profilerne befinder sig på servere i udlandet. Herefter – og da de øvrige betingelser for at godkende indgrebene i retsplejelovens § 794 findes at være opfyldt – tiltræder Højesteret, at det er tilladt politiet at aflæse Ts Facebook- og Messengerprofiler. [35]

[35] Se avgörande från Højesteret den 10 maj 2012 i sag 129/2011, tillgängligt på www.hoejesteret.dk/hoejesteret/nyheder/Afgorelser/Documents/K-129-11.pdf

Højesteret använde således andra anknytningspunkter (kriminaliteten omfattades av dansk jurisdiktion, utreddes av danska myndigheter och ingreppet kunde vidtas utan hjälp av utländska myndigheter) än sådana som den svenska hållningen avseende territorialitetsprincipen (lagringsplatsen) skulle ta sikte på.

I Norge kan, som tidigare framhållits, såväl hemlig dataavläsning som hemlig rannsakan riktas mot användarkonton på internetbaserade kommunikations- och lagringstjänster. Motsvarande motsvarande kriterier som de Højesteret i Danmark framhöll och andra anknytningspunkter till Norge synes då vara av relevans beträffande jurisdiktionsfrågan.[36]

11.3.5 Vår bedömning

Utredningens bedömning: Det finns starka skäl att nyansera den hittillsvarande svenska hållningen avseende vad territorialitetsprincipen vid exekutiv jurisdiktion innebär för elektroniskt lagrade uppgifter. 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 aktivt arbeta för att få till stånd internationella överenskommelser i aktuella frågor. Ett första steg för Sverige att ta bör vara att ratificera it-brottskonventionen för att alls få delta i de samtal och diskussioner som nu förs i Europarådet.

Nya tekniska lösningar för bl.a. lagring och kommunikation har inneburit utmaningar för brottsbekämpande myndigheter såvitt avser jurisdiktion. Fenomenet är inte lokalt utan snarare globalt. Trots detta finns inga breda internationella överenskommelser på området utöver it-brottskonventionen, vilken endast löser en mycket liten del av den beskrivna problematiken. För svensk del är inga internationella överenskommelser på det här relevanta området tillämpliga eftersom vi inte har tillträtt it-brottskonventionen.

[36] Se t.ex. kap. 5 i *Skjulte tvangsmidler*, Ingvild Bruce og Geir Sunde Haugland, Universitetsforlaget / kommentarutgaver.no - 28-03-2017.

I svenska lagar som ger myndigheter möjligheter att vidta åtgärder mot enskilda (t.ex. tvångsmedel) nämns aldrig uttryckligen att det ska föreligga exekutiv jurisdiktion för Sverige för att åtgärdena ska få vidtas. Det är underförstått att så ska vara fallet och att de svenska lagarna endast gäller om svensk jurisdiktion föreligger. I de lagar som reglerar det internationella samarbetet finns visserligen regler som ger svenska myndigheter vissa möjligheter att agera även när det inte finns jurisdiktion med sedvanlig tillämpning av territorialitetsprincipen. Ett exempel på detta är reglerna om direktöverföring vid hemlig avlyssning av elektronisk kommunikation enligt lagen om internationell rättslig hjälp i brottmål. Sådana regler grundar sig på avtal som antingen är bi- eller multilaterala. När det inte finns några sådana avtal (och inhemska bestämmelser) gäller enligt den angivna lagen att åklagaren kan begära rättslig hjälp från den andra staten (se t.ex. 1 kap. 7 § lagen om internationell rättslig hjälp i brottmål). Någon möjlighet att utan sådan hjälp vidta åtgärder föreskrivs inte i lag, och skulle inte heller ha någon verkan även om den föreskrevs.

När det särskilt gäller den s.k. loss of location-problematiken är det många gånger praktiskt möjligt för den brottsbekämpande myndigheten att ta del av uppgifter som lagras utanför det egna territoriet utan att befinna sig där uppgifterna finns. Så kan i de fallen ske utan den andra statens hjälp. En sådan möjlighet finns aldrig när det är fråga om annat än uppgifter som finns lagrade (eller kanske snarare manifesterade) på annat sätt än elektroniskt, t.ex. på papper. Eftersom det finns risk för att uppgifter av värde för en brottsutredning kan försvinna under den tid som det tar att utreda (om det alls är möjligt att utreda) var uppgifterna finns lagrade kan de beskrivna skillnaderna på mycket goda grunder utgöra en anledning att ifrågasätta om den svenska hållningen avseende territorialitetsprincipen vid frågor om exekutiv jurisdiktion alltid har skäl för sig när det gäller utredningar som tangerar ”det digitala rummet”. Som framgått har flera andra stater valt att använda sig av ett annat synsätt när det gäller hur territorialitetsprincipen ska tillämpas under dessa förhållanden.

Enligt vår uppfattning finns det ett principiellt och två mer praktiskt orienterade skäl till att tillämpa territorialitetsprincipen för exekutiv jurisdiktion på det sätt som nu sker i Sverige. Det principiella är att genom en sådan tillämpning uppstår en överensstäm-

melse mellan hur principen tillämpas i den fysiska och den digitala världen; två verkligheter som givetvis binds samman av att de elektroniska uppgifterna ju rent faktiskt lagras på servrar och skickas genom nät som existerar i den fysiska världen (dvs. inom och mellan staters faktiska territorier). Genom att använda samma princip för att bestämma vem eller vilka som har jurisdiktion uppnås således förutsebarhet. Det bör också tilläggas att den svenska hållningen är tämligen enkel att tillämpa. Genom att säga att så snart det föreligger osäkerhet så saknas jurisdiktion uppställer man ju krav på visshet avseende var uppgifterna lagras. Till detta principiella argument kommer alltså åtminstone två argument som får anses vara mer praktiskt orienterade.

För det första kan en ändrad svensk uppfattning om när exekutiv jurisdiktion ska anses föreligga leda till risk för konflikter med andra stater som tillämpar territorialitetsprincipen på annat sätt (t.ex. enligt nuvarande svensk hållning). Utan överenskommelser om vad som ska gälla mellan Sverige och andra stater kan det således tänkas att en annan stat anser att Sverige, om man enligt svensk inhemsk rätt tillåter brottsbekämpande myndigheter att från Sverige ta del av uppgifter som lagras i den andra staten, inkräktar på den andra statens suveränitet (genom att hämta uppgifter därifrån). För det andra torde en sådan inhämtning av uppgifter från en annan stat kunna innebära att det finns risk för att den som verkställer åtgärden gör sig skyldig till brott i den andra staten (t.ex. dataintrång). Detta problem ska dock inte överdrivas, utan är snarare ett närmast akademiskt påpekande. Det är svårt att på annat sätt förklara att det, såvitt utredningen känner till, inte uppstått någon sådan situation trots att flera stater alltså redan har lämnat den tolkning av territorialitetsprincipen som Sverige tillämpar.

Det finns enligt vår mening också väldigt goda skäl för ett annat synsätt än det nuvarande i frågan när Sverige ska anses ha jurisdiktion. Även här kan argumenten delas in i en principiell och en mer praktiskt orienterad kategori. Till de principiella argumenten hör att även en ändrad hållning skulle kunna vara förutsägbar, givet att den manifesteras tydligt. Det skulle således kunna bli lika enkelt (eller svårt) som i dag att veta när svensk jurisdiktion föreligger om bara de anknytningspunkter som används för att avgränsa jurisdiktionen är tydligt uttryckta. Som ett exempel kan nämnas att om den svenska hållningen innebar att när en brottsutredning bedrivs i

Sverige om ett brott begånget här och den misstänkte finns här i landet samt den tjänst där den misstänkte har sitt användarkonto är allmänt tillgängligt från Sverige så skulle den jurisdiktionsmässiga avgränsningen vara tämligen klar, och därmed också förutsägbar.

Såvitt avser de praktiska skälen för att förändra den svenska hållningen är det enligt vår mening starkaste argumentet att det, när en brottsutredning (eller ett underrättelseärende) pågår i Sverige och riktas mot en person som befinner sig här samt avser ett brott som begåtts (eller planeras) i riket, framstår som tämligen märkligt att svenska brottsbekämpande myndigheter inte ska kunna samla in elektroniskt lagrade uppgifter trots att de kan tillgängliggöras i Sverige utan att någon risk t.ex. för informationssäkerheten uppstår i den stat (eller i förekommande fall de stater) där uppgifterna lagras. Än mer märkligt blir detta med hänsyn till att lagringsplatsen i de allra flesta fall torde vara både irrelevant och okänd för den som äger eller disponerar informationen, och som alltså finns i Sverige, så länge hen kan få fram informationen på eget kommando. Med så många anknytningspunkter till en svensk utredning är det helt enkelt svårt att se varför lagringsplatsen i dessa fall ska avgöra den exekutiva jurisdiktionsfrågan. En jämförelse kan här göras med den danska högsta domstolens avgörande från 2012 där Højesteret nöjde sig med klart färre anknytningsfaktorer än de nu nämnda för att anse att dansk jurisdiktion förelåg.

Det faktum att artikel 32 i it-brottskonventionen tillåter en konventionspart att genom ett informationssystem inom sitt territorium samla in uppgifter som finns lagrade i annan stat när det finns frivilligt samtycke av den som äger/disponerar informationen talar enligt vår mening dessutom i viss mån för att användande av inloggningsuppgifter (som erhållits på lagligt vis) för att bereda sig tillgång till uppgifter på ett användarkonto på en internettjänst inte utgör en kränkning av den andra statens suveränitet, vilket har hävdats som en riskfaktor avseende mellanstatliga konflikter. Om det hade ansetts som en kränkning med inloggning från en annan stats brottsbekämpande myndigheter borde inte ett principiellt undantag från den hävdvunna tolkningen av territorialitetsprincipen alls kunnat ha accepterats av de 56 stater som ratificerat konventionen. Mot detta kan dock hållas att det kan ifrågasättas om inloggning med samtycke faktiskt utgör sådan myndighetsutövning som kan föranleda kränkningar.

Till det anförda kommer den omständigheten att en rad stater har infört unilaterala lösningar som innebär att inloggning från den egna staten med lagligen erhållna inloggningsuppgifter för inhämtning av uppgifter som lagras i en annan stat eller på okänd plats är tillåtet. Dessa lösningar synes, såvitt utredningen känner till, inte ha föranlett mellanstatliga konflikter vilket talar för en viss acceptans av förfarandet stater emellan. Det synes således föreligga ett, åtminstone tyst, accepterande av åtgärderna, vilket också kan tolkas som att inloggning inte utgör en kränkning av den andra statens suveränitet.

Det kan vidare framhållas att det inte heller bör vara särskilt svårt för Sverige att hitta en tolkning av territorialitetsprincipen som kan accepteras av oss själva även när andra stater gör samma tolkning beträffande uppgifter som lagras här (reciprocitet). Det kan därför rimligen på goda grunder antas att införande av motsvarande möjlighet i Sverige som införts i andra länder, under vissa givna förhållanden (så att det finns tillräckligt tydliga anknytningspunkter hit), inte skulle leda till några mellanstatliga konflikter. Dessutom får det anses oklart vad som är gällande rätt i sammanhanget eftersom det saknas bindande överenskommelser och territorialitetsprincipen uppenbarligen tillämpas olika i olika länder, något som också Europarådet pekat på. Som också nämnts innebär för övrigt artikel 32 i it-brottskonventionen varken ett tillåtande eller ett uteslutande av gränsöverskridande åtkomst till elektroniskt lagrade uppgifter i andra situationer än de som anges i artikeln.

Mot det anförda kan hållas att slutsatserna är behäftade med viss osäkerhet. Detta i synnerhet eftersom artikel 32 har varit föremål för internationella diskussioner under lång tid utan att någon enighet i frågan har kunnat uppnås. Alla världens länder är inte heller är anslutna till it-brottskonventionen. Dessutom är utgångspunkten för it-brottskonventionen att platsen för lagring fortfarande är den relevanta faktorn när rättslig hjälp ska begäras, se t.ex. art. 29 och 31. Att platsen för lagring är en relevant faktor även vid elektroniskt lagrade uppgifter framgår också i de rapporter som redovisats från såväl Europarådet som EU, där ju vikten av internationellt rättsligt samarbete understryks. Det talar i någon mening för att risken för mellanstatliga konflikter fortfarande kan vara aktuell om synsättet avseende jurisdiktion för elektroniskt lagrade uppgifter ändras allt för drastiskt. Att däremot förändra den svenska hållningen när det är fråga om t.ex. situationer då det inte är klarlagt eller inte helt kan

klarläggas var uppgifter lagras (loss of location) eller då det finns akut behov av att få del av information, t.ex. på grund av en nödsituation eller på grund av att uppgifterna annars kommer försvinna bör däremot inte öka risken för mellanstatliga konflikter nämnvärt. Det synes primärt vara i sådana situationer som det i andra stater finns möjligheter för brottsbekämpande myndigheter att ta del av elektroniskt lagrade uppgifter oberoende av var den lagras.

Som nämndes inledningsvis regleras inte frågan om jurisdiktion i svensk författning (vissa undantag finns dock i lagen om internationell rättslig hjälp i brottmål och den föreslagna lagen om europeisk utredningsorder). Trots de starka skäl som finns för att ändra den svenska tolkningen av territorialitetsprincipen vid exekutiv jurisdiktion framstår det inte som lämpligt att göra det lagstiftningsvägen inom ramen för denna utredning. Frågan bör i stället analyseras i särskild ordning och i ett sådant perspektiv att samtliga rättsområden som berörs av den beaktas.

Slutsatsen av vårt resonemang är således att det finns starka skäl att ändra den svenska tolkningen av territorialitetsprincipen för exekutiv jurisdiktion beträffande elektroniskt lagrade uppgifter men att något lagförslag inte bör lämnas. Konsekvensen av vår slutsats kan möjligen framstå som förvånande eftersom de förslag som vi fört fram i föregående kapitel, särskilt möjligheten att bereda sig tillgång till uppgifter på misstänktas användarkonton, många gånger kan förväntas bli svåra att tillämpa utan en tydligt ändrad svensk hållning. De stora tjänsteföretagen är ju oftast globala aktörer som lagrar uppgifter i andra stater än i Sverige. Till det kommer att företagen i många fall inte själva känner till var specifika uppgifter lagras. Om den svenska hållningen förblir oförändrad blir givetvis effektiviteten av hemlig dataavläsning, när åtgärden ska användas beträffande uppgifter på sådana konton, begränsad i förhållande till vad som skulle gälla om andra mer tillåtande jurisdiktionsregler gällde.

Vårt ställningstagande att inte föreslå någon lagändring hindrar dock inte att svensk jurisdiktion kan anses finnas i exempelvis situationer då loss of location föreligger. Som vårt förslag om hemlig dataavläsning är utformat ska domstolsprövning alltid ske av frågan om hemlig dataavläsning ska tillåtas. I domstolsprövningen ligger implicit att också pröva frågor om jurisdiktion. Frågan om en ändrad hållning avseende territorialitetsprincipen kan således prövas av domstol i samband med tillståndsprövningen, likt det som skedde i

Danmark 2012 (se avsnitt 11.3.4). Det finns enligt vår mening goda skäl för åklagare att söka få prövat var gränserna för territorialitetsprincipen går i samband med ansökningar om hemlig dataavläsning när åtgärden ska avse användarkonton till internetbaserade tjänster. Utifrån bl.a. de för- respektive nackdelar med en ändrad svensk hållning som vi påtalat ovan finns således möjlighet för de högre domstolarna att ta ställning till om den gällande ordningen för exekutiv jurisdiktion har skäl för sig även vid hemlig dataavläsning i nu aktuellt avseende.

Avslutningsvis bör framhållas att Sverige parallellt med eventuella domstolsprövningar av exekutiv jurisdiktion bör gå i fronten för internationella överenskommelser. Som nämnts föreligger det med unilaterala lösningar vissa risker för mellanstatliga konflikter. Genom internationella överenskommelser kan sådana risker minskas. Den svenska utgångspunkten vid förhandlingar om sådana överenskommelser bör enligt vår mening vara att verka för att territorialitetsprincipen bättre anpassas till nutida förhållanden, särskilt såvitt avser det digitala rummet. Ett första steg för Sverige att ta bör vara att ratificera it-brottskonventionen för att alls få delta i de samtal och diskussioner som nu förs i Europarådet.

12 Konsekvenser och genomförande

12.1 Konsekvenser

Utredningens bedömning: 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 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 nuvarande anslag inte förslår. Ramhöjningen bör finansieras genom omfördelningar inom rättsväsendets anslag, utgiftsområde 4.

De kostnadsökningar som kan förväntas för andra myndigheter inom rättsväsendet och för offentliga ombud bedöms rymmas inom befintliga anslag.

12.1.1 Inledning

Utredningen ska enligt direktiven bedöma de ekonomiska konsekvenserna av förslagen för staten, kommuner och landsting och konsekvenserna i övrigt av förslagen. Om förslagen förväntas leda till kostnadsökningar för staten, kommuner och landsting, ska utredaren föreslå hur dessa ska finansieras. Enligt 15 § kommittéförordningen gäller också att om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, brottsligheten och det brottsförebyggande arbetet, 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 ska konsekvenserna i respektive avseende anges i betänkandet.

Ingenting i vår kartläggning talar för att några ekonomiska konsekvenser för kommuner eller landsting kommer att uppstå till följd av våra förslag. Inte heller kan vi se att förslagen har betydelse för 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.

I kapitel 9 har vi redovisat de grundläggande avvägningar vi gjort. Där redovisas bl.a. vilken betydelse våra förslag kan få för brottsligheten och det brottsförebyggande arbetet. Det som har anförts där motsvarar även i övrigt det som ska finnas med i en kommittés konsekvensutredning, se 6 § förordningen om konsekvensutredning vid regelgivning. Det saknas skäl att upprepa vad som anförts där utan det är tillräckligt med en hänvisning dit. I detta kapitel redovisas därför endast de ekonomiska konsekvenserna av förslagen närmare.

12.1.2 Ekonomiska konsekvenser av förslaget om hemlig dataavläsning

Ökade kostnader för brottsbekämpande myndigheter som ska verkställa hemlig dataavläsning

Utredningen har under hela utredningstiden mötts av synpunkten att hemlig dataavläsning kommer att vara ett verktyg för de brottsbekämpande myndigheterna som är förenat med betydande kostnader. Detta har framhållits såväl av de brottsbekämpande myndigheterna i Sverige som vid studiebesök hos brottsbekämpande myndigheter i andra länder där åtgärden, eller motsvarigheter till den finns.

Det primära skälet till att hemlig dataavläsning är dyrt jämfört med andra hemliga tvångsmedel är den teknik som används i samband med verkställighet av åtgärden. Det bör framhållas att när vi här talar om teknik i samband med verkställighet så avser vi främst tekniska metoder för att bereda sig tillträde till informationssystem och den programvara som kan placeras i informationssystem för att möjliggöra och genomföra verkställigheten. Hemlig dataavläsning kan också verkställas t.ex. efter att den brottsbekämpande myndigheten, från t.ex. datorer som finns i den brottsbekämpande myndighetens lokaler, har loggat in på den misstänktes användarkonto till en kommunikationstjänst. I de fallen torde kostnaden för hemlig dataavläsning i praktiken inte vara större än kostnaden för personal som genomför inloggningen. Det är också möjligt att med hårdvaruhjälpmedel genomföra hemlig dataavläsning, t.ex. genom att fästa hårdvara som registrerar tangentnedslagningar på ett tangentbord. Inte heller i de fallen torde det uppstå några större kostnader, i praktiken endast kostnaden för det tekniska hjälpmedlet och personalkostnaden för den som ska placera detta.

Det finns i praktiken två alternativa vägar för att anskaffa den teknik som behövs för verkställighet av hemlig dataavläsning, antingen inköp från privata leverantörer eller egenutveckling (se fördjupning beträffande de två alternativen i avsnitt 8.4.2). Utredningen har inte funnit skäl att reglera hur de brottsbekämpande myndigheterna ska anskaffa den teknik som behövs utan anser att det är en fråga som bör lämnas till dem själva. Mot bakgrund av uppgifterna om att tekniken för hemlig dataavläsning är dyr, oavsett anskaffningsmetod, har utredningen begärt in uppgifter från de brottsbekämpande myndigheterna beträffande vilken storleksordning av kostnader det rör sig

om. En undersökning gjord av utredningen på egen hand eller på annat sätt har nämligen bedömts som helt utsiktslös mot bakgrund av att det endast är de brottsbekämpande myndigheterna som har kunskaper om vilken teknik som kan behövas och vilka medel som krävs för att få tillgång till sådan.

Av samhällsekonomiska skäl anser de brottsbekämpande myndigheterna som ska kunna verkställa hemlig dataavläsning att det bör ske någon form av samordning mellan myndigheterna avseende verkställighet av hemlig dataavläsning. De uppgifter om kostnader som utredningen tagit del av och som redovisas i det följande avser därför dessa myndigheters gemensamma kostnader.

Den ökade kostnaden för de brottsbekämpande myndigheterna som ska verkställa hemlig dataavläsning om metoden införs har beräknats till cirka 100 miljoner kronor årligen. I kostnadsökningen innefattas nyrekrytering, utbildning, kompetensutveckling, anskaffning av teknisk utrustning, drift och underhåll samt kostnader för medverkande operatörer. Däremot innefattas inte 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. Kostnaderna för de resurser som inte innefattas i den nämnda summan har bedömts rymmas inom befintliga resurser efter omdispositioner.

Den enskilt största posten som tillkommer med hemlig dataavläsning avser inköp av nödvändig teknisk utrustning. Även kostnaden för personal som kommer bli nödvändig att rekrytera, vilken till stor del kommer att utgöras av personer med specialistkompetens, är en stor post.

De redovisade kostnaderna har beräknats utifrån en uppskattad kapacitet på cirka 20–30 samtidiga installationer, vilket är vad som bedömts rimligt. Detta har förklarats enligt följande. Verkställighet av hemlig dataavläsning mot en person kan, men behöver inte, medföra flera installationer och komplexiteten i varje enskild installation kan variera. Vissa installationer kan genomföras med relativt kort förberedelse och med en relativt enkel installation medan andra kräver en mer komplex installation och med en mer omfattande kartläggning av både person och det informationssystem som tillståndet avser.

Utredningen saknar reell möjlighet att ifrågasätta de lämnade uppgifterna såvitt avser de enskilda kostnaderna som framhållits. De ökade kostnaderna för myndigheterna som ska verkställa åtgärden blir under alla förhållanden betydande utifrån de uppgifter som redovisats.

Enligt 15 § kommittéförordningen ska utredningen föreslå finansiering om förslaget förväntas leda till ökade kostnader. Som redovisats finns det mycket som talar för att kostnaderna för de brottsbekämpande myndigheterna kommer att öka. De brottsbekämpande myndigheterna samverkar redan i dag, bl.a. avseende infrastrukturella lösningar, vid användning av hemliga tvångsmedel. Inom ramen för detta samarbete, som finns till bl.a. för att samma kostnader inte ska uppstå på mer än ett ställe, delas kostnader mellan myndigheterna enligt vissa kostnadsfördelningsmodeller. Ur ett kostnadseffektivitetsperspektiv torde motsvarande lösning vara att föredra även för hemlig dataavläsning. Frågor om detta diskuteras, för det fall att hemlig dataavläsning införs, mellan de myndigheter som ingår i nuvarande samarbete. Mot den bakgrunden är det svårt att nu ange hur stora kostnadsökningar som faktiskt kommer bli fallet för respektive brottsbekämpande myndighet och således också hur de ökade kostnaderna bör fördelas.

I regeringens budgetproposition för 2018 framgår att det samlade anslaget för Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket uppgår till drygt 28 miljarder kronor år 2018. De kostnadsökningar som hemlig dataavläsning medför bör, efter fördelning mellan myndigheterna, rymmas inom de befintliga anslagen. I vart fall bör finansiering kunna ske genom omfördelning av befintliga anslag inom de utgiftsområden som träffas. När det gäller anskaffning av nödvändig teknisk utrustning torde det huvudsakligen vara fråga om anläggningstillgångar som finansieras genom lån i Riksgälden (se 2 kap. 1 § kapitalförsörjningsförordningen). Beroende på hur stora investeringar som behövs kan låneramen för den eller de myndigheter som ska uppta lån behöva ökas.

Ökade kostnader för Säkerhets- och integritetsskyddsnämnden

Vi har inte några riktade förslag beträffande Säkerhets- och integritetsskyddsnämnden utöver att den ska underrättas om tillståndsbeslut av domstolar, se 29 § i förslaget till lag om hemlig dataavläsning. Den åtgärden kommer, såvitt vi kan bedöma, i sig inte att innebära några beaktansvärda ekonomiska konsekvenser för nämnden med hänsyn till det begränsade antal tillstånd som kommer att meddelas årligen. Däremot kommer, som framhållits i avsnitt 10.12.1, den tillsyn som ska utövas beträffande hemlig dataavläsning i vart fall i två avseenden sannolikt behöva avvika från hur tillsynen bedrivs i dag.

Det första är att tillsyn avseende hemlig dataavläsning kommer att kräva en annan teknisk kompetens än vad tillsynen avseende de nu gällande hemliga tvångsmedlen fordrar. Det hänger samman dels med metodens i sig tekniska karaktär och de åtgärder som vidtas i samband med verkställighet, dels de skyddsmekanismer för den personliga integriteten och informationssäkerheten som vi föreslagit i 19 och 20 §§ lagen om hemlig dataavläsning. För att i praktiken kunna kontrollera regelefterlevnaden av många av de bestämmelser vi föreslagit kommer det således ställas höga krav på t.ex. förståelse för teknik och informationssäkerhet. Såvitt framkommit finns sådan kompetens som torde krävas inte vid Säkerhets- och integritetsskyddsnämnden i dag.

Den andra omständigheten som kan komma att skilja sig från hur tillsynen utövas i dag är att tillsynen torde behöva vara mer aktiv, med vilket avses att tillsynen kan behöva utövas under pågående verkställighet. Skälen till det har presenterats i avsnitt 10.12.1 och hänger främst samman med den risk för misstro och ryktesspridning som kan uppstå om det inte sker en effektiv och aktiv tillsyn av hemlig dataavläsning med hänsyn till de risker för integritet och informationssäkerhet som åtgärden kan medföra.

När det gäller vilka ekonomiska konsekvenser dessa skillnader i tillsyn kan innebära gör vi följande bedömning. Nämnden kommer att behöva rekrytera personal med teknisk kompetens. Hemlig dataavläsning kommer att aktualiseras vid ett begränsat antal tillfällen årligen men med hänsyn till vikten av en aktiv och effektiv tillsyn av åtgärden bör, åtminstone till en början, i vart fall en ytterligare årsarbetskraft beräknas jämfört med vad som används i dag.

Enligt nämndens årsredovisning för 2016 var det vid utgången av det året 14 personer i tjänst på nämndens kansli. En årsarbetskraft beräknad som ett genomsnitt av kostnaderna för personal för 2016 motsvarar cirka 800 000 kronor. På nämndens kansli tjänstgör personer på olika ansvarsnivåer och därmed också med olika lönenivåer. Personer med den tekniska komptens som kommer att behövas beräknas kosta mer än en genomsnittsårsarbetskraft. Kostnadsökningen för den extra årsarbetskraften vi bedömer nödvändig för Säkerhets- och integritetsskyddsnämnden bör därför beräknas till 1 500 000 kronor, i vilken kostnad även kringkostnader som utbildning och resor bör rymmas. Rimligen bör en mindre del av det befintliga anslaget till nämnden kunna möta de ökade kostnaderna. Till den del anslaget inte förslår bör det höjas. Ramhöjningen bör dock kunna finansieras genom omfördelningar inom rättsväsendets anslag, utgiftsområde 4.

Ökade kostnader för Sveriges domstolar, Åklagarmyndigheten och offentliga ombud

Varje ärende om hemlig dataavläsning ska enligt vårt förslag domstolsprövas. Så ska som utgångspunkt ske efter ansökan av åklagare. Rätten ska alltid hålla sammanträde vid vilket ett offentligt ombud ska närvara. Vi bedömer dock att det kommer att bli fråga om ett begränsat antal verkställighetstillfällen per år och dessutom att dessa i flertalet fall kommer att ersätta ansökningar om andra hemliga tvångsmedel. Det talar för att kostnaderna för Sveriges domstolar inte bör öka i sådan utsträckning att de inte ryms inom befintliga anslag. Samma sak gäller beträffande kostnaderna för offentliga ombud och Åklagarmyndigheten.

Det kan också förutses att domstolar, offentliga ombud och åklagare kommer att behöva fortbilda sig beträffande det nya tvångsmedlet. Kostnaden för sådan fortbildning kan dock inte förväntas bli större än att det ryms inom befintliga anslag.

Det blir inga ökade kostnader för företag som biträder de brottsbekämpande myndigheterna vid verkställighet

Vi inför en uttrycklig möjlighet för aktörer som bedriver anmälningspliktigverksamhet enligt 2 kap. 1 §, dvs. i praktiken företag som tillhandahåller allmänna kommunikationsnät mot ersättning och eller allmänt tillgängliga elektroniska kommunikationstjänster, att medverka vid hemlig dataavläsning. De aktörer som biträder en brottsbekämpande myndighet ska enligt den bestämmelsen 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 varför kostnadsökningar för dessa inte bedöms uppstå. Kostnaderna för medverkan belastar i stället den brottsbekämpande myndighet som får hjälp av operatören. Dessa kostnader ingår i den kostnadsökning som nämnts ovan beträffande de brottsbekämpande myndigheterna.

12.2 Ikraftträdande m.m.

Utredningens förslag: Lagen om hemlig dataavläsning ska träda i kraft den 1 januari 2019 och tidsbegränsas att gälla till och med den 31 december 2023. Övriga lagändringar ska träda i kraft den 1 januari 2019.

Utredningens bedömning: Det finns inte behov av några särskilda övergångsbestämmelser.

Den föreslagna lagen om hemlig dataavläsning bör träda i kraft så snart som möjligt. Vår bedömning är att det med hänsyn till remissförfarande och övriga beredningsåtgärder inte är möjligt att låta de nya bestämmelserna träda i kraft förrän den 1 januari 2019. Av de skäl som anförts i anförts i avsnitt 10.1.2 bör författningen tidsbegränsas att gälla till och med den 31 december 2023. Övriga lagändringar, vilka är följder av att hemlig dataavläsning införs som tvångsmedel, bör också träda i kraft den 1 januari 2019.

När det gäller processrättslig lagstiftning är utgångspunkten att nya regler ska tillämpas genast efter ikraftträdandet. Det innebär att nya regler ska tillämpas på varje processuell företeelse som inträffar

efter det att regleringen har trätt i kraft. Det medför att de brottsbekämpande myndigheterna och domstolarna ska tillämpa de nya bestämmelserna även i förundersökningar och tvångsmedelsärenden som har inletts innan de föreslagna bestämmelserna träder i kraft. En sådan ordning är enligt vår bedömning lämplig avseende de av utredningen föreslagna ändringarna. Det finns därför inte behov av några särskilda övergångsbestämmelser.

13 Författningskommentar

13.1 Förslaget till lag (2019:000) om hemlig dataavläsning

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.

Paragrafen innehåller en definition av det nya tvångsmedlet hemlig dataavläsning och en definition av det för lagen centrala begreppet informationssystem. Övervägandena i avsnitt 10.2.

I paragrafens *första stycke* finns en legaldefinition av hemlig dataavläsning. Den knyter an till bestämmelsen om dataintrång i 4 kap. 9 c § brottsbalken genom att de uppgifter som får läsas av eller tas upp in är *uppgifter avsedda för automatiserad behandling*. Begreppet ska tolkas på samma sätt som enligt bestämmelsen i brottsbalken. Alla sorters uppgifter, dvs. fakta, information eller begrepp, som uttrycks i en för en dator anpassad och läsbar form kan således omfattas av bestämmelsen. För den vidare innebörden av begreppet uppgifter som är avsedda för automatiserad behandling hänvisas till prop. 2006/07:66 s. 49.

Av bestämmelsen framgår vidare att hemlig dataavläsning utförs genom *avläsning eller upptagning.* Avläsning är avsett att vara ett neutralt begrepp som kan ta sikte både på en helt teknisk process,

utförd av en dator eller annat tekniskt hjälpmedel, för att exempelvis göra informationen läsbar och på den process som sker när den som ska granska uppgifterna tar del av informationsinnehållet. Begreppet upptagning anges för att tydliggöra att även om avläsning inte sker i realtid så får uppgifterna tas upp för att sedan granskas i efterhand. I andra hemliga tvångsmedelsbestämmelser används ibland begreppet inhämtning. Det är också vad det är fråga om enligt förevarande bestämmelse och det begreppet ryms i begreppen avläsning och upptagning.

Avläsningen ska avse uppgifter, avsedda för automatiserad behandling *i ett informationssystem*. Uttrycket klargör att uppgifterna ska kunna härledas till det informationssystem tillståndet till hemlig dataavläsning avser. Avläsningen får ske i informationssystemet, jfr prop. 1994/95:227 s. 25, men definitionen uppställer inget krav på det. Däremot ska alltså uppgifterna som läses av eller tas upp finnas i eller ha funnits i informationssystemet.

Eftersom det är fråga om ett hemligt tvångsmedel anges också i bestämmelsen att åtgärden ska ske *i hemlighet*. Hemlighållandet tar sikte på kännedomen om åtgärden hos den vars uppgifter läses av eller tas upp. Därtill kommer att åtgärden ska genomföras med ett *tekniskt hjälpmedel*. Begreppet avser, liksom i övrigt i tvångsmedelssammanhang, såväl hårdvara som programvara, se prop. 1994/95:227 s. 29. Således kan hemlig dataavläsning exempelvis ske sedan hårdvara som kan snappa upp lösenord fästs på informationssystemet eller efter att programvara som kan fånga upp meddelanden installerats i informationssystemet. Kravet på tekniskt hjälpmedel innebär emellertid inte att någonting måste installeras i eller fästas på viss fysisk utrustning. Eftersom begreppet informationssystem också omfattar virtuella tjänster, se nedan, kan hemlig dataavläsning också genomföras genom att den som verkställer åtgärden använder sin dator, som ju är ett tekniskt hjälpmedel, för att logga in på en misstänkts användarkonto till exempelvis en internetbaserad kommunikationstjänst. Kravet på att tekniskt hjälpmedel ska användas riktar sig mot den brottsbekämpande myndigheten. Det är alltså denna som ska ha kontrollen över det tekniska hjälpmedlet. Det innebär att det inte är fråga om hemlig dataavläsning när en polisman vid spaning mot en person ser vilket lösenord denne knappar in på sin mobiltelefon eller kan läsa ett meddelande som mottas i telefonen.

Ett centralt begrepp i bestämmelsen och i lagen är *informationssystem*, vilket har valts för att klargöra att det inte endast är uppgifter i fysisk utrustning som hemlig dataavläsning får avse. I andra stycket anges uttömmande vad som menas med informationssystem enligt lagen. Det följer av att det anges att informationssystem kan vara *antingen* det som anges i första punkten *eller* det som anges i andra punkten.

Den *första punkten* i andra stycket slår fast att *elektronisk kommunikationsutrustning* är informationssystem i lagens mening. Begreppet ska ha samma innebörd som det har när det används på andra ställen i tvångsmedelssammanhang, t.ex. i 23 kap. 9 a § och 27 kap. 19 § rättegångsbalken och 1 § lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen), se t.ex. prop. 2015/16:68 s. 74. Det innebär att elektronisk kommunikationsutrustning innefattar all slags utrustning som kan användas för att kommunicera elektroniskt, t.ex. datorer, mobiltelefoner, servrar och liknande utrustning. Utrustning som är fysiskt sammankopplad med elektronisk kommunikationsutrustning, t.ex. sladdar, tangentbord, USB-minnen eller en datormus, kan innefattas i begreppet. Att en dator genom en sladd är uppkopplad mot ett nätverk innebär emellertid givetvis inte att hela nätverket och all den utrustning som är anslutet till det utgör det informationssystem som får läsas av. Avgränsningen av vilken utrustning som ska anses omfattas av tillståndet får göras utifrån vad som framstår som rimligt med hänsyn till det identifierade informationssystem som anges i tillståndet.

När det gäller andra styckets *andra punkt* är det fråga om informationssystem som avgränsas på annat sätt än fysiskt. Som exempel nämns i lagtexten kommunikationstjänster, lagringstjänster eller liknande tjänster. 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 den fysiska lagringsplatsen för uppgifterna är. Begreppet *kommunikationstjänst* har en vidare innebörd än begreppet elektronisk kommunikationstjänst i 1 kap. 7 § lagen om elektronisk kommunikation, jfr prop. 2002/03:110 s. 358 ff. och Post- och telestyrelsens rapport PTS-ER-2009:12. Det innebär att såväl sådana elektroniska kommunikationstjänster som avses enligt den angivna bestämmelsen som andra kommunikationstjänster, t.ex. internet-

baserade meddelandetjänster omfattas. Med begreppet *lagringstjänst* avses här i allmänhet tjänster som innebär att enskilda kan lagra uppgifter elektroniskt på annat utrymme (och på annan geografisk plats) än i den egna fysiska utrustningen, s.k. molntjänster. Med *liknande tjänster* avses exempelvis internetbaserade innehållstjänster vars primära syfte inte är kommunikation eller lagring men som innefattar möjlighet till endera av dessa. Så kan exempelvis vara fallet i speltjänster eller bokningstjänster.

Av begränsningen som görs i inledningen av den andra punkten i andra stycket följer att det i de fallen inte är hela tjänsten som avses. Det anges i bestämmelsen genom uttrycket *ett användarkonto till, eller en på motsvarande sätt avgränsad del av*, tjänsten. Det innebär således att begreppet informationssystem i de fallen avser bara en enskild persons utrymme i tjänsten, dvs. den enskildes virtuellt begränsade yta i tjänsten. För att uppnå viss möjlighet att möta teknikutvecklingen anges inte bara användarkonto utan också en på motsvarande sätt avgränsad del av tjänsten.

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.

Paragrafen anger vilka typer av uppgifter som får läsas av eller tas upp med hemlig dataavläsning och att vissa åtgärder får vidtas. Övervägandena finns i avsnitt 10.3.

I paragrafens *första stycke* slås först fast att hemlig dataavläsning inte får användas i andra situationer än när tillstånd har meddelats enligt lagen. Det innebär att den teknik som används för hemlig dataavläsning inte kan användas för att verkställa andra hemliga tvångsmedel, jfr 27 kap. 25 § rättegångsbalken.

I första stycket anges vidare, och uttömmande, de olika uppgiftstyper som hemlig dataavläsning *får användas* för att läsa av eller ta upp. Med *uppgifter* i första styckets ingress avses uppgifter avsedda för automatiserad behandling, se kommentaren till 1 §. Att det är fråga om olika uppgiftstyper får betydelse för lagens fortsatta struktur. I förevarande bestämmelse regleras endast vilka uppgifter hemlig dataavläsning alls kan få användas för att läsa av eller ta upp. Vilka uppgifter som ett tillstånd sedan faktiskt avser i ett enskilt fall bestäms utifrån ändamålet med åtgärden. Exempelvis får uppgifter enligt första styckets femte punkt endast läsas av om ändamålet är brottsutredande verksamhet. Den punkten aktualiseras således aldrig i underrättelseverksamhet. Genom att punkterna i första stycket knyts samman av ordet *eller* ska klargöras att samtliga uppgiftstyper inte alltid får läsas av eller tas upp när ett tillstånd till hemlig dataavläsning har meddelats.

Av *första styckets fem första punkter* framgår att hemlig dataavläsning får användas för att läsa av eller ta upp uppgifter som får hämtas in genom gällande hemliga tvångsmedel. Detta framgår eftersom det är samma definitioner av uppgifterna som får läsas av eller tas upp som anges i definitionerna av vilka uppgifter som de ”bakomliggande” hemliga tvångsmedlen får användas för att hämta in. *Punkt 1* klargör således att det är samma uppgifter som får hämtas in genom hemlig avlyssning av elektronisk kommunikation (enligt 27 kap. 18 § rättegångsbalken), som får läsas av eller tas upp när punkten aktualiseras. *Punkt 2* klargör att det är samma uppgifter som får hämtas in antingen med hemlig övervakning av elektronisk kommunikation (enligt 27 kap. 19 § första stycket 1 rättegångsbalken)

eller genom inhämtning enligt inhämtningslagen (enligt 1 § 1 den lagen, som dock endast avser historiska uppgifter, se vidare i kommentaren till 10 § andra stycket). *Punkt 3* klargör att sådana lokaliseringsuppgifter som får hämtas in genom hemlig övervakning av elektronisk kommunikation (enligt 27 kap. 19 § första stycket 3 rättegångsbalken) och vid inhämtning enligt inhämtningslagen (se 1 § 3 den lagen) får läsas av eller tas upp när punkten aktualiseras. Motsvarande möjlighet som enligt de bestämmelserna finns att hämta in uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt utrymme finns dock inte, se vidare i avsnitt 10.3.1. *Punkt 4* klargör att det är uppgifter som får hämtas in genom hemlig kameraövervakning (se 27 kap. 20 a § rättegångsbalken) som får läsas av eller tas upp när punkten aktualiseras. *Punkt 5* klargör att det är uppgifter som får hämtas in genom hemlig rumsavlyssning (se 27 kap. 20 d § rättegångsbalken) som får läsas av eller tas upp när punkten aktualiseras.

Möjlighet till hemlig inhämtning av uppgifter som anges i *sjätte och sjunde punkterna* finns i praktiken inte i dag. *Punkt 6* möjliggör avläsning eller upptagning av uppgifter som *finns lagrade i ett informationssystem*. Det saknar således betydelse hur uppgifterna lagrats, dvs. om det skett genom en medveten handling av en person eller om de lagrats till följd av en inställning i informationssystemet utan att användaren känner till detta. Det saknar också betydelse om uppgifterna är varaktigt eller temporärt lagrade. Vidare saknar det betydelse vilket format uppgifterna lagrats i. Det centrala enligt punkten är att uppgifterna finns lagrade i informationssystemet när avläsningen eller upptagningen genomförs. Uppgifter som avses kan exempelvis vara datafiler, såsom text-, bild- och ljudfiler men också program- eller systemfiler som innehåller information av värde för det ändamål som föranlett åtgärden. Eftersom begreppet informationssystem innefattar utrustning som anslutits till ett informationssystem kan även uppgifter som finns lagrade på ett externt lagringsmedium som kopplats in i en dator läsas av eller tas upp enligt punkten. När det är fråga om uppgifter som är lagrade i ett informationssystem som avses i 1 § andra stycket 2, t.ex. på ett användarkonto för en internetbaserad lagringstjänst anses uppgifterna lagrade i informationssystemet om de kan tillgängliggöras med det (se dock diskussion om jurisdiktion i avsnitt 11.3.5).

Det är vidare ett krav enligt punkten att de uppgifter som läses av eller tas upp *inte avses i punkterna 1–5*. Detta krav gäller för att avgränsa de uppgifter som avses i punkt 6 från övriga punkter och, i förlängningen, för att anpassning av verkställighetstekniken på sätt som lagen föreskriver ska kunna ske, se 19 § och kommentaren till den bestämmelsen. En del av de uppgifter som lagras i informationssystem torde vara sådana som kan samlas in genom användning av andra hemliga tvångsmedel. Uppgifterna får då inte läsas av eller tas upp med stöd av punkten, utan tillståndet ska då i stället avse den av de föregående punkterna som uppgifterna hänför sig till. Genom kravet säkerställs att behovet av information, dvs. vilka uppgifter det finns behov av att samla in, i det enskilda fallet blir avgörande för vad ansökan om tillstånd omfattar. 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 punkten 2 och innehåll i meddelanden som kan hämtas in enligt punkten 1. Det kan tänkas att kravet kan ge upphov till gränsdragningsfrågor. Eftersom det emellertid kommer att vara möjligt att meddela tillstånd till hemlig dataavläsning avseende fler än en av punkterna samtidigt, se kommentaren till 3 §, ska risken för överlappning mellan punkterna och svåra gränsdragningar inte överdrivas. Sådana frågor får hanteras vid tillämpningen.

Enligt *punkt 7* får uppgifter som *visar hur ett informationssystem används* läsas av eller tas upp. Vad som avses är själva användandet av informationssystemet. Det kan exempelvis handla om användning som inte leder till att information lagras men som bedöms vara av intresse för det ändamål som föranlett åtgärden. Med detta avses realtidsuppgifter om vad en användare av ett informationssystem utnyttjar detta för. Det blir således fråga om realtidsövervakning av själva informationssystemet. Exempel på uppgifter som avses kan vara vilka program eller appar som körs, anteckningar som görs som inte sparas och hur informationssystemet i andra avseenden används. Genom tillägget i punkten, *inte avses i 1–6*, klargörs att det är sådana uppgifter som här exemplifierats, och således inte allt som visar hur informationssystemet används, som avses.

I bestämmelsens *andra stycke* ges den brottsbekämpande myndigheten som verkställer en åtgärd som avses i någon av punkterna 1 eller 2 möjlighet att *hindra meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts från att nå fram.* Detta är

motsvarande möjlighet som finns vid hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § andra stycket rättegångsbalken och ska tillämpas på samma sätt som enligt den bestämmelsen. 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.

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.

I bestämmelsen lagfästs proportionalitetsprincipen. Övervägandena finns i avsnitt 10.4.

Proportionalitetsprincipen brukar i korthet beskrivas på det sättet att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden. Bestämmelsen innebär en skyldighet för rätten, och i förekommande fall för åklagaren, att alltid beakta proportionalitetsprincipen när en begäran om hemlig dataavläsning prövas. Den får betydelse också för hur ett tillstånd ska utformas och vilka villkor som ska förenas med det.

Bestämmelsen får särskild betydelse när ansökan avser mer än en typ av uppgift enligt 2 § eftersom intrånget i den personliga integriteten typiskt sett blir större ju mer omfattande åtgärden tillåts vara. Även frågor om risker för informationssäkerhet och företagshemligheter får betydelse vid den prövning av åtgärdens proportionalitet som ska göras. Exempelvis bör rätten vid bedömningen väga in om det finns risk för att den brottsbekämpande myndigheten kan få del av uppgifter som helt saknar betydelse för det ärende åtgärden gäller. Annat som bör vägas in är om aktuella uppgifter förväntas vara av särskilt känslig karaktär. I så fall kan rätten begränsa tillståndet att avse endast vissa uppgifter, se 13 § sista stycket.

Också när det är fråga om att läsa av eller ta upp uppgifter från informationssystem som används av någon som inte är misstänkt för brott finns anledning att vara restriktiv i tillståndsgivningen. I de materiella bestämmelserna tas viss särskild hänsyn till integritets- och informationssäkerhetsrisker för de personer som här avses men det bör understrykas att det redan med en strikt tillämpning av proportionalitetsprincipen endast i undantagsfall bör komma i fråga att använda hemlig dataavläsning mot sådana personer. Undantagsfall bör föreligga när det handlar om mycket allvarlig brottslighet såsom terroristbrottslighet och annan systemhotande brottslighet, både i förundersöknings- och underrättelseverksamhet. Med misstänkt bör dock i detta sammanhang jämställas person som avses i 6 § första stycket och 8 § första stycket 1 även om det i de fallen inte pågår en förundersökning.

Proportionalitetsprincipen gäller under hela verkställigheten och ska alltså, även sedan tillstånd getts, beaktas självmant och löpande av de brottsbekämpande myndigheterna. Man kan tänka sig situationer där integritetsintrånget under verkställigheten blir så stort att avläsningen måste avbrytas, trots att åtgärden fortfarande skulle ha betydelse för utredningen.

Hemlig dataavläsning under en förundersökning

4 §

Hemlig dataavläsning får, om inte annat anges i andra eller tredje styckena, 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.

I paragrafen ges grundläggande bestämmelser om vad som ska gälla för tillståndsgivningen till hemlig dataavläsning under förundersökning. Övervägandena beträffande första och tredje styckena finns i avsnitt 10.5.1–10.5.4 och beträffande andra stycket i avsnitt 10.5.5.

Första stycket

I *första stycket* slås huvudregeln fast för vad som ska gälla för tillstånd till hemlig dataavläsning under förundersökning. Lagstiftningstekniken, att slå fast huvudregeln i bestämmelsens första stycke och sedan ange undantag från denna i de efterföljande styckena, återkommer i flera av lagens paragrafer.

En första förutsättning för hemlig dataavläsning enligt bestämmelsen är att det pågår en förundersökning. Detta är samma krav som gäller enligt samtliga bestämmelser om hemliga tvångsmedel i rättegångsbalken. Bestämmelsen ska i den delen inte ha någon annan innebörd än de bestämmelserna. Förundersökningen ska, beträffande alla uppgiftstyper utom för avläsning eller upptagning av rumsavlyssningsuppgifter enligt 2 § första stycket 5, *avse brott som anges i 27 kap. 18 § rättegångsbalken*. De brotten är följande.

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 enligt första eller andra punkten om en sådan gärning är belagd med straff.

4. Annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

Hemlig dataavläsning får således aldrig tillåtas för att utreda något annat brott än de angivna. Det innebär att det ställs högre krav för att meddela tillstånd till hemlig dataavläsning avseende uppgifter som annars skulle kunna hämtas in med hemlig övervakning av elektronisk kommunikation än vad som krävs för tillstånd till det tvångsmedlet.

Enligt huvudregeln ska det finnas en *skäligen misstänkt* för att hemlig dataavläsning ska få vidtas. Det är samma nivå på misstankegraden som gäller för övriga gällande hemliga tvångsmedel. Skälig misstanke är en lägre misstankegrad än sannolika skäl, vilket krävs för häktning som huvudregel, men en högre misstankegrad än ”kan misstänkas” (se t.ex. 23 kap. 9 § rättegångsbalken). För att hemlig dataavläsning ska få användas under förundersökning krävs att den person som är föremål för åtgärden är skäligen misstänkt för ett konkret brott. I doktrinen har uttalats att begreppet skälig misstanke är jämförbart med uttrycket ”antagligt” (se Ekelöf m.fl., *Rättegång, femte häftet*, 8 uppl., 2011, s. 117). Det är inte möjligt att med någon större precision ange det beviskrav som ligger i att någon är ”skäligen misstänkt” utan frågan måste bedömas efter omständigheterna i det enskilda fallet. Prövningen av styrkan i misstankarna måste grunda sig på en objektiv och allsidig bedömning av utredningsmaterialet. JO har vid ett flertal tillfällen uttryckt saken på så sätt att det krävs att det finns konkreta omständigheter av viss styrka som pekar på att den misstänkte har begått brottet. Detta innebär att brottsmisstanken måste vara konkret grundad och att ett beslut om tvångsmedel aldrig kan grunda sig enbart på allmänna kunskaper om en persons livsföring eller hans eller hennes tidigare brottslighet.

Det krävs också att åtgärden är av *synnerlig vikt för utredningen*. Även detta krav gäller för övriga hemliga tvångsmedel och innebörden ska vara densamma som i de fallen. Begreppet inrymmer ett kvalitetskrav avseende de upplysningar som åtgärden kan ge. Det ska finnas skäl att räkna med att avläsningen – ensam eller i förening med andra åtgärder – verkligen kan få effekt. Utredningsläget ska också vara sådant att hemlig dataavläsning är nödvändigt. Åtgärden får inte tillåtas om det som kan vinnas genom avläsningen är åtkomligt med andra, mindre ingripande metoder. När alternativa åtgärder står till buds ska en granskning av utredningsläget genomföras för att kunna bedöma behovet av varje åtgärd. Granskningen måste mynna ut i bedömningen att utredningen i princip inte kan

föras framåt med andra medel (inklusive andra hemliga tvångsmedel som i den föreliggande situationen bedöms som mindre ingripande) för att hemlig dataavläsning ska kunna tillåtas. Mot bakgrund av att samma uppgifter som hemlig dataavläsning kan ge tillgång till även kan få hämtas in med andra tvångsmedel och med hänsyn till riskerna för integritet och informationssäkerhet (se kap. 9) bör en utgångspunkt vid prövningen av om åtgärden är av synnerlig vikt vid hemlig dataavläsning vara att andra åtgärder inte är tillräckliga, väsentligt svårare att genomföra än vad hemlig dataavläsning eller förväntas leda till större integritetsintrång, se vidare avsnitt 10.5.3. Den utgångspunkten ställer krav på den som gör ansökan att utreda och tömma ut möjligheterna till andra åtgärder innan ansökan om hemlig dataavläsning görs. Den ställer också krav på den som ska pröva en ansökan och fatta beslut i frågor om hemlig dataavläsning att förhöra sig om vilka alternativ som finns och prövats.

I första styckets *andra och tredje mening* finns tilläggskrav när det gäller avläsning eller upptagning enligt 2 § första stycket 4, dvs. av kameraövervakningsuppgifter. Tilläggskraven innebär att sådan åtgärd endast får vidtas på en plats där den misstänkte kan antas komma att uppehålla sig och att platsen inte får vara inne i någons stadigvarande boende. Det första ledet av kravet är detsamma som gäller för hemlig kameraövervakning enligt 27 kap. 20 b § andra stycket rättegångsbalken och innebär att det måste finnas en direkt koppling mellan den misstänkte och platsen. Det kan röra sig om flera olika platser och det är inget som hindrar att antalet platser utökas genom nya domstolsbeslut. Om övervakningen av en viss plats i det enskilda fallet kan anses godtagbar ska bedömas utifrån en proportionalitetsavvägning. Hemlig kameraövervakning kan i praktiken inte riktas mot någons stadigvarande boende annat än utifrån, eftersom tillstånd till tillträde till sådant utrymme för att montera kameror inte får meddelas. För att uppnå överensstämmelse med var hemlig kameraövervakning får verkställas finns i första styckets tredje mening en bestämmelse om att hemlig dataavläsning enligt 2 § första stycket 4 inte får användas i någons stadigvarande boende.

För att förstå kraven om plats vid hemlig dataavläsning enligt 2 § första stycket 4 behöver man först förstå hur åtgärden går till att verkställa. Den brottsbekämpande myndigheten som verkställer hemlig dataavläsning får enligt 17 § andra stycket aktivera funktioner

i informationssystemet. Den funktion som behöver aktiveras när det är fråga om avläsning av kameraövervakningsuppgifter är kamerafunktionen i t.ex. en mobiltelefon. Den brottsbekämpande myndigheten är således oförhindrad att efter ett tillstånd enligt 2 § första stycket 4 aktivera en kamera i informationssystemet för att ta upp sådana uppgifter. Till skillnad från vad som är fallet vid sedvanlig hemlig kameraövervakning placeras således inte övervakningskameror ut på den plats som tillståndet avser, utifrån de anvisningar eller krav som anges i det. I stället är alltså kameran placerad i informationssystemet, t.ex. i en mobiltelefon. Det innebär att den brottsbekämpande myndigheten, för att verkställighet ska anses ske i enlighet med tillståndet, måste ha full kontroll på var informationssystemet är i varje givet ögonblick. Den som ska pröva förutsättningarna för tillstånd bör förhöra sig om hur den brottsbekämpande myndigheten tänkt att det ska gå till att ha kontroll över att den misstänkte och informationssystemet finns på den plats tillståndet ska avse och försäkra sig om att det är möjligt för den brottsbekämpande myndigheten att verkställa åtgärden enligt tillståndet.

Andra stycket

I bestämmelsens *andra stycke* finns ett första undantag till huvudregeln. Det innebär att hemlig dataavläsning enligt 2 § första stycket 2 och 3 får användas för att *utreda vem som skäligen kan misstänkas för brottet om åtgärden är av synnerlig vikt för utredningen*. Åtgärden får alltså endast avse uppgifter som annars kan hämtas in genom hemlig övervakning av elektronisk kommunikation. Bestämmelsen motsvarar 27 kap. 20 § andra stycket rättegångsbalken och begreppen ska ha samma innebörd som där. Genom att *brottet* anges i bestämd form klargörs att det ska pågå en förundersökning om ett sådant brott som anges i första stycket för att åtgärd enligt andra stycket ska få vidtas. Syftet med en åtgärd enligt andra stycket är att kunna identifiera en skäligen misstänkt gärningsman. Att syftet ska vara att *utreda vem som skäligen kan misstänkas för brottet* utesluter dock inte att åtgärden primärt kan ta sikte på att utröna var t.ex. en brottsplats är belägen, om den upplysningen är av avgörande betydelse för att utreda vem som skäligen kan misstänkas för brottet. Om det finns en skäligen misstänkt person kan åtgärden användas i

syfte att identifiera ytterligare personer som skäligen kan misstänkas för brott. Åtgärden ska vidare vara av *synnerlig vikt för utredningen*. Det innebär, på samma sätt som vid beslut om hemlig övervakning av elektronisk kommunikation, ett kvalitetskrav på de upplysningar som åtgärden kan ge. Upplysningarna får inte inskränka sig till detaljer av mindre betydelse. Uttrycket innefattar därutöver ett krav på att utredningsläget gör åtgärden nödvändig (prop. 1988/89:24 s. 24 f.). Av särskild betydelse beträffande frågan om synnerlig vikt för utredningen är att åtgärden avser uppgifter i informationssystem som inte används av misstänkt, se vidare i kommentaren till 5 §.

Som ett ytterligare krav gäller att om åtgärden innebär att uppgifter om meddelanden, dvs. enligt 2 § första stycket 2 läses av eller tas upp så får *uppgifterna endast avse förfluten tid.* Med formuleringen avses att avläsning eller upptagning enligt bestämmelsen endast är möjlig i fråga om uppgifter om meddelanden som har överförts, och alltså inte uppgifter om meddelanden i realtid. Se vidare om innebörden i prop. 2011/12:55 s. 129 f.

Tredje stycket

I bestämmelsens *tredje stycke* anges förutsättningarna för hemlig dataavläsning enligt 2 § första stycket 5, dvs. för att läsa av eller ta upp rumsavlyssningsuppgifter. Skillnaden mot första stycket är dels de brott som kan föranleda åtgärden, dels de platskrav som gäller. Det som anförts i kommentaren till första stycket om att någon ska vara *skäligen misstänkt* för brottet och att åtgärden ska vara av *synnerlig vikt för utredningen* gäller även här. När det gäller de brott som kan föranleda åtgärden så motsvarar de brotten som kan föranleda tillstånd till hemlig rumsavlyssning enligt brottskatalogen i 27 kap. 20 d § andra stycket rättegångsbalken. Således ska det pågå en förundersökning om något av följande brott.

1. Brott för vilket det inte är föreskrivet lindrigare straff än fängelse i fyra år.

2. Spioneri enligt 19 kap. 5 § brottsbalken.

3. Brott som avses i 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av

någon som har agerat för en främmande makts räkning och det kan antas att brottet inte leder till endast böter.

4. Annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i fyra år och det är fråga om

a) människohandel enligt 4 kap. 1 a § brottsbalken,

b) våldtäkt enligt 6 kap. 1 § första eller andra stycket brottsbalken,

c) grovt sexuellt tvång enligt 6 kap. 2 § tredje stycket brottsbalken,

d) våldtäkt mot barn enligt 6 kap. 4 § första eller andra stycket brottsbalken,

e) grovt sexuellt övergrepp mot barn enligt 6 kap. 6 § andra stycket brottsbalken,

f) grovt utnyttjande av barn för sexuell posering enligt 6 kap. 8 § tredje stycket brottsbalken,

g) grovt koppleri enligt 6 kap. 12 § tredje stycket brottsbalken,

h) grov utpressning enligt 9 kap. 4 § andra stycket brottsbalken,

i) grovt barnpornografibrott enligt 16 kap. 10 a § femte stycket brottsbalken,

j) grovt övergrepp i rättssak enligt 17 kap. 10 § tredje stycket brottsbalken,

k) grovt narkotikabrott enligt 3 § narkotikastrafflagen (1968:64), eller

l) grov narkotikasmuggling enligt 6 § tredje stycket lagen (2000:1225) om straff för smuggling,

5. Försök, förberedelse eller stämpling till brott som avses i 1–3, om en sådan gärning är belagd med straff.

6. Försök, förberedelse eller stämpling till brott som avses i 4, om en sådan gärning är belagd med straff och det med hänsyn till omständigheterna kan antas att gärningens straffvärde överstiger fängelse i fyra år.

Åtgärden får endast användas på *en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig*. Det är samma platskrav som gäller enligt rättegångsbalken för hemlig rumsavlyssning. Det ska alltså inte bara vara fråga om ett allmänt antagande om att den misstänkte kommer att uppehålla sig på platsen utan 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. I bestämmelsens näst sista mening framgår att om *platsen är någon annan stadigvarande bostad än den misstänktes* får hemlig dataavläsning användas *endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.* Det strängare kravet gäller alltså endast annan stadigvarande bostad än den misstänktes egen bostad. Därmed gäller kravet inte när tillståndet avser tillfälliga bostäder, såsom hotellrum eller andra tillfälliga sovarrangemang i t.ex. möteslokaler. Bestämmelsen innebär att det på grund av yttre omständigheter i förening med t.ex. andra inhämtade tillförlitliga uppgifter med fog kan förväntas 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 entydigt pekar på att den misstänkte, som annars har ett kringflackande liv och är svår att nå, varje vecka en viss tidpunkt besöker en bekant. Ett annat exempel är att det genom andra spaningsmetoder framkommit att den misstänkte har beställt tågbiljett i syfte att besöka och bo hos en bekant en tid.

Liksom beträffande verkställighet av hemlig dataavläsning för avläsning eller upptagning av kameraövervakningsuppgifter handlar det här om att det måste ske en aktivering av en funktion i informationssystemet, dock inte kameran utan i stället en funktion för ljudupptagning (t.ex. en mikrofon i en mobiltelefon). Den som ska pröva förutsättningarna för tillstånd bör således även i dessa fall 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.

I bestämmelsens sista mening framgår att hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter aldrig får avse sådana platser där hemlig rumsavlyssning inte får ske. Även detta krav motsvarar vad som gäller för hemlig rumsavlyssning enligt rättegångsbalken. Se vidare om vilka platser som avses i kommentaren till 12 §.

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.

Paragrafen innehåller bestämmelser om kopplingen mellan informationssystemet och den enskilde när hemlig dataavläsning ska genomföras under en förundersökning. Övervägandena finns i avsnitt 10.5.5.

Första stycket är huvudregeln. Enligt den krävs en koppling mellan en misstänkt och det informationssystem där uppgifterna som ska läsas av eller tas upp finns i. Kopplingen görs genom att det i bestämmelsen anges att den misstänkte ska använda informationssystemet eller att det annars ska finnas särskild anledning att anta att denne har använt eller kommer att använda informationssystemet. I begreppet *används* ligger ett sådant användande som omfattas av sedvanligt språkbruk. Således används ett informationssystem exempelvis när den misstänkte utnyttjar det för att ringa, skicka meddelanden eller utnyttja internet från eller spara elektroniska uppgifter med. Det bör för tydlighetens skull framhållas att en misstänkt som via en mobiltelefon eller dator kopplar upp sig mot internet i bestämmelsens mening använder mobiltelefonen eller datorn, vilka ju båda kan utgöra informationssystem. Däremot anses inte de servrar som den misstänkte från datorn eller mobiltelefonen anropar vara använda av denne i den mening som avses i bestämmelsen. Det

krävs inte att den misstänkte kan sägas inneha systemet och inte att hen är den enda 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 de som använder kontot. När det gäller begreppet *särskild anledning att anta* hänvisas till vad som anfördes om begreppet i kommentaren till 4 § tredje stycket ovan. Det ska alltså vara fråga om någon faktisk omständighet som med viss styrka talar för att den misstänkte har använt eller kommer att använda informationssystemet.

Det uppställs också ett krav i första stycket på att informationssystemet ska vara *identifierbart*. Kravet finns för att det ska vara möjligt för domstolen att ta ställning till kopplingen mellan den som ska utsättas för åtgärden och informationssystemet. Genom det klargörs också för den myndighet som ska verkställa ett beslut om hemlig dataavläsning vilket informationssystem som avses. Typiskt sett torde ett informationssystem vara identifierbart och möjligt att koppla till den person som är föremål för åtgärden t.ex. genom angivande av märke och modell när det är fråga om fysiskt avgränsade informationssystem och tjänst i förening med användarnamn, e-postadress eller liknande uppgifter när det är fråga om informationssystem som avgränsas på annat sätt än fysiskt.

I *andra stycket* finns ett första undantag från huvudregeln om att det ska vara den misstänkte som använder informationssystemet. Undantaget gäller endast beträffande uppgifter enligt 2 § första stycket 1–3, dvs. uppgifter som får hämtas in genom hemlig avlyssning eller övervakning av elektronisk kommunikation. Hemlig dataavläsning får tillåtas avseende sådana uppgifter i ett annat 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 vikt för utredningen som föreskrivs i 4 § första stycket gäller även i dessa fall. Faktorer som kan vara av särskild betydelse för bedömningen av om det är av synnerlig vikt för utredningen att använda hemlig dataavläsning mot annan än misstänkt är den brottslighet som utreds, vem som är misstänkt och utredbarheten av brottet om åtgärden inte vidtas. Det torde endast i undantagsfall vara av synnerlig vikt för utredningen att använda hemlig dataavläsning i informationssystem som används av andra än den misstänkte när det är fråga om annan brottslighet än

terroristrelaterad eller grovt organiserad brottslighet. När det ändå föreligger synnerlig vikt i sådana fall ska åtgärden också passera proportionalitetsprövningen.

Som nämnts uppställs också ett krav som innebär att det ska finnas *synnerlig anledning att anta* att den misstänkte under den tid som tillståndet avser *har kontaktat eller kommer att kontakta* informationssystemet. Kravet är detsamma som gäller vid hemlig avlyssning eller övervakning av elektronisk kommunikation under motsvarande förhållanden enligt 27 kap. 20 § första stycket 2 rättegångsbalken och ska ha samma innebörd som där. 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, se vidare i prop. 2002/03:74 s. 49. Det bör påpekas att med att kontakta annat informationssystem avses inte det anrop som görs till en server vid sedvanligt internetanvändande. Det är således inte möjligt för den brottsbekämpande myndigheten att använda hemlig dataavläsning i en server som den misstänkte genom sitt informationssystem anropar för att till exempel göra en sökning på internet med en sökmotor. Det som avses är i stället framför allt informationssystem, t.ex. en telefon eller dator eller ett e-postkonto som den misstänkte, från sitt informationssystem, ringer eller skickar meddelande till. Informationssystemet ska vara identifierbart och innebörden av detta begrepp är detsamma som enligt första stycket.

I *tredje stycket* framgår förutsättningarna för att använda hemlig dataavläsning enligt 2 § första stycket 2 och 3 för att utreda vem som skäligen kan misstänkas för ett brott. Utöver de förutsättningar och begränsningar som följer av 4 § andra stycket gäller när hemlig dataavläsning ska användas för det ändamålet att det ska vara fråga om ett identifierbart informationssystem som antingen har använts vid ett brott, i anslutning till en brottsplats vid brottstidpunkten eller på annat sätt är av synnerlig betydelse för att utreda vem som skäligen kan misstänkas för brottet. Bestämmelsen motsvarar i vissa avseenden 27 kap. 20 § andra stycket rättegångsbalken men har en något snävare utformning än den bestämmelsen, för att understryka att kravet på synnerlig vikt ska tillämpas restriktivt.

Att informationssystemet har *använts vid ett brott* innebär att informationssystemet haft avgörande betydelse vid själva genomförandet av brottet eller använts för att understödja brottet, se för

exempel på vad som avses med detta i punkterna 1 och 2 i definitionen av it-relaterad brottslighet i avsnitt 7.2. Att informationssystemet *använts i anslutning till en brottsplats vid brottstidpunkten* innebär i typfallet att ett informationssystem har använts på eller vid en brottsplats när ett brott har begåtts och att den brottsbekämpande myndigheten vet om att så är fallet. Avgränsningen för hur stort område kring brottsplatsen som åtgärden får vidtas inom måste bedömas från fall till fall. Det är naturligt att ett större område kan bli föremål för övervakning om brottet har begåtts på landsbygden än om det skett i en storstad. Att informationssystemet på annat sätt är av *synnerlig betydelse* för att utreda vem som skäligen kan misstänkas för brottet kan exempelvis vara fallet beträffande informationssystem som befunnits längs den väg gärningsmannen befaras har använt som flyktväg från en brottsplats. En annan situation där kravet kan vara uppfyllt är när det finns misstanke om brott som kan pågå en längre tid och där gärningsmannen kan tänkas förflytta sig, t.ex. vid människorov (4 kap. 1 § brottsbalken). Kravet på synnerlig betydelse i nu aktuellt avseende får i övrigt tolkas utifrån vad som nu anförts. Det bör emellertid, liksom i övriga fall då *synnerlig* används i lagstiftning, innefatta ett högt ställt krav på konkretisering. Detta krav gäller utöver det grundläggande kravet på att åtgärden ska vara av synnerlig vikt för utredningen

Liksom i situationen enligt andra stycket är det när hemlig dataavläsning sker enligt tredje stycket inte fråga om att använda åtgärden i ett informationssystem som tillhör en misstänkt person. Det som anfördes i kommentaren till andra stycket om vad som ska iakttas när den som blir föremål för hemlig dataavläsning inte är misstänkt gör sig därför gällande för situationen enligt tredje stycket.

Enligt den avslutande meningen i tredje stycket får det inte komma i fråga att använda åtgärden avseende uppgifter i ett informationssystem som tillhör någon som enligt lagen om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Sådana företag kan ju vara skyldiga att bistå vid sedvanlig verkställighet av hemlig övervakning av elektronisk kommunikation, se t.ex. 27 kap. 25 § andra stycket rättegångsbalken och 6 kap. 19 § lagen om elektronisk kommunikation. Om den brottsbekämpande myndigheten vid sådan verkställighet inte får ut de uppgifter som förväntats ska det inte vara möjligt för myndigheten att vända sig till domstol för att få tillstånd

att i hemlighet, genom hemlig dataavläsning enligt denna bestämmelse, t.ex. undersöka företagets servrar eller andra datorer. Även om detta torde följa redan genom en strikt tillämpning av proportionalitetsprincipen finns i bestämmelsens sista mening ett uttryckligt förbud mot sådan tillämpning.

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.

I paragrafen ges några grundläggande bestämmelser om vad som ska gälla för tillståndsgivning av hemlig dataavläsning när sådana förhållanden som kan föranleda hemliga tvångsmedel enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) föreligger. Övervägandena finns i avsnitt 10.6.2.

Första stycket

I *första stycket* framgår grunderna för att få meddela beslut om hemlig dataavläsning utanför en förundersökning. Dessa grunder motsvarar de lagliga grunder som gäller för att hemlig tvångsmedelsanvändning enligt 1 § preventivlagen ska kunna komma i fråga (preventivlagsfallen). Hemlig dataavläsning kan enligt bestämmelsen få användas i preventivlagsfallen för samtliga uppgiftstyper enligt 2 § första stycket utom för avläsning eller upptagning av rumsavlyssningsuppgifter (2 § första stycket 5) om förutsättningarna enligt bestämmelsen är uppfyllda, se vidare i kommentaren till tredje stycket.

Det finns två alternativa grunder för tillstånd enligt förevarande bestämmelse. Den första innebär att det med hänsyn till omständigheterna ska finnas en påtaglig risk för att en person kommer att utöva viss brottslig verksamhet. Enligt förarbetena till preventivlagen, vilka mot bakgrund av att rekvisiten är desamma enligt denna lag som enligt preventivlagen är tillämpliga vid tolkningen av denna bestämmelse, kommer prövningen av om rekvisiten är uppfyllda normalt att få 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). När det gäller frågan om *påtaglig risk* är en självklar utgångspunkt enligt förarbetena att en riskbedömning vid preventiv tvångsmedelsanvändning inte får bygga endast på spekulationer eller allmänna bedömningar utan ska vara grundad på faktiska omständigheter som föreligger vid beslutstillfället. Detta kan vara t.ex. uttalanden, hotelser eller annat faktiskt agerande som talar för att brottslig verksamhet av visst slag kommer att utövas. Risken ska vidare avse en klart förutsebar utveckling utifrån dessa omständigheter, t.ex. att ett terrordåd eller attentat kan komma att ske. Att risken ska vara påtaglig innebär också ett krav på viss sannolikhet för att risken ska förverkligas. Däremot krävs det inte att risken avser en konkretiserad gärning. Tillstånd till tvångsmedelsanvändning bör alltså kunna meddelas i fall när flera inträffade omständigheter kan påvisas som starkt talar för en risk för att ett brott av ett visst slag kommer att inträffa men utan att det går att konkretisera hur risken kan förverkligas, t.ex. vilket närmare tillvägagångssätt som kommer att användas vid ett terrordåd eller vilket mål detta kommer att avse. Bedömningen av risken bör ta

sin utgångspunkt i både avsikt och förmåga (prop. 2013/14:237 s. 195 f.).

Uttrycket *en person* innefattar inte något krav på att det ska vara fråga om en till namnet känd viss person. Om Säkerhetspolisen har information om att en person, vars namn är okänt, kan komma att genomföra ett terroristbrott, förhindrar således bristen på information om personens namn inte i sig att tillstånd till tvångsmedel lämnas (prop. 2005/06:177 s. 83).

Genom rekvisitet *brottslig verksamhet* framgår att regleringen inte ställer upp något krav på att det ska finnas en misstanke om ett specifikt brott. Det föreligger därför en principiell skillnad i förhållande till tillämpningsområdet för straffprocessuella tvångsmedel enligt rättegångsbalken som förutsätter att ett specifikt brott har begåtts. Däremot måste den befarade brottsliga verksamheten innefatta någon av de gärningar som räknas upp i 1 § preventivlagen (jfr prop. 2005/06:177 s. 83). De gärningar som anges där är följande.

1. Sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken.

2. Mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel.

3. Uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken.

4. Högförräderi, krigsanstiftan, spionerі, grovt spionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6 eller 8 § eller 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken.

5. Företagsspionerі enligt 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten kommer att utövas på uppdrag av eller understödjas av en främmande makt eller av någon som kommer att agera för en främmande makts räkning.

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

uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.

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

Tillstånd till hemlig dataavläsning får enligt bestämmelsens *andra mening* 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. Även denna grund motsvarar vad som anges i preventivlagen för tillstånd till hemliga tvångsmedel enligt den lagen. Därför är förarbetsuttalandena till preventivlagens bestämmelse av betydelse även här.

Bestämmelsen innebär att det, när det finns en påtaglig risk för att brottslighet av angivet slag kommer att begås inom en organisation eller grupp, föreligger en viss lättnad beträffande kravet på riskbedömning i förhållande till de personer som tillhör eller verkar för organisationen eller gruppen. Tvångsmedelsbeslut måste dock alltid riktas mot en viss utpekad person inom organisationen eller gruppen. Däremot behöver graden av risk som kan knytas till personen i dessa fall inte nå upp till nivån *påtaglig risk*, utan det är tillräckligt att det kan befaras att personen *medvetet kommer att främja* den brottsliga verksamheten. I dessa fall ska alltså två olika riskbedömningar göras, en i förhållande till organisationen eller gruppen (påtaglig risk) och en annan i förhållande till den person som man överväger att rikta tvångsmedelsanvändningen mot (kan befaras medvetet främja), se prop. 2013/14:237 s. 196.

Vad avser den riskbedömning som ska göras i förhållande till organisationen gäller samma krav som för bedömningar enligt den första meningen. I dessa fall tillkommer dock även krav på att risken ska avse brottslig verksamhet som kommer att utövas inom organisationen eller gruppen. Detta innebär att det ska finnas en koppling mellan organisationen eller gruppen och den brottsliga verksamheten, se prop. 2013/14:237 s. 196.

När det sedan gäller den riskbedömning som ska göras i förhållande till den person som ska bli föremål för tvångsmedelsanvändningen krävs att det kan befaras att personen kommer att främja den brottsliga verksamheten. Termen främjande är avsedd att ha samma betydelse som enligt brottsbalken. De krav som ställs där för att ett främjande i objektiv mening ska anses föreligga ska således tillämpas även i detta sammanhang. I likhet med vad som gäller enligt första meningen är dock inte avsikten att de brottsbekämpande myndigheterna ska behöva konkretisera exakt vilken eller vilka åtgärder som den aktuella personen kan befaras vidta. Den bedömning som ska göras bör därför snarare ta sikte på att värdera de omständigheter som talar för en risk för främjande än att bedöma vad ett sådant främjande kan tänkas bestå i. Bestämmelsen innebär att det ställs ett visst krav på konkretion beträffande de omständigheter som talar för att ett främjande kommer att ske. Det måste alltså finnas vissa objektivt fastställbara tecken på att den person som man överväger att använda tvångsmedel mot kommer att vidta någon åtgärd som i det aktuella fallet innebär ett främjande. Kravet på sannolikhet för att någon kommer att utöva ett främjande är dock lägre än kravet på sannolikhet för att brottslig verksamhet kommer att utövas inom organisationen eller gruppen. Detta framgår av att det är tillräckligt att ett främjande kan befaras. Omständigheter som kan tala för att en främjandefara föreligger bör t.ex. i vissa fall kunna vara den ställning personen har i organisationen (som t.ex. ledare eller aktiv medlem) eller att denne tidigare dömts för brottslighet som är relevant i sammanhanget. Tidigare brottslighet som kan vara relevant är inte endast sådan som innefattar brott som kan leda till tvångsmedel enligt lagen. Exempelvis kan, när den aktuella risken avser ett attentat, tidigare vålds- eller vapenbrottslighet vara av betydelse. Medlemskap i en organisation är emellertid inte i sig tillräckligt för ett tvångsmedelsbeslut mot någon, se prop. 2013/14:237 s. 196 f.

För att ett främjande ska kunna läggas till grund för ett beslut om hemlig dataavläsning krävs också att det kan befaras att främjandet kommer att ske medvetet. Det är alltså inte tillräckligt att det kan befaras att en person mera allmänt kommer att stödja en organisation eller grupp, t.ex. genom att lämna ekonomiskt stöd eller liknande, om personen inte är medveten om att han eller hon därigenom främjar brottslig verksamhet. Kravet innebär att det ska kunna befaras att den aktuella personen antingen kommer att agera i

direkt syfte att främja brottslig verksamhet eller att denne inser att detta kommer att bli effekten av hans eller hennes handlande (prop. 2013/14:237 s. 197).

Andra stycket

Ett första krav enligt andra stycket är att tillstånd endast får meddelas om åtgärden är av synnerlig vikt för att förhindra sådan brottslig verksamhet som anges i första stycket. Begreppet synnerlig vikt har utvecklats i kommentaren till 4 § första 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 angavs där.

I andra stycket föreskrivs också ett platskrav och en särskild begränsning avseende platser som är någons stadigvarande bostad för de tillfällen då hemlig dataavläsning ska användas enligt 2 § första stycket 4, dvs. för att läsa av eller ta upp kameraövervakningsuppgifter. Platskravet och begränsningen motsvarar vad som föreskrivs i 4 § första stycket, dock med skillnaden att en sådan person som kan antas uppehålla sig på platsen inte är misstänkt utan i stället den person som anges i första stycket. Med denna anmärkning gäller vad som angetts i kommentaren till 4 § första stycket andra och tredje meningen även beträffande den situation som här avses.

Tredje stycket

Av *tredje stycket* framgår uttryckligen att tillstånd enligt första stycket inte får avse hemlig dataavläsning enligt 2 § första stycket 5. 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, vilket stämmer helt överens med att preventivlagen inte tillåter hemlig rumsavlyssning i underrättelseverksamhet.

Motsatsvis innebär tredje stycket även att hemlig dataavläsning för de andra uppgiftstyper som anges i 2 § första stycket är tillåtna i underrättelseverksamhet på de grunder som anges i första stycket. Att sådana uppgifter som får läsas av eller tas upp enligt 2 § första stycket 6 och 7 således omfattas av bestämmelsen utgör i jämförelse

med preventivlagen en utvidgning avseende vilka typer av uppgifter som får samlas in i dag.

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.

Paragrafen innehåller bestämmelser om kopplingen mellan informationssystemet och den enskilde när det är fråga om tillstånd som avses i 6 §. Övervägandena finns i avsnitt 10.6.2.

I bestämmelsens *första stycke* klargörs att den reglerar kopplingen mellan informationssystemet och den som blir föremål för åtgärden när det är fråga om hemlig dataavläsning som baseras på 6 §, dvs. i preventivlagsfallen. Bestämmelsen är likadant utformad som 5 § första stycket med den enda skillnaden att den enskilde som är föremål för åtgärden inte är en misstänkt utan en person som anges i 6 §, vilket är en naturlig följd av att bestämmelsen reglerar preventivlagsfallen. Den person som kan bli föremål för åtgärden, och som alltså kopplingen till informationssystemet ska finnas till, är således antingen en person som det finns påtaglig risk kommer att utöva sådan brottslig verksamhet som anges i 1 § preventivlagen eller en person som tillhör eller verkar för en organisation eller grupp inom vilken det finns påtaglig risk för att det kommer att utövas sådan brottslig verksamhet och som det kan befaras medvetet kommer att främja denna verksamhet (se kommentaren till 6 § första stycket). I övrigt är ingen skillnad avsedd i förhållande till vad som gäller enligt 5 § första stycket, varför det hänvisas till den kommentaren.

Bestämmelsens *andra stycke* motsvarar, med samma skillnad som enligt första stycket avseende person, 5 § andra stycket. Eftersom

ingen skillnad är avsedd i förhållande till vad som gäller enligt den bestämmelsen hänvisas även här till den kommentaren.

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.

I paragrafen ges bestämmelser om vad som ska gälla för tillståndsgivning vid hemlig dataavläsning när sådana förhållanden som kan föranleda hemliga tvångsmedel enligt lagen om särskild utlänningskontroll (LSU) föreligger. Övervägandena finns i avsnitt 10.6.3.

I *första stycket* framgår grunder för att meddela tillstånd till hemlig dataavläsning utanför en förundersökning. Dessa grunder motsvarar de lagliga grunder som gäller för tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation enligt LSU (LSU-fallen). Första stycket är indelat i fyra punkter som innehåller förutsättningar för hemlig dataavläsning i LSU-fallen. Förutsättningarna

enligt samtliga ska vara uppfyllda för att tillstånd ska få meddelas vilket framgår av att punkterna binds samman av ordet *och*.

I första styckets *första punkt* anges att det ska ha fattats ett beslut om utvisning enligt 1 § 2 LSU. I punkten skrivs av tydlighetsskäl också ut vilka omständigheter som kan föranleda ett sådant beslut. Bestämmelsen är utformad helt i enlighet med vad som framgår av nämnda lagrum i LSU.

I paragrafens första styckes *andra punkt* framgår att det finns fyra olika grunder enligt vilka lagen om hemlig dataavläsning kan aktualiseras när ett beslut enligt första punkten har fattats. Strukturen i punkten utgår från vad som gäller enligt LSU. Enligt den lagen förutsätts för att hemlig tvångsmedelsanvändning ska kunna aktualiseras att en myndighet eller en domstol, på någon av de grunder som är angivna i lagen, har fattat beslut om att dess bestämmelser om hemliga tvångsmedel (19–22 §§ LSU) alls ska få tillämpas. Om inget sådant beslut i det enskilda fallet har fattats gäller således inte 19–22 §§ LSU i förhållande till en utlänning i ett enskilt fall, och denne kan då inte heller bli föremål för hemliga tvångsmedel.

Grunderna för beslut att tillämpa 19–22 §§ LSU mot en utlänning i ett enskilt fall, vilka alltså är samma grunder som framgår av förevarande bestämmelse för att ”aktivera” lagen om hemlig dataavläsning i LSU-fallen, är följande.

1. 11 § LSU. När ett beslut om utvisning som grundas på 1 § 2 LSU tills vidare inte ska verkställas på grund av inhibition eller ett tidsbegränsat uppehållstillstånd får den myndighet som beslutar om utvisning enligt LSU bestämma att reglerna i 19–22 §§ LSU, ska tillämpas på utlänningen. De myndigheter som får besluta om utvisning enligt LSU är Migrationsverket och regeringen.

2. 11 a § LSU. När ett beslut om avvisning eller utvisning enligt 8 eller 8 a kap. utlänningslagen (2005:716) eller motsvarande äldre bestämmelser inte kan verkställas och det finns sådana omständigheter i fråga om utlänningen som avses i 1 § 2 LSU får Migrationsverket bestämma att 19–22 §§ LSU ska tillämpas på utlänningen.

3. 14 § LSU. När tidsfristen enligt 12 § LSU (tre år) för beslut enligt 11 eller 11 a §§ LSU att aktivera lagens regler om hemliga tvångsmedel har löpt ut men det bedöms föreligga fortsatt risk för att utlänningen begår eller medverkar till brott som anges i 1 § 2 LSU får Stockholms tingsrätt på ansökan av Säkerhetspolisen bestämma att 19–22 §§ LSU ska tillämpas på utlänningen.

4. 15 § LSU. Rätten får fatta interimistiskt beslut i fråga som avses i 14 § LSU, om det finns skäl till det. Ett sådant beslut får avse tiden till dess ärendet avgjorts slutligt.

Den andra punkten i förevarande bestämmelse innebär således att det krävs ett beslut om att lagen om hemlig dataavläsning ska tillämpas i ett enskilt fall mot en utlänning för vilken det meddelats ett sådant utvisningsbeslut som avses i första punkten. Beslut om att lagen ska tillämpas får endast fattas på sådana grunder och av de myndigheter (i praktiken Migrationsverket, regeringen eller Stockholms tingsrätt) som kan göra 19–22 §§ LSU tillämpliga i motsvarande fall. Av bestämmelsen i andra punkten framgår också att motsvarande förfarande ska tillämpas när det är fråga om att göra lagen om hemlig dataavläsning tillämplig som när 19–22 §§ ska aktiveras. Genom detta uttryckssätt klargörs att det är förfaranderegelerna i LSU som ska tillämpas vid prövningen av om lagen om hemlig dataavläsning ska få tillämpas mot en utlänning som avses i första punkten.

I första styckets *tredje punkt* framgår för vilket ändamål hemlig dataavläsning får användas i förevarande situation. Ändamålet är samma som gäller för annan tvångsmedelsanvändning enligt LSU, nämligen att det ska vara av betydelse för att utreda om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för, planlägger eller förbereder terroristbrott eller försök, förberedelse eller stämpling till sådant brott. Ingen annan betydelse är avsedd än vad som gäller enligt LSU.

I *fjärde punkten* i första stycket framgår ytterligare ett krav som motsvarar vad som uppställs för tillstånd till hemliga tvångsmedel enligt LSU, nämligen att det ska finnas *synnerliga skäl*. Även om ett något annorlunda uttryckssätt används jämfört med de övriga hemliga tvångsmedelbestämmelserna (där begreppet *synnerlig vikt* används) är kravet likvärdigt. Det kan därför hänvisas till vad som anförts i kommentaren till 4 § första stycket.

I bestämmelsens *andra stycke* anges att ett tillstånd enligt första stycket inte får avse åtgärder enligt 2 § första stycket 4 eller 5. Av detta följer uttryckligen att hemlig dataavläsning i LSU-fallen inte får användas för avläsning eller upptagning av kameraövervaknings- eller rumsavlyssningsuppgifter. I den delen motsvarar bestämmelsen vad som gäller enligt LSU som inte möjliggör hemlig kameraövervakning eller hemlig rumsavlyssning.

Av andra stycket följer också motsatsvis att hemlig dataavläsning får användas för att läsa av eller ta upp övriga uppgiftstyper enligt 2 § första stycket, om förutsättningarna enligt bestämmelsen är uppfyllda. Att sådana uppgifter som får läsas av eller tas upp enligt 2 § första stycket 6 och 7 således omfattas av bestämmelsen utgör i jämförelse med LSU en utvidgning avseende vilka typer av uppgifter som får samlas in enligt LSU i dag.

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.

I paragrafen anges vilken koppling som ska finnas mellan informationssystemet utlänningen när det är fråga om tillstånd som avses i 8 §. Övervägandena finns i avsnitt 10.6.3.

I bestämmelsen klargörs att den reglerar kopplingen mellan informationssystemet och den som blir föremål för åtgärden när det är fråga om hemlig dataavläsning som grundas på 8 §, dvs. i LSU-fallen. Bestämmelsen är likadant utformad som 5 § första stycket med den enda skillnaden att den enskilde som är föremål för åtgärden inte är en misstänkt utan en person som anges i 8 § första stycket 1, vilket är en följd av att bestämmelsen reglerar LSU-fallen. Den person som kan bli föremål för åtgärden, och som alltså kopplingen till informationssystemet ska finnas till, är en utlänning som det fattats ett utvisningsbeslut för enligt 1 § 2 LSU. Det är således i förhållande till denne som kopplingen till informationssystemet ska prövas. I övrigt är ingen skillnad avsedd i förhållande till vad som gäller enligt 5 § första stycket, varför det hänvisas till den kommentaren.

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.

I paragrafen ges bestämmelser om att uppgifter enligt 2 § första stycket 2 och 3 under särskilda förutsättningar, motsvarande de som gäller för inhämtning av sådana uppgifter enligt inhämtningslagen, får läsas av eller tas upp i underrättelseverksamhet. Övervägandena finns i avsnitt 10.6.4.

Enligt bestämmelsens *första stycke* avser den endast hemlig dataavläsning *enligt 2 § första stycket 2 och 3*. Det innebär för det första att den har ett betydligt snävare potentiellt användningsområde än övriga bestämmelser som reglerar förutsättningarna för tillstånd till hemlig dataavläsning.

Vidare är det ett krav enligt första stycket att åtgärden är av *synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar* vissa särskilt angivna brott. Det kursiverade uttryckssättet motsvarar kraven som gäller enligt 2 § 1 inhämtningslagen för att inhämtning av uppgifter ska få vidtas enligt den lagen, med den skillnaden att åtgärden här ska vara av synnerlig vikt i stället för av särskild vikt. *Synnerlig vikt* ska ha samma innebörd som när uttrycket används i andra sammanhang i denna lag, se kommen-

taren till 4 § första stycket. Kravet utgör både ett kvalitetskrav på de upplysningar som åtgärden kan ge och ett krav på behovet av inhämtningen i det enskilda fallet. Självklart ska synnerlig vikt i detta sammanhang ta sikte på förebyggandet, förhindrandet eller upptäckandet av den brottsliga verksamheten i stället för utredningen. För tolkningen av begreppen *brottslig verksamhet* och *förebygga, förhindra eller upptäcka* hänvisas till vad som anförts i prop. 2011/12:55 s. 121.

Det är endast när den brottsliga verksamheten som ska förebyggas, förhindras eller upptäckas innefattar brott för vilket inte är föreskrivet lägre straff än fängelse i två år eller brott som anges i 3 § inhämtningslagen som åtgärd enligt bestämmelsen kan aktualiseras. Det är således samma krav som uppställs för att inhämtning enligt inhämtningslagen ska få ske. De brott som anges i 3 § inhämtningslagen, som är tidsbegränsad till utgången av 2019, är följande brott.

1. Sabotage enligt 13 kap. 4 § brottsbalken.

2. Kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel.

3. Brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken.

4. Spionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5 eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken.

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

I *andra meningen i första stycket* finns en begränsning som motsvarar vad som gäller enligt inhämtningslagen, nämligen att 2 § andra stycket inte ska tillämpas. När hemlig dataavläsning används i inhämtningslagsfallen får således den brottsbekämpande myndigheten inte hindra meddelanden från att nå fram.

I bestämmelsens *andra stycke* begränsas de uppgifter som enligt 2 § 2 får läsas av eller tas upp så att avläsning eller upptagning i dessa fall endast får avse uppgifter om meddelanden som har överförts, och alltså inte uppgifter om meddelanden i realtid. Det mot-

svarar vad som gäller enligt inhämtningslagen för sådana uppgifter, se prop. 2011/12:55 s. 120 och 129 f.

I *tredje stycket* finns bestämmelser om att hemlig dataavläsning i inhämtningslagsfallen endast får avse uppgifter i ett identifierbart informationssystem. Bestämmelsen liknar regleringen i 5 § tredje stycket, där det inte heller krävs en koppling till en viss person. I förevarande bestämmelse uppställs dock inga andra krav än att informationssystemet är identifierbart. Det innebär att det inte är nödvändigt att veta vem som använder informationssystemet men att det måste stå alldeles klart att avläsning eller upptagning sker ifrån ett visst informationssystem. Kravet på synnerlig vikt enligt första stycket gör emellertid att informationssystemet ska vara av intresse av någon specifik anledning. Kravet på att informationssystemet ska vara *identifierbart* är detsamma som enligt andra bestämmelser i lagen, se kommentaren till 5 § första stycket.

Av samma skäl som anförts i kommentaren till 5 § tredje stycket finns i bestämmelsens sista mening en begränsning som innebär att en åtgärd enligt bestämmelsen inte får avse uppgifter i ett informationssystem som tillhör någon som enligt lagen 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.

I paragrafen anges begränsningar som innebär att hemlig dataavläsning inte får avse uppgifter i vissa informationssystem. Övervägandena finns i avsnitt 10.7.2.

Bestämmelsen består av tre punkter som klargör att det finns ett absolut förbud mot hemlig dataavläsning avseende uppgifter i vissa informationssystem. I samtliga punkter uppställs först ett krav på att informationssystemet *stadigvarande används* i en verksamhet. Stadigvarande används är samma krav som gäller avseende platser där hemlig rumsavlyssning inte får ske, se 27 kap. 20 e § tredje stycket rättegångsbalken. När den bestämmelsen infördes angavs i förarbetena att begreppet medför att det inte är möjligt att undgå rumsavlyssning endast genom att tillfälligtvis upplåta eller inrätta en lokal för sådan skyddad verksamhet (prop. 2005/06:178 s. 102). På motsvarande vis gäller enligt förevarande bestämmelse att informationssystem som endast undantags- eller tillfälligtvis används i sådan verksamhet inte omfattas av förbudsregeln. Typiskt sett torde därför förbudsregeln inte träffa t.ex. privata mobiltelefoner eller datorer som någon gång används i sådan verksamhet som avses.

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 rättegångsbalken, dvs. verksamheter där rumsavlyssning inte får ske. Verksamheterna anknyter också till sådana verksamheter som omfattas av frågeförbudet i 36 kap. 5 § andra-sjätte styckena rättegångsbalken.

Den *första punkten* avser primärt medieföretag, t.ex. ett förlag eller en nyhetsbyrå, som bedriver verksamhet för vilken det råder tystnadsplikt enligt reglerna i 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen. Den tystnadsplikt det är fråga om kan exempelvis avse vem som är författare eller utgivare av periodisk skrift eller vem som har lämnat meddelande som omfattas av meddelarfriheten.

Andra punkten avser verksamhet som bedrivs av advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer, psykoterapeuter eller familjerådgivare enligt socialtjänstlagen. Det är fråga om väl avgränsade yrkesgrupper i vilkas verksamhet känsliga uppgifter ofta förekommer.

Den *tredje punkten* tar sikte på informationssystem som används av präster inom trossamfund eller av dem som har motsvarande ställning inom sådana samfund. Punkten avser dock endast infor-

mationssystem som används i verksamhet för bikt eller enskild själavård.

Det ankommer på den brottsbekämpande myndigheten att i sitt kartläggningsarbete skaffa fram underlag så att den som ska göra ansökan hos domstolen kan lägga fram uppgifter som tydliggör att informationssystemet inte omfattas av förbudsregeln.

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.

I paragrafen ges förutsättningarna för att en domstol ska kunna meddela tillträdestillstånd till annars skyddade platser samt undantag från möjligheten att meddela tillträdestillstånd. Övervägandena finns i avsnitt 10.8.

Bestämmelsen är utformad med viss ledning av 27 kap. 20 e § andra och tredje styckena och 25 a § rättegångsbalken. Eftersom

hemlig dataavläsning kan användas för att läsa av eller ta upp andra uppgifter än sådana som kan hämtas in genom hemlig rumsavlyssning utgör bestämmelsen en utvidgning av de tillfällen tillträdestillstånd kan meddelas.

I *första stycket* anges förutsättningarna för att meddela ett tillträdestillstånd när hemlig dataavläsning ska verkställas. I bestämmelsens *första mening* slås fast att tillträdestillstånd får meddelas för att i hemlighet installera tekniska hjälpmedel, med vilka typiskt sett avses hårdvara eller programvara. Eftersom installation ska ske på platsen (*på en plats*) ger ett tillträdestillstånd inte den verkställande myndigheten rätt att ta med sig informationssystemet därifrån. Tillträdestillståndet får avse en plats *som annars skyddas mot intrång*. Huvudsakligen är det de platser som skyddas genom bestämmelserna i 4 kap. 6 § brottsbalken om hemfridsbrott och olaga intrång som avses. Det är således inte bara fråga om bostäder utan också bl.a. arbetsplatser och föreningslokaler. Även det som skyddas genom bestämmelsen i 8 kap. 8 § brottsbalken om egenmäktigt förfarande avses med plats som annars skyddas mot intrång. Det krävs således ett särskilt tillstånd av rätten för tillträde till exempelvis en bil, se även prop. 2005/06:178 s. 104. Det krävs inget särskilt tillstånd enligt denna bestämmelse för att ta sig in i ett informationssystem som annars skyddas mot intrång (t.ex. enligt 4 kap. 9 c § brottsbalken). Sådana intrång sker i stället med stöd av 17 § andra stycket.

Det relevanta vid tillträdestillstånd för hemlig dataavläsning är att informationssystemet som tillståndet avser finns på platsen. Därför uppställs som huvudregel i *andra meningen* i första stycket ett krav på att det ska finnas särskild anledning att anta att informationssystemet finns på platsen. 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.

I första styckets *tredje mening* uppställs ett ännu högre krav när det är fråga om att platsen är någon annan stadigvarande bostad än den misstänktes. I de fallen krävs i stället att ett tillträdestillstånd endast får meddelas om det finns synnerlig anledning att anta att informationssystemet finns där. Med *synnerlig anledning* avses att det ska föreligga någon faktisk omständighet som påtagligt visar att

man med fog kan förvänta sig att informationssystemet finns på platsen, se vidare om kravet i annat sammanhang t.ex. JO 1988/89 s. 68. Det ska understrykas att det strängare kravet alltså endast avser annan stadigvarande bostad än den misstänktes. Därmed kommer kravet inte att gälla när åtgärden ska riktas mot tillfälliga bostäder, såsom hotellrum eller andra tillfälliga sovarrangemang i t.ex. möteslokaler.

Ett beslut om befogenhet till tillträde gäller för hela tillståndstiden (om rätten inte beslutar annat) och även efter tillståndsperiodens utgång till den del det avser borttagande, avinstallation eller obrukbargörande av det tekniska hjälpmedlet, se 20 § fjärde stycket. 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 sig in i t.ex. en bostad eller ett annat utrymme som tillståndet gäller för att genomföra installationen (eller avinstallationen), jfr prop. 2005/06:178 s. 104 f.

I *andra stycket* klargörs att personer som kan bli föremål för hemlig dataavläsning i preventivlags- och LSU-fallen jämställs med misstänkta vid bedömningen av vems den stadigvarande bostaden är. Regeln innebär att det endast krävs särskilda skäl för tillträdestillstånd när informationssystemet finns på en plats som är någon av de angivna personkategoriernas stadigvarande bostad.

I bestämmelsens *tredje stycke* framgår att ett tillträdestillstånd aldrig får avse platser som stadigvarande används för de verksamheter som anges i 11 §. Utformningen av bestämmelsen motsvarar helt utformningen av 27 kap. 20 e § tredje stycket rättegångsbalken, som anger vilka platser hemlig rumsavlyssning inte får ske på. Bestämmelsen ska tillämpas på motsvarande vis som den nämnda bestämmelsen i rättegångsbalken. Det innebär bl.a. att kravet på *stadigvarande används* medför att det inte är möjligt att undvika att tillträdestillstånd meddelas endast genom att tillfälligtvis upplåta eller inrätta en lokal för sådan skyddad verksamhet, jfr prop. 2005/06:178 s. 102. Kravet på sådan stadigvarande användning som anges i exempelvis punkten 1 behöver inte vara begränsad till att avse ett medieföretags redaktion utan kan omfatta också t.ex. en arbetsplats i en journalists hem, se prop. 2013/14:237 s. 180. När det gäller de enskilda punkterna i bestämmelsen hänvisas i övrigt till vad som anförts i kommentaren till 11 §.

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.

I paragrafen finns regler om tillståndsprövningen vid hemlig dataavläsning och vad ett tillstånd till åtgärden ska innehålla. Övervägandena finns i avsnitt 10.9.1, 10.9.3 och 10.9.4.

I *första stycket* framgår först att frågor om hemlig dataavläsning alltid ska prövas av rätten. Det innebär att det i inhämtningslagsfallen enligt 10 § är en annan instans som fattar beslut än vad som gäller enligt inhämtningslagen. I övrigt innebär det samma ordning som gäller för övriga hemliga tvångsmedel.

Vem som ska göra ansökan om hemlig dataavläsning följer av första meningens andra led och andra meningen. Dessa bestämmelser följer mönstret enligt gällande hemlig tvångsmedelsreglering och innebär att åklagaren ansöker om tillstånd i samtliga fall utom när ansökan avser LSU-fallen. Liksom det som gäller vid tillståndsansökan för hemliga tvångsmedel enligt 21 § andra stycket LSU är det då i stället Polismyndigheten eller Säkerhetspolisen som ska göra ansökan. Det hänger samman med de ärendenas särpräglade natur.

Att åklagaren gör ansökan i övriga fall innebär att denne också kommer att ansöka om tillstånd till hemlig dataavläsning i inhämt-

ningslagsfallen. Detta skiljer sig från nuvarande ordning enligt inhämtningslagen, där myndigheten själv fattar beslut och ansökan således inte behövs. Det skiljer sig även från förslaget i SOU 2017:75 som innebär att åklagaren ska pröva om förutsättningar för inhämtning enligt inhämtningslagen föreligger på ansökan av den brottsbekämpande myndighet i vars verksamhet inhämtningen ska ske.

I bestämmelsens *andra stycke* framgår vad ett beslut om att tillåta hemlig dataavläsning ska innehålla. Enligt styckets *första punkt* ska det av beslutet framgå vilken tid åtgärden avser. Liksom för övriga hemliga tvångsmedel gäller enligt *tredje stycket* först och främst 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 ske och att åtgärden ska bli användbar. Den bortre gränsen för ett tillstånd är enligt bestämmelsen en månad från dagen för tillståndsbeslutet. Att längsta tiden för tillstånd föreslås vara en månad åt gången beror i första hand på att det i flera fall kommer att finnas behov av att förbereda verkställigheten i flera avseenden innan hemlig dataavläsning kan tas i bruk. En del sådana förberedande åtgärder torde inte kunna företas innan rätten lämnat tillstånd till tvångsmedlet. Krävs det inte några mera omfattande förberedelser kan det sannolikt ofta finnas skäl att begränsa tillståndet till betydligt kortare tid. I synnerhet bör så vara fallet när tillståndet avser åtgärd enligt 2 § 6 (lagrade uppgifter) eftersom målet med åtgärden då kan vara uppfyllt när själva avläsningen eller upptagningen av den lagrade informationen skett. Visserligen ska beslutet om tillstånd till hemlig dataavläsning omedelbart upphävas enligt 16 § andra stycket om det inte längre finns skäl för tillstånd men det kan ändå finnas anledning för domstolen att av integritetsskäl begränsa åtgärdens tillåtna varaktighet.

Av bestämmelsen om hur lång tid ett tillstånd får gälla framgår att den bortre tidsgränsen endast tar sikte på tid som infaller efter beslutet. Det innebär motsatsvis att det inte finns någon lagstadgad bortre tidsgräns för tid som infallit innan tillståndet meddelades, vilket kan ha stor betydelse när lagrade uppgifter ska läsas av eller tas upp samt när historiska meddelanden, historiska uppgifter om meddelanden och historiska lokaliseringsuppgifter får läsas av eller tas upp enligt tillståndet. Regleringen motsvarar vad som gäller enligt gällande hemliga tvångsmedelsbestämmelser. Den enskilde domaren är dock oförhindrad att, t.ex. av integritetsskäl, begränsa de uppgifter

som får tas upp även såvitt avser tiden före beslutet. När det gäller tillståndstiden bör det vara möjligt att förlänga ett tillstånd till hemlig dataavläsning enligt samma principer som gäller för övriga hemliga tvångsmedel. Ju fler gånger ett tillstånd förlängs desto högre krav bör ställas vid proportionalitetsprövningen.

I *andra styckets andra punkt* föreskrivs att det i tillståndet ska anges vilket informationssystem tillståndet avser. Ledning vid bestämmande av hur dessa uppgifter ska antecknas kan hämtas från hur bestämmelserna om övriga hemliga tvångsmedel tillämpas. Informationssystemet ska, oavsett vilken typ av informationssystem det är fråga om (se 1 § andra stycket), vara identifierbara, se 5, 7, 9 och 10 §§. Med detta avses exempelvis för elektronisk kommunikationsutrustning t.ex. ett visst serienummer, IMEI-nummer, MAC-adress eller liknande uppgifter. Även mindre specificerade uppgifter torde kunna godtas under förutsättning att de alltjämt möjliggjort prövning av kopplingen mellan informationssystemet och den som åtgärden avser när sådan prövning krävs. Absoluta minimikrav måste vara att åtgärden kan verkställas på grundval av uppgifterna om informationssystemet och att det inte finns någon förväxlingsrisk med andra informationssystem. När det gäller andra typer av informationssystem bör det vara de användarkonton eller andra avgränsade delar av tjänsterna som åtgärden ska anges, t.ex. en e-postadress eller användarnamn till ett konto på en internetbaserad tjänst. Även i dessa fall måste uppgifterna i vart fall kunna användas vid verkställighet och hindra förväxlingsrisk.

I den *tredje punkten* i andra stycket anges att det ska anges i tillståndet vilken typ av uppgift enligt 2 § första stycket tillståndet avser. Med denna avgränsning, som får stor betydelse för vilka anpassningar av verkställighetstekniken som ska göras enligt 19 § första stycket, klargörs för såväl den verkställande myndigheten som för tillsynsmyndigheten både vad åtgärden får användas för och därmed också vilka typer av uppgifter som får läsas av eller tas upp. 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 enligt den punkt som här avses. 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 ska ange vilken uppgiftstyp som ansökan avser.

Enligt *fjärde punkten* i andra stycket ska, när ett platskrav föreligger enligt lagen, den plats som hemlig dataavläsning får verkställas på antecknas i tillståndet. Sådana platskrav föreligger när hemlig dataavläsning ska användas för att läsa av eller ta upp kameraövervakningsuppgifter (2 § första stycket 4) eller rumsavlyssningsuppgifter (2 § första stycket 5), se 4 § första och tredje styckena samt 6 § andra stycket. Att den eller de platser åtgärden får verkställas på ska antecknas i tillståndet är motsvarande krav som gäller för hemlig kameraövervakning och hemlig rumsavlyssning enligt 27 kap. 21 § fjärde stycket rättegångsbalken och, för hemlig kameraövervakning, enligt 8 § tredje stycket preventivlagen. Bestämmelsen ska tillämpas på motsvarande vis som enligt de bestämmelserna. Platsen ska antecknas i tillståndet på ett ändamålsenligt vis.

Enligt den *femte punkten* i andra stycket ska, när avläsning eller upptagning avser rumsavlyssningsuppgifter (2 § första stycket 5) även namnet på den som är skäligen misstänkt anges i tillståndet. Det är motsvarande krav som gäller enligt 27 kap. 21 § femte stycket rättegångsbalken vid tillstånd till hemlig rumsavlyssning.

I bestämmelsens *fjärde stycke* finns motsvarande krav som när tillträdestillstånd har meddelats under förundersökning, nämligen att tillträdestillståndet ska anges i beslutet. Det ligger i sakens natur att platsen som tillträdestillståndet avser således antecknas i tillståndsbeslutet.

Bestämmelsens *avslutande stycke* innehåller krav på att det i beslut om att tillåta hemlig dataavläsning också i övrigt ska anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Sådana villkor som avses kan vara av många och skiftande slag. De kan vara av teknisk karaktär, t.ex. en föreskrift om att den brottsbekämpande myndigheten som ska verkställa åtgärd enligt 2 § första stycket 4 eller 5 måste göra det tekniskt omöjligt att genomföra hemlig dataavläsning på annan plats än tillståndet avser. De kan också vara av annan karaktär, såsom att den brottsbekämpande myndigheten som ska verkställa åtgärd enligt 2 § 4 eller 5 genom fysisk spaning säkerställer att det som i tillståndet föreskrivits avseende plats för verkställighet följs. Vidare kan sådana villkor begränsa de uppgifter som får läsas av eller tas upp, exempelvis genom att det i tillståndet anges att detta avser endast lagrade uppgifter av viss filtyp, viss karaktär eller med viss beteckning. Tillämpningen av stycket kan också ta sikte på att begränsa mängden

överskottsinformation som hämtas in, se prop. 2011/12:55 s. 130. Det går inte, och är inte heller ändamålsenligt, att här uttömmande redogöra för vilka sorts villkor som domstolen kan föreskriva. Det är den enskilde domaren som i det enskilda fallet har bäst förutsättningar att avgöra på vilket sätt ett tillstånd kan avgränsas. Det utrymme som lämnas till domaren att på lämpligaste vis meddela de villkor hen finner nödvändiga är medvetet stort och flexibelt.

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.

I paragrafen finns bestämmelser om möjligheten för åklagaren att fatta interimistiska beslut om hemlig dataavläsning och om rättens prövning av sådana beslut. Övervägandena finns i avsnitt 10.9.5.

I *första stycket* framgår förutsättningarna för att åklagaren ska få meddela ett interimistiskt beslut om hemlig dataavläsning. Förutsättningarna enligt första stycket motsvarar de förutsättningar som gäller för sådana beslut för andra hemliga tvångsmedel enligt 27 kap. 21 a § rättegångsbalken och 6 a § preventivlagen.

En första förutsättning är att *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*. Med uttrycket avses detsamma som enligt reglerna i rättegångs-

balken och preventivlagen, dvs. att det endast är i situationer när ändamålet med åtgärden riskerar att gå förlorat om rättens tillstånd skulle avvaktas som det bör aktualiseras med ett interimistiskt beslut. Möjligheten till interimistiska beslut är således avsedd att tillämpas endast i undantagsfall. Framför allt bör möjligheten tillgripas vid de tidpunkter då det inte går att få en domstolsprövning inom domstolarnas ordinarie öppettider eller inom jourdomstolssystemet. Att inhämta ett domstolsbeslut tar emellertid oundvikligen viss tid, även om behovet av tvångsmedlet uppstår under domstolarnas öppettider. Detta gäller särskilt när det är fråga om ärenden där ett offentligt ombud ska medverka vid handläggningen, vilket alltid är fallet vid hemlig dataavläsning (se nedan i 15 §). Även i sådana fall kan förutsättningar föreligga för ett interimistiskt beslut om ändamålet med åtgärden annars riskerar att gå förlorat.

När förutsättningar för beslut enligt bestämmelsen föreligger *får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut*. Det är således åklagaren som får fatta beslutet att interimistiskt tillåta åtgärden. När åklagaren beslutar om tillstånd till hemlig dataavläsning med stöd av bestämmelsen gäller samma krav på beslutets innehåll som för rättens beslut enligt 13 § andra–femte styckena. Även skyldigheten att, när det finns skäl för det, föreskriva villkor för att tillgodose intresset av att enskildas integritet inte i onödan kränks gäller således för åklagarens beslut.

Av *sista meningen i första stycket* framgår att interimistiska beslut inte får fattas avseende hemlig dataavläsning enligt 2 § första stycket 5 (avläsning eller upptagning av rumsavlyssningsuppgifter) eller vid hemlig dataavläsning i fall som anges i 8 § (LSU-fallen). Det stämmer överens med att det inte är möjligt för åklagare att meddela interimistiska beslut avseende hemlig rumsavlyssning enligt 27 kap. 21 a § rättegångsbalken eller för hemliga tvångsmedel enligt LSU. Interimistiska åklagarbeslut om hemlig dataavläsning får således meddelas i förundersökningsfallen för samtliga uppgiftstyper utom rumsavlyssningsuppgifter samt i preventivlags- och inhämtningslagsfallen. Det följer motsatsvis av sista meningen i första stycket.

Bestämmelsens *andra stycke* är helt överensstämmande med 27 kap. 21 a § andra stycket rättegångsbalken och 6 a § andra stycket preventivlagen och ska tillämpas på samma vis som dessa bestämmelser. Enligt första meningen ska åklagaren, när denne har meddelat interimistiskt tillstånd till hemlig dataavläsning, utan dröjsmål

skriftligt anmäla beslutet till rätten. Att anmälan ska göras utan dröjsmål innebär i princip att den ska göras så snart någon hos domstolen kan ta emot den. Vid interimistiska beslut som meddelas under domstolens öppettider ska anmälan därmed normalt göras i samband med att beslutet meddelas. I övriga fall blir huvudregeln att anmälan ska ske senast i samband med att domstolen åter öppnar. 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.

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. Vid hemlig dataavläsning kan så exempelvis ha skett genom att lagrade uppgifter från ett informationssystem har lästs av eller tagits upp. 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 det emellertid hända att förhållandena har ändrats så att förutsättningar för tvångsmedlet föreligger. Den nu aktuella bestämmelsen hindrar inte att rätten eller åklagaren i sådana fall fattar ett nytt beslut om tillstånd till tvångsmedlet. Inte heller hindrar bestämmelsen att sådana uppgifter, som på grund av rättens beslut inte får användas, hämtas in på nytt med stöd av ett senare meddelat tillstånd, jfr prop. 2013/14:237 s. 182.

Om rätten finner att det saknats skäl för tillstånd (vid tidpunkten för åklagarens prövning), 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. Av 5, 7 och 10 §§ framgår vilka personer som kan utsättas för hemlig dataavläsning. Dessa *omfattas* av åtgärden i den utsträckning som framgår av sista meningen i tredje stycket. När begreppet *någon annan som uppgifterna avser* infördes i 27 kap. 21 a § rättegångsbalken användes i förarbetena som exempel den situationen att ett tvångsmedelstillstånd avser A, som avlyssnas när denne samtalar med B om brottslig verksamhet där enligt uppgifter vid samtalet även C, som inte själv utsatts för avlyssningen, medverkat. Uppgifterna från avlyssningen får i det fallet, om domstolen finner att det saknats skäl för åtgärden, inte användas i en brottsutredning till nackdel för vare sig A, B eller C (prop. 2013/14:237 s. 183). Exemplet kan användas även i hemlig dataavläsningsfallet. Med någon annan som uppgif-

terna avser inkluderas också en person som omnämns i inhämtade dokument eller som syns på inhämtade videor eller fotografier när hemlig dataavläsning avsett lagrade uppgifter.

Att uppgifterna enligt vad som föreskrivs i bestämmelsen *inte får användas i en brottsutredning* avser användning både i en förundersökning och i motsvarande utredning enligt 23 kap. 22 § rättegångsbalken.

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.

I paragrafen finns bestämmelser om sammanträde och offentliga ombud vid domstolsprövningen av hemlig dataavläsning samt om handläggningen av ärenden om hemlig dataavläsning. Övervägandena finns i avsnitt 10.9.6.

I *första stycket* framgår att ett offentligt ombud alltid ska närvara vid domstolsprövningen av ansökan om hemlig dataavläsning. Detta kan sägas utgöra en utvidgning jämfört med andra hemliga tvångsmedelsbestämmelser eftersom offentliga ombud annars inte närvarar i ärenden som gäller hemlig övervakning av elektronisk kommunikation eller vid prövningen av inhämtning enligt inhämtningslagen. När det gäller hemlig dataavläsning finns emellertid inga undantag. Domstolens skyldighet är att så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde.

Vid ett sammanträde enligt första stycket ska den som gjort ansökan, och det offentliga ombudet närvara. *Den som gjort ansökan* är åklagaren i alla fall utom i LSU-fallen. Då är det i stället Polis-

myndigheten eller Säkerhetspolisen som ansöker om tillstånd, se 13 § första stycket.

I andra stycket anges att för offentliga ombud gäller 27 kap. 26 och 27 §§, 28 § andra stycket samt 29 och 30 §§ rättegångsbalken. Anledningen till att 28 § första stycket inte räknas upp är att första stycket i förevarande bestämmelse gäller i stället för den. Det offentliga ombudet ska i enlighet med vad som anges i 27 kap. 26 § rättegångsbalken bevaka enskildas integritetsintressen i ärenden hos domstol 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 § rättegångsbalken gäller för offentliga ombud även enligt denna lag. Enligt 27 kap. 28 § andra stycket rättegångsbalken gäller ett uppdrag som offentligt ombud även i högre rätt. Även reglerna om ersättning till det offentliga ombudet och om sekretess i 27 kap. 29 och 30 §§ rättegångsbalken gäller således även för offentliga ombud enligt denna lag.

I *tredje stycket* finns förfaranderegler. Enligt dessa 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 lagen. Det innebär bl.a. att domstolens beslut om hemlig dataavläsning är ett slutligt beslut som kan överklagas enligt 49 kap. 3 § första stycket rättegångsbalken. 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 rättegångsbalken framgår att hovrätten kan inhibera verkställigheten vid ett överklagande. Därtill ger den föreslagna regleringen besked till den prövande domstolen vad som ska gälla såvitt avser hantering av ärendet innan och efter sammanträde, dvs. ärendet ska hanteras på samma vis som sker beträffande övriga hemliga tvångsmedelsärenden.

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.

I paragrafen finns bestämmelser om omedelbar verkställighet och omedelbart upphävande av beslut om tillstånd till hemlig dataavläsning. Övervägandena finns i avsnitt 10.9.7.

I *första stycket* föreskrivs att beslut i frågor om hemlig dataavläsning får verkställas omedelbart. Det hänger samman med att 30 kap. 12 § rättegångsbalken inte är direkt tillämplig på lagen.

I *andra stycket* anges det självklara att om det inte längre finns skäl för ett tillstånd till hemlig dataavläsning så ska beslutet om tillstånd omedelbart upphävas. Det är den som ansökt eller rätten som ska upphäva beslutet. Med *den som ansökt* avses åklagaren eller, i förekommande fall, Polismyndigheten eller Säkerhetspolisen, se kommentaren till 13 § första stycket. Ett särskilt fall som kan uppstå vid hemlig dataavläsning är att det efter tillståndsprövningen visar sig att det informationssystem tillståndet avser är ett ”förbjudet” informationssystem enligt 11 §. Då finns inte längre skäl för tillståndet och åtgärden ska omgående avbrytas.

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 också, om det är nödvändigt för att verkställighet ska kunna ske, använda tekniska hjälpmedel i det informationssystem tillståndet avser.

I paragrafen finns regler om verkställighet av hemlig dataavläsning. Övervägandena finns i avsnitt 10.10.1.

I *första stycket* framgår att de tekniska hjälpmedel som behövs för hemlig dataavläsning får användas vid verkställighet, dvs. vid själva avläsningen eller upptagningen av de uppgifter som tillståndet avser. Det är motsvarande bestämmelse som gäller vid verkställighet av hemlig avlyssning eller övervakning av elektronisk kommunikation enligt 27 kap. 25 § rättegångsbalken. Av förarbetena till den bestämmelsen framgår att med tekniska hjälpmedel avses både programvara och hårdvara, se prop. 1994/95:227 s. 29. Genom sin neutrala lydelse lämnas den verkställande myndigheten stor frihet att avgöra vilken teknik som ska användas i det enskilda fallet och om det tekniska hjälpmedlet ska finnas i eller utanför informationssystemet. I 20 § föreskrivs dock om aktsamhetskrav som kan sägas begränsa de tekniska hjälpmedel som får användas.

I paragrafens *andra stycke* finns en bestämmelse om vad den verkställande myndigheten får göra för att kunna verkställa ett tillstånd till hemlig dataavläsning. Det första stycket behandlar alltså själva avläsningen eller upptagningen medan förevarande stycke reglerar stadier innan avläsning eller upptagning sker, vilket är nödvändigt för att tydliggöra vilka åtgärder som behöver vidtas inför verkställighet.

Enligt andra stycket får förberedande åtgärder vidtas inom ramen för ett beslutat tillstånd *om det är nödvändigt för att verkställighet ska kunna ske*. En prövning av detta rekvisit måste göras av den verkställande myndigheten innan verkställighet påbörjas. Andra stycket gäller, liksom det första, *när tillstånd har lämnats*. Det innebär att de åtgärder som tas upp i stycket inte får vidtas med stöd av bestämmelsen dessförinnan.

Om det är nödvändigt för att verkställighet ska kunna ske får den verkställande myndigheten *bryta eller kringgå systemskydd och utnyttja tekniska sårbarheter*. 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 för att kunna verkställa hemlig dataavläsning, se avsnitt 8.4.1. Ramen för de åtgärder som får vidtas sätts av den kursiverade lydelsen.

Den verkställande myndigheten får också *använda tekniska hjälpmedel i det informationssystem tillståndet avser,* vilket kan vara nödvändigt för att kunna verkställa beslut om hemlig dataavläsning

som avser upptagning av lokaliserings-, kameraövervaknings- eller rumsavlyssningsuppgifter (2 § första stycket 3–5). I sådana fall kan den brottsbekämpande myndigheten få aktivera t.ex. kamera-, mikrofon- eller GPS-funktion i informationssystemet. Med använda avses såväl aktivering av programvara som finns i informationssystemet eller installation av annan programvara, t.ex. den som ska användas för verkställigheten.

Det bör tilläggas att bestämmelsen inte utesluter att mer än en teknik används vid och innan verkställighet eller att tekniker eller metoder enligt både första och andra stycket används. När tillstånd till hemlig dataavläsning har meddelats utgör det inte ett dataintrång när tekniker eller tillvägagångssätt som nämns i bestämmelsen används i samband med verkställighet av åtgärden.

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.

Av bestämmelsen framgår den medverkansmöjlighet som gäller för vissa privaträttsliga aktörer. Övervägandena finns i avsnitt 10.12.2.

I bestämmelsens *första stycke* slås fast att det finns möjlighet för den som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § lagen om elektronisk kommunikation att lämna den verkställande myndigheten sådant bistånd som behövs i samband med verkställighet. Hänvisningen till bestämmelsen i lagen om elektronisk kommunikation 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.

Det anges inte vad biståndet kan avse men som exempel har framhållits att det kan handla om att en operatör bistår med att identifiera

vilka tjänster en specifik användare har, identifiera vilka förbindelser som används, rådgivning avseende vilka tekniska hjälpmedel som kan användas, tillhandahållande av möjlighet att installera brottsbekämpande myndigheters tekniska hjälpmedel i operatörens nät för verkställighet eller hjälp med andra liknande stödåtgärder, se vidare avsnitt 10.12.2.

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 kan förväntas uppstå torde främst vara hänförliga till nedlagd tid hos den medverkande. Även kostnader för att t.ex. upplåta utrymme, som inte är hänförliga till tidsåtgång utan till själva upplåtandet, torde kunna uppstå. I första hand är det direkta kostnader, liknande de som nu angetts, som ska ersättas enligt bestämmelsen. Även vid medverkan som sedan inte leder till en genomförd verkställighet bör ersättningsrätt enligt bestämmelsen föreligga om kostnader uppstått.

Det anges inte hur ersättningsfrågan ska regleras utan det förväntas att den som medverkat och den brottsbekämpande myndigheten hittar lösningar i dessa frågor.

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.

I paragrafen finns bestämmelser om anpassning av verkställighetstekniken och vad som ska gälla om tillräcklig anpassning av den inte vidtagits. Övervägandena finns i avsnitt 10.10.2.

I *första stycket* klargörs den anpassningsskyldighet avseende verkställighetstekniken som föreligger för den verkställande myndigheten vid hemlig dataavläsning. Den teknik som ska vara anpassad enligt bestämmelsen är sådan som används *i samband med verkställighet*, vilket innefattar såväl första som andra stycket i 17 §. Bestämmelsen har tillkommit för att begränsa riskerna för den personliga integriteten när hemlig dataavläsning används. I bestämmelsen regleras inte hur anpassning ska ske, endast att så måste ske. Det blir en fråga för i första hand den verkställande myndigheten och i andra hand tillsynsmyndigheten, inom ramen för sin tillsynsverksamhet, att avgöra om de anpassningar som gjorts är eller varit tillräckliga för att nå upp till lagens krav.

Anpassningsskyldigheten innebär att tekniken som används i samband med verkställighet inte ska möjliggöra avläsning eller upptagande av *någon annan typ av uppgift* än sådan som tillståndet tillåter. Typ av uppgift har samma innebörd som i 2 § första stycket, se kommentaren till den bestämmelsen. Av 13 § andra stycket 3 följer att det i tillståndet ska anges vilken uppgiftstyp som det avser. Överskottsinformation omfattas således inte av bestämmelsen (se i stället 23-27 §§).

Med att det inte ska vara *möjligt* avses den faktiska möjligheten i det enskilda fallet. Det innebär att om tillståndet exempelvis tillåter hemlig dataavläsning för att läsa av eller ta upp uppgifter enligt 2 § första stycket 1 (kommunikationsavlyssningsuppgifter) så ska det inte vara *faktiskt möjligt* att med den teknik som används läsa av eller ta upp lagrade uppgifter. Det ska då inte heller vara *faktiskt möjligt* att läsa av eller ta upp kameraövervakningsuppgifter eller rumsavlyssningsuppgifter. Om ett tekniskt hjälpmedel är konstruerat så att det i och för sig vore möjligt att med det läsa av eller ta upp olika uppgiftstyper krävs, för att det inte ska anses möjligt i lagens mening, att hjälpmedlet är inställt på ett sådant sätt att det inte är praktiskt möjligt att utan ändringar av inställningarna i hjälpmedlet komma åt andra uppgiftstyper än de som tillståndet avser. Möjligheten till avläsning eller upptagning bestäms i de fallen utifrån vilka funktionaliteter som är på- respektive avslagna i det tekniska hjälpmedlet.

En särskild regel om vad som ska gälla om uppgifter av annan uppgiftstyp, trots anpassningsskyldigheten, lästs av eller tagits upp (otillåten tilläggsinformation) finns i *andra stycket.* Om otillåten tilläggsinformation lästs av eller tagits upp ska upptagningar av dessa uppgifter omedelbart förstöras och Säkerhets- och integritetsskyddsnämnden underrättas. Anledningen till det hårda kravet är att insamlingen av uppgifter i detta fall varit olaglig, eftersom den ju inte har omfattats av tillståndet. Skälet till att tillsynsmyndigheten ska underrättas är för att den ska få kännedom om felet och därmed kunna rikta sin tillsyn eller vidta de andra åtgärder den finner nödvändiga.

I *tredje stycket* finns en bestämmelse som motsvarar vad som gäller enligt 14 § tredje stycket när hemlig dataavläsning har verkställts efter ett interimistiskt åklagartillstånd som domstolen sedan anser inte borde ha meddelats, nämligen att uppgifter som framkommit vid felaktig avläsning eller upptagning inte får användas i en brottsutredning till nackdel för den som omfattats av åtgärden eller för någon annan som uppgifterna avser. Det som anfördes i kommentaren till 14 § tredje stycket sista meningen gäller därför även här.

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.

I paragrafen föreskrivs aktsamhetsregler, dels generella sådana, dels specifika aktsamhetsregler som tar sikte på informationssäkerhet. Övervägandena redovisas i avsnitt 10.10.3.

I *första stycket* finns 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 § sista stycket rättegångsbalken och vid husrannsakan i 28 kap. 6 § första stycket rättegångsbalken. I förarbetena till den förstnämnda bestämmelsen angavs att den kan få betydelse t.ex. i fråga om hur tillträdet ska ske till den plats som ska avlyssnas eller på vilket sätt utrustningen ska installeras, se prop. 2005/06:178 s. 107. Uttalandet har skäl för sig även vid hemlig dataavläsning. Regeln är dock inte bara tillämplig i det fysiska rummet utan också i det virtuella eller digitala rum som hemlig dataavläsning kan verkställas i. 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 alls uppstår, men föreskriver att sådan måste vara *absolut nödvändig*. Det finns skäl att påpeka att ändamåls-, behovs- och proportionalitetsprincipen gäller även i verkställighetsstadiet.

I *andra stycket* finns en mer specifikt inriktad aktsamhetsregel som tar sikte på informationssäkerhet. Begreppet *informationssäkerhet* ska tolkas brett och omfatta de kriterier som NISU-utredningen anförde avseende informationssäkerhet i betänkandet *Informations- och cybersäkerhet* (SOU 2015:23 s. 42):

– Informationen finns alltid när den behövs (tillgänglighet).

– Det går att lita på att informationen är korrekt och inte manipulerad eller förstörd (riktighet).

– Endast behöriga personer får ta del av informationen (konfidentialitet).

– Det går att följa hur och när informationen har hanterats och kommunicerats (spårbarhet).

I begreppet informationssäkerhet när det används i detta sammanhang innefattas också nät- och cybersäkerhet.

Det som andra stycket tar sikte på är informationssäkerhet utanför informationssystemet som tillståndet avser. Med *utanför* menas allt som inte utgörs av informationssystemet, se kommentaren till 1 §. När ett tillstånd till hemlig dataavläsning avser elektronisk kommunikationsutrustning (1 § andra stycket 1) är exempel på

det som finns utanför informationssystemet det nät som utrustningen är ansluten till eller annan utrustning som kopplats ihop med kommunikationsutrustningen (och som inte utgör en del av den). När det är fråga om tillstånd till hemlig dataavläsning som avser användarkonton eller på motsvarande sätt avgränsade delar av kommunikationstjänster, lagringstjänster eller liknande tjänster (1 § andra stycket 2) utgör allt som inte ryms inom definitionen sådant som finns *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 bestämmelsen.

Andra stycket riktar sig till *den som ansvarar för verkställighet.* Genom begreppet framgår att det alltid ska finnas en ansvarig person för varje verkställighetsärende. Regler om vem som kan utses till sådan ansvarig person finns i 31 §.

Den ansvariga personen ska vidta *nödvändiga och tillräckliga* åtgärder för att informationssäkerheten utanför det informationssystem tillståndet avser inte ska *åsidosättas, minskas eller skadas till följd av verkställigheten*. Hur detta ska gå till framgår inte av bestämmelsen utan är upp till den ansvarige själv. Det kommer att kunna skilja från fall till fall hur omfattande åtgärder som ska vidtas och om åtgärderna ska vara av teknisk eller annan karaktär. Viktigt är att den bortre gränsen för ansvaret utgörs av att det endast är *till följd av verkställigheten* som informationssäkerheten inte får påverkas. Det innebär att allt som inte är hänförligt till själva verkställigheten faller utanför ansvarsområdet. Samtliga de tekniska metoder som anges i 17 §, dvs. även sådana som enligt den bestämmelsens andra stycke behövs för att verkställighet ska kunna ske, innefattas i begreppet *till följd av verkställigheten*. Det är i första hand den verkställighetsansvarige och i andra hand tillsynsmyndigheten som kontrollerar efterlevnaden av bestämmelsen.

I *tredje stycket* finns också bestämmelser som tar sikte på bl.a. informationssäkerhet. Dessa gäller dock själva informationssystemet 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. Eftersom det är möjligt att bryta eller kringgå systemskydd, se 17 § andra stycket, kan det förekomma att informationssäkerheten i det infor-

mationssystem tillståndet avser minskas. Det utesluts alltså inte, men måste vara absolut nödvändigt. Vad förevarande stycke emellertid tar sikte på är att den brottsbekämpande myndigheten när verkställighet av hemlig dataavläsning avslutas inte ska lämna informationssystemet i sämre, dvs. mindre säkert, skick än när verkställigheten påbörjades. Detta uttrycks genom att den verkställande myndigheten åläggs en skyldighet att se till att säkerheten i informationssystemet ska hålla åtminstone samma nivå som vid verkställighetens början. Genom uttrycket *åtminstone* följer att den brottsbekämpande myndigheten är oförhindrad att öka säkerheten i systemet när detta är möjligt. Hur skyldigheten enligt stycket ska fullgöras förklaras inte och kan skilja sig från fall till fall. I första hand är det den verkställande myndigheten och i andra hand tillsynsmyndigheten som kontrollerar efterlevnaden av bestämmelsen.

I det avslutande *fjärde stycket* framgår 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. Motsvarande bestämmelse finns i 27 kap. 25 a § fjärde stycket. Det är neutralt utformat hur den brottsbekämpande myndigheten ska fullgöra sin skyldighet enligt bestämmelsen. Innebörden är dock helt klar. Det ska inte vara möjligt för den verkställande myndigheten, eller någon annan, att efter det att tillståndstiden har löpt ut (eller åtgärden avbrutits i förtid) kunna utnyttja samma verktyg igen. För att tillgodose kravet bör det exempelvis vara möjligt för den brottsbekämpande myndigheten att ”tidsinställa” det tekniska hjälpmedel som används.

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.

I paragrafen finns en bestämmelse om vad som ska gälla för uppgifter som skyddas genom den s.k. beslagsförbudsregeln. Övervägandena finns i avsnitt 10.7.3.

Bestämmelsen knyter genom hänvisningen till 27 kap. 2 § första stycket rättegångsbalken an till det s.k. beslagsförbudet i rättegångsbalken. Dess utformning innebär att uppgifter som är en del av en fil eller annan informationsenhet (se NJA 2015 s. 631 p. 25 och 26) som inte skulle ha fått tas i beslag inte heller får läsas av eller tas upp genom hemlig dataavläsning.

I *första stycket* avhandlas vad som ska gälla om det kommer fram att det är fråga om beslagsförbudsskyddade uppgifter, nämligen att avläsningen omedelbart ska avbrytas. I *andra stycket* regleras vad som ska gälla om upptagning skett av uppgifter som skyddas av skyddet enligt beslagsförbudsregeln, nämligen att upptagningen ska förstöras. Av dessa regler följer att uppgifterna inte kan användas i den fortsatta utredningen.

De uppgifter det kan vara fråga om är sådana som en befattningshavare eller någon annan som avses i 36 kap. 5 § rättegångsbalken inte får höras som vittne om och som innehas av honom eller henne eller av den som tystnadsplikten gäller till förmån för. Det innebär motsatsvis att i den mån tystnadsplikt enligt 36 kap. 5 § rättegångsbalken inte gäller för uppgiften, t.ex. i vissa fall när det är fråga om grövre brott eller vid medgivande enligt det lagrummet, föreligger normalt inte hinder mot beslag. I de fallen ska heller inte den här föreslagna regeln innebära förbud mot att läsa av eller ta upp uppgifterna, vilket är naturligt eftersom det ju då inte skulle råda något beslagsförbud.

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.

I paragrafen regleras det s.k. avlyssningsförbudet. Övervägandena finns i avsnitt 10.7.4.

Bestämmelsen motsvarar vad som anges i 27 kap. 22 § rättegångsbalken. Det finns tre skillnader av närmast redaktionell karaktär mellan rättegångsbalkens bestämmelse och förevarande bestämmelse. Den första är att det i förevarande bestämmelse anges att det är hemlig dataavläsning enligt 2 § första stycket 1 och 5 som åtgärden avser i stället för hemlig avlyssning av elektronisk kommunikation och hemlig rumsavlyssning. Den andra är att det är avläsning i stället för avlyssning som regleras. Den tredje är att det är uppgifterna – och alltså inte meddelandena eller samtalen eller talen som åtgärden inte får avse. I alla tre avseenden är det rent språkliga skillnader jämfört med vad som gäller enligt rättegångsbalken som behövs för att stämma in i den struktur som används i förevarande lag. I sak ska avläsningsförbudet enligt förevarande bestämmelse vara av samma innebörd som avlyssningsförbudet enligt 27 kap. 22 § rättegångsbalken och, såvitt avser hemlig avlyssning av elektronisk kommunikation, enligt 11 § preventivlagen. Det hänvisas därför till de förarbetsuttalanden som gjorts vid införande av de bestämmelserna, se prop. 1989/90:124 s. 46 f., 2005/06:177 s. 90 f., 2005/06:178 s. 102 f., prop. 2009/10:119 s. 27 f. och 2013/14:237 s. 184.

Genom sin placering och utformning gäller bestämmelsen vid samtliga tillfällen då hemlig dataavläsning används enligt 2 § första stycket 1 eller 5, dvs. både under och före förundersökning.

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.

I paragrafen anges vad som ska gälla bl.a. beträffande hur överskottsinformation får användas, hur granskning av upptagningar ska gå till och hur och när enskild ska underrättas om åtgärden när den används i förundersökning. Övervägandena finns i avsnitt 10.11.

I *första styckets första mening* klargörs att de regler som gäller för hemlig avlyssning av elektronisk kommunikation under förundersökning i frågor som rör användning av överskottsinformation och granskning av upptagningar görs direkt tillämpliga även för hemlig dataavläsning genom hänvisningar till rättegångsbalkens regler. I *andra meningen* finns ett undantag som innebär att när hemlig dataavläsning används eller har använts för att läsa av eller ta upp rumsavlyssningsuppgifter (2 § första stycket 5) så gäller i stället rättegångsbalksreglerna om användning av överskottsinformation (27 kap. 23 a § andra stycket) och behandling av uppgifter (27 kap. 24 § tredje stycket) vid hemlig rumsavlyssning.

I *andra stycket* finns regler om underrättelse till enskild. Genom en direkt hänvisning blir samma regler som används vid annan tvångsmedelsanvändning under förundersökning tillämpliga. Eftersom hemlig dataavläsning inte anges i de bestämmelserna förtydligas

i andra styckets andra mening att det som anges om hemlig avlyssning av elektronisk kommunikation i 27 kap. 31–33 §§ alltid ska tillämpas vid hemlig dataavläsning, dvs. oberoende av vilka uppgifter åtgärden använts för att läsa av eller ta upp enligt 2 § första stycket. I bestämmelsens sista mening förtydligas att när kameraövervakningsuppgifter eller rumsavlyssningsuppgifter har lästs av eller tagits upp med hemlig dataavläsning enligt 2 § första stycket 4 eller 5 så ska beträffande underrättelsen också det som gäller för hemlig kameraövervakning eller hemlig rumsavlyssning tillämpas. Det innebär bl.a. att innehavaren av den plats som tillståndet avsett typiskt sett ska underrättas.

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.

I paragrafen anges vad som ska gälla beträffande hur överskottsinformation får användas, hur granskning av upptagningar ska gå till och hur och när enskild ska underrättas om åtgärden när hemlig dataavläsning används i preventivlagsfallen. Övervägandena finns i avsnitt 10.11.

I *första stycket* klargörs att de regler som gäller enligt preventivlagen i frågor som rör användning av överskottsinformation och granskning av upptagningar genom hänvisningar görs direkt tillämpliga även för hemlig dataavläsning i preventivlagsfallen. Kraven enligt den lagen är liknande de som gäller enligt rättegångsbalken men ger färre möjligheter att använda överskottsinformationen, se prop. 2013/14:237 s. 199. Det föreskrivs inte, som i 23 §, att det är det som

gäller för hemlig avlyssning av elektronisk kommunikation som ska gälla eftersom preventivlagen i nu aktuella avseenden inte gör skillnad mellan de olika tvångsmedlen som används i den lagen.

I *andra stycket* finns regler om underrättelse till enskild vid hemlig dataavläsning i preventivlagsfallen. Genom en direkt hänvisning blir samma regler som används vid annan tvångsmedelsanvändning enligt preventivlagen tillämpliga. Eftersom hemlig dataavläsning inte anges i de bestämmelserna det hänvisas till förtydligas i andra styckets andra mening att det som anges om hemlig avlyssning av elektronisk kommunikation i 16–18 §§ preventivlagen alltid ska tillämpas vid hemlig dataavläsning, dvs. oberoende av vilka uppgifter åtgärden använts för att läsa av eller ta upp enligt 2 §. I bestämmelsens sista mening förtydligas att när kameraövervakningsuppgifter har lästs av eller tagits upp med hemlig dataavläsning enligt 2 § första stycket 4 så ska beträffande underrättelsen också det som gäller för hemlig kameraövervakning tillämpas. Det innebär bl.a. att innehavaren av den plats som tillståndet i den delen avsett typiskt sett ska underrättas. Det ska påpekas att underrättelseskyldigheten enligt preventivlagen begränsas genom att det endast är när åtgärd vidtas enligt en av sju punkter i den lagens brottskatalog som underrättelse ska lämnas. Samma ska således gälla vid hemlig dataavläsning.

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.

I paragrafen förtydligas vissa begrepp. Övervägandena finns i avsnitt 10.11.

Genom bestämmelsen tydliggörs att när de bestämmelser som det hänvisas till i 23 och 24 §§ blir tillämpliga enligt lagen ska begreppen *telefonnummer* eller *annan adress* eller en *viss elektronisk kommunikationsutrustning* inte användas. I stället ska begreppet *informationssystem*, som används i denna lag, användas.

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.

I paragrafen anges vad som ska gälla beträffande hur överskottsinformation får användas och hur granskning av upptagningar ska gå till när hemlig dataavläsning används i LSU-fallen. Övervägandena finns i avsnitt 10.11.

I bestämmelsen klargörs att de regler som gäller enligt LSU i frågor som rör användning av överskottsinformation och granskning av upptagningar genom hänvisningar görs direkt tillämpliga även för hemlig dataavläsning i LSU-fallen.

Det finns inte några regler om underrättelseskyldighet i LSU, se prop. 2006/07:133 s. 52. Därför finns inte något andra stycke motsvarande strukturen i 23 och 24 §§.

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.

I paragrafen anges vad som ska gälla beträffande hur överskottsinformation får användas och hur granskning av upptagningar ska gå till när hemlig dataavläsning används i inhämtningslagsfallen. Övervägandena finns i avsnitt 10.11.

I bestämmelsen klargörs att de regler som gäller enligt inhämtningslagen i frågor som rör användning av överskottsinformation och granskning av upptagningar genom hänvisningar görs direkt tillämpliga även för hemlig dataavläsning i inhämtningslagsfallen.

Underrättelse till enskild aktualiseras inte vid inhämtning enligt inhämtningslagen, och inte heller i förevarande bestämmelse.

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 2–8 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.

Paragrafen anger vilka domstolar som är behöriga att pröva frågor om tillstånd till hemlig dataavläsning. Övervägandena finns i avsnitt 10.9.2.

Forumreglerna som anges i bestämmelsen följer befintliga forumregler, både avseende förundersöknings- och underrättelsefallen (dock ej inhämtning enligt inhämtningslagen). Det innebär enligt *första stycket* att när förundersökning pågår så är det 19 kap. rättegångsbalken som anvisar vilken domstol som är behörig. Som huvudregel gäller enligt dessa regler att rätten i den ort där brottet förövades är behörig. Om det är lämpligt, får prövningen i stället ske 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 §§). Mot bakgrund av att det i 27 kap. 34 § rättegångsbalken finns en alternativ forumregel avseende brottslighet som avses i 27 kap. 2 § andra stycket 2–8 rättegångsbalken (samhällsfarlig brottslighet) införs motsvarande alternativa forumregel här. I sådana fall är således Stockholms tingsrätt alltid behörig att pröva frågan.

När det gäller underrättelsefallen framgår av *andra stycket* att Stockholms tingsrätt är exklusivt forum. Detta är samma som gäller i dag enligt preventivlagen och LSU. Mot bakgrund särskilt av underrättelsefallens särpräglade natur och det begränsade antal verkställighetstillfällen det lär bli fråga om är Stockholms tingsrätt också exklusivt forum när det är fråga om tillståndsprövning av åtgärd i inhämtningslagsfallen, dvs. när ansökan om hemlig dataavläsning grundas på 10 §.

Underrättelse till Säkerhets- och integritetsskyddsnämnden

29 §

När ett tillstånd till hemlig dataavläsning har lämnats ska rätten underrätta Säkerhets- och integritetsskyddsnämnden om beslutet.

I paragrafen föreskrivs skyldigheter för domstol att underrätta Säkerhets- och integritetsskyddsnämnden. Övervägandena finns i avsnitt 10.12.1.

Enligt bestämmelsen, som kommit till som en följd av de risker för såväl den personliga integriteten som för informationssäkerheten som kan uppstå om hemlig dataavläsning används på fel sätt, ska domstolen när en fråga om tillstånd till hemlig dataavläsning har prövats underrätta Säkerhets- och integritetsskyddsnämnden. Bestämmelsen ger tillsynsmyndigheten en indikation på att hemlig dataavläsning kommer att användas och således också en möjlighet att i tidigare skede än vad som annars torde vara fallet, dvs. redan under pågående verkställighet, utöva sin tillsyn. En sådan tidig tillsyn torde många gånger vara nödvändig för att upptäcka tekniska brister vid verkställighet i förhållande till lagens krav och för att skaffa sig en faktisk uppfattning av om huruvida den verkställande myndigheten vidtar de tämligen omfattande åtgärder som lagen föreskriver vid verkställighet (se t.ex. 19 och 20 §§). Bestämmelsen är begränsad till meddelade tillstånd och innebär att det endast är i de fallen, och alltså inte när en ansökan har avslagits, som underrättelse ska ske.

I bestämmelsen anges att underrättelsen ska ske när frågan har prövats. Det ligger i sakens natur att underrättelse bör ske i tämligen nära anslutning till beslutstillfället, kanske någon dags fördröjning kan accepteras. Det får alltså inte dröja veckor innan Säkerhets- och integritetsnämnden underrättas. I så fall kan en del av själva syftet med bestämmelsen gå om intet. Formen för underrättelsen framgår inte av bestämmelsen. Det innebär att den kan ske på lämpligt vis, antingen muntligen eller skriftligen.

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.

I paragrafen föreskrivs om tystnadsplikt för personer som i viss verksamhet fått del av uppgifter om hemlig dataavläsning. Övervägandena finns i avsnitt 10.12.3.

Bestämmelsen anger för vem och avseende vilka uppgifter tystnadsplikt gäller. Den är utformad med ledning av 6 kap. 20 och 21 §§ lagen om elektronisk kommunikation. Med uttrycket *den som i samband med*, som anges i inledningen av *första stycket*, klargörs att vem som helst kan omfattas av tystnadsplikten, så länge hen fått del av eller tillgång till uppgifterna i samband med sådan tillståndspliktig verksamhet som avses i bestämmelsen. Typiskt sett torde det vara personer som är eller har varit verksamma i sådan verksamhet, antingen genom anställning eller genom uppdrag av eller hos företag. 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 således vara hänförliga till exempelvis tekniken som används vid verkställighet, personen som ska bli föremål för åtgärd, informationssystemet som innehåller uppgifterna som ska läsas av eller den brottsbekämpande myndigheten som ansvarar för verkställighet. Någon uttömmande exemplifiering av vilka uppgifter som kan omfattas är inte möjlig och inte heller ändamålsenlig. Genom ordalydelsens breda omfång är tanken i stället att varje uppgift som direkt eller indirekt gäller användning av hemlig dataavläsning ska omfattas.

Innebörden av tystnadsplikten är att den som tystnadsplikten gäller för inte obehörigen får föra vidare eller utnyttja det hen fått del av eller tillgång till. Ordalydelsen innebär således att denne varken genom tal eller i skrift får föra uppgifterna vidare. Hen får inte heller

exempelvis utnyttja uppgifter om verkställighetstekniken som hen fått kännedom om.

I *andra stycket* påminns om de straffbestämmelser som gäller för den som bryter mot tystnadsplikten, se 20 kap. brottsbalken.

I 44 kap. 5 § 5 offentlighets- och sekretesslagen införs en bestämmelse som innebär att den grundlagsstadgade rätten att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som föreskrivs i förevarande bestämmelse.

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 för uppdraget.

I paragrafen anges vem som utser personer som får ansvara för verkställighet av hemlig dataavläsning och vilka krav som ska ställas på sådana personer. Övervägandena finns i avsnitt 10.12.4.

I *första stycket* framgår att det är den verkställande myndigheten som utser personer som får ansvara för verkställighet av hemlig dataavläsning. De myndigheter som kan komma i fråga för att verkställa hemlig dataavläsning är Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket. Vilken myndighet som får använda hemlig dataavläsning bestäms i varje given situation av det brott som är för handen, de förutsättningar som följer av lagen och av instruktionerna för de angivna myndigheterna. Att beslutanderätten ligger hos *myndigheten* innebär att det är myndighetschefen, eller den som myndighetschefen utser, som får fatta beslutet.

Av *andra stycket* framgår de grundläggande kvalifikationskraven som ska gälla för den som ska utses som ansvarig för att verkställa hemlig dataavläsning. Av dessa framgår först att den som ska utses ska ha de särskilda kunskaper om informationssäkerhet som behövs. Kravet ställs upp först eftersom det är centralt, främst mot bakgrund

av de särpräglade tekniska metoder som verkställighet av hemlig dataavläsning kan aktualisera, de risker som kan uppstå för informationssäkerheten med dessa och de krav på anpassning av verkställighetsteknikerna som föreskrivs i lagen. Med *särskilda kunskaper om informationssäkerhet* avses såväl utbildning och erfarenhet på området. Till detta krav kommer kraven att den som utses ska ha särskild kompetens, utbildning och erfarenhet som är nödvändig. Dessa krav kan ta sikte på den verksamhet som personen ska verka i liksom på andra faktorer än kunskaper om informationssäkerhet. Som ett avslutande krav gäller att personen i fråga även i övrigt ska vara särskilt lämpad för uppdraget.

13.2 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 prövningsrätt vid sådana förhållanden som lagen avser. Övervägandena finns i avsnitt 10.12.5.

Ett tillägg görs i bestämmelsens första stycke som innebär att åklagaren får meddela interimistiskt beslut om hemlig dataavläsning för att läsa av eller ta upp rumsavlyssningsuppgifter enligt 2 § första stycket 5 lagen om hemlig dataavläsning om förutsättningarna som krävs enligt bestämmelsen och lagen i övrigt är uppfyllda. Genom

detta tillägg uppnås överensstämmelse för den åtgärden med vad som gäller för hemlig rumsavlyssning.

13.3 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, hemlig övervakning 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. *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 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.

I paragrafen regleras vilka åtgärder som omfattas av lagen. Övervägandena finns i avsnitt 11.2.3.

I den förteckning som framgår av bestämmelsens *första stycke* tas hemlig dataavläsning upp som en åtgärd som omfattas av lagen. Åtgärden placeras i punkt 11 och får till följd att de åtgärder som framgick i de tidigare punkterna 11 och 12 får ny numrering och därmed att den nya punkten 13 införs.

I övrigt lämnas paragrafen oförändrad.

2 kap.

1 §

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 *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 11.2.3.

I *första stycket* klargörs genom den nya hänvisningen till 1 kap. 2 § första stycket 11 att rättslig hjälp med hemlig dataavläsning 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. Således ska både förutsättningarna enligt lagen om hemlig dataavläsning och förevarande lag tillämpas vid prövningen. Som följdändringar av att de två sista punkterna i 1 kap. 2 § första stycket har fått ny numrering tas den nya punkten 13 upp i första stycket i stället för punkt 12 och punkt 12 i *andra stycket* i stället för punkt 11.

I övrigt lämnas paragrafen oförändrad.

2 kap.

2 §

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.

I paragrafen regleras frågor om när dubbel straffbarhet uppställs som krav för rättslig hjälp. Övervägandena finns i avsnitt 11.2.3.

Genom hänvisningen i bestämmelsen till punkt 11 framgår att det krävs dubbel straffbarhet, dvs. att den gärning som ansökan avser motsvarar ett brott enligt både svensk lag och enligt lagen i den stat där åtgärden behövs, för att rättslig hjälp med åtgärden ska få lämnas. Som följdändringar av att de två sista punkterna i 1 kap. 2 § första stycket har fått ny numrering tas den nya punkten 13 upp, i stället för punkt 12, som en åtgärd för vilken det krävs dubbel straffbarhet och punkt 12, i stället för punkt 11, som en åtgärd för vilken det inte krävs dubbel straffbarhet.

I övrigt lämnas paragrafen oförändrad.

2 kap.

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, *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.

I paragrafen framgår krav och rekommendationer avseende innehållet i en ansökan om rättslig hjälp i Sverige. Övervägandena finns i avsnitt 11.2.3.

Den enda ändring som görs i bestämmelsen är att det i *andra stycket* hänvisas till 4 kap. 28 c §. Ändringen, som upplyser om att det i den bestämmelse det hänvisas till finns särskilda krav avseende vad en ansökan om rättslig hjälp i Sverige med hemlig dataavläsning ska innehålla, är föranledd av förslaget i 4 kap. 28 c §.

Hemlig dataavläsning

Hemlig dataavläsning avseende någon i Sverige

4 kap.

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 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 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 dataavläsning.

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.

I paragrafen, som är ny, anges vad som ska gälla för rättslig hjälp med hemlig dataavläsning i Sverige. Övervägandena finns i avsnitt 11.2.3.

Paragrafen motsvarar väsentligen vad som gäller för rättslig hjälp med andra hemliga tvångsmedel enligt lagen. I *första stycket* klargörs först att det är åklagare som handlägger ansökan. Detta motsvarar vad som gäller för alla hemliga tvångsmedel enligt lagen och ska tillämpas på samma sätt. I *andra meningen* i första stycket framgår de krav som ställs beträffande ansökan. Motsvarande krav gäller vid ansökan om rättslig hjälp i Sverige med hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 § och ska tillämpas på samma sätt. 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 genomföra prövningen av om åtgärden ska tillåtas, t.ex. uppgifter om misstanke, brott, den som ska bli föremål för åtgärden, omständigheter som gör att åtgärden är av synnerlig vikt för utredningen och informationssystemet. Första styckets *sista mening* motsvarar vad som gäller enligt bestämmelserna om rättslig hjälp i Sverige med övriga hemliga tvångsmedel utom hemlig rumsavlyssning och ska tillämpas på samma vis. En uttrycklig hänvisning till 14 § lagen om hemlig dataavläsning klargör att åklagarens interimistiska beslutanderätt bestäms genom den bestämmelsen.

Andra stycket klargör att granskning inte behöver ske av upptagningar och uppteckningar. Kravet är samma som för övriga hemliga tvångsmedel med den skillnaden att hänvisningen sker till 23 § lagen om hemlig dataavläsning i stället för till 27 kap. 24 § rättegångsbalken. Eftersom den förstnämnda bestämmelsen hänvisar direkt tillbaka till den senare är innebörden emellertid exakt densamma som för de andra hemliga tvångsmedlen.

I *tredje styckets första mening* uppställs kravet att ett interimistiskt åklagarbeslut ska underställas domstolens prövning innan upptagna eller upptecknade uppgifter från en hemlig dataavläsning får lämnas över till den andra staten. Kravet överensstämmer med det som

gäller andra hemliga tvångsmedel enligt lagen när det föreligger en möjlighet för åklagaren att fatta interimistiskt beslut och ska tillämpas på samma sätt. I *andra meningen* i tredje stycket 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 23 § lagen om hemlig dataavläsning. Samma sak gäller, dock med direkt hänvisning till 27 kap. 24 § rättegångsbalken, för övriga hemliga tvångsmedel och ska tillämpas på samma sätt här.

I *fjärde stycket* regleras vad som ska gälla 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 av elektronisk kommunikation enligt 4 kap. 25 § tredje stycket ska tillämpas. Bestämmelserna i 27 kap. 31–33 §§ rättegångsbalken, till vilka den angivna regeln hänvisar och gör vissa avsteg ifrån, blir vid hemlig dataavläsning tillämpliga först genom en hänvisning i 23 § andra stycket den lagen. För att tydliggöra att 27 kap. 31–33 §§ rättegångsbalken ska tillämpas enligt bestämmelserna i lagen om hemlig dataavläsning, se t.ex. 25 § den lagen om begreppet informationssystem, görs i förevarande regel en hänvisning till 23 § andra stycket lagen om hemlig dataavläsning. I övrigt är ingen annan tillämpning av 4 kap. 25 § tredje stycket avsedd.

4 kap.

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.

I paragrafen, som är ny, regleras frågor omedelbar överföring, tekniskt bistånd och gränsöverskridande åtgärder när hemlig dataavläsning avser avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter. Övervägandena finns i avsnitt 11.2.3.

Första stycket innebär att hemlig dataavläsning, när åtgärden avser avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter får ske genom omedelbar överförning. Hänvisningarna i bestämmelsen innebär att den får samma innebörd som 4 kap. 25 a §. Se därför prop. 2004/05:144 s. 201 f., 2006/07:133 s. 92 och prop. 2011/12:55 s. 139.

I *andra styckets första mening* regleras frågan om tekniskt bistånd med omedelbar överföring av meddelanden eller uppgifter om meddelanden. Genom hänvisning till vissa delar av 4 kap. 25 b § blir det som gäller enligt den paragrafens andra, tredje och femte stycken tillämpligt även för hemlig dataavläsning, se prop. 2004/05:144 s. 202 f. och 2011/12:55 s. 139. Den avslutande meningen i andra stycket motsvarar i praktiken fjärde stycket i 4 kap. 25 b § men hänvisningarna är till bestämmelserna i lagen om hemlig dataavläsning i stället för till rättegångsbalkens bestämmelser.

I *tredje stycket* regleras frågor om gränsöverskridande åtgärder. Motsvarande ska gälla som gäller för hemlig avlyssning av elektronisk kommunikation när ansökan avser hemlig dataavläsning för kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter, vilket framgår av hänvisningarna till 4 kap. 26 a § första och andra styckena samt 26 b §. Hänvisningarna till bestämmelser i lagen om hemlig dataavläsning i sista meningen motsvarar i praktiken 4 kap. 26 a § tredje stycket. Se vidare prop. 2004/05:144 s. 206 ff. och 2011/12:55 s. 140 ff.

Hemlig dataavläsning avseende någon i utlandet

4 kap.

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.

I paragrafen, som är ny, regleras vad som ska gälla vid rättslig hjälp med hemlig dataavläsning avseende någon i utlandet. Övervägandena finns i avsnitt 11.2.3.

I *första stycket* framgår att domstol i Sverige får pröva en ansökan om hemlig dataavläsning om det är ett krav för att rättslig hjälp i den andra staten ska kunna ske. Prövningen sker då enligt lagen om hemlig dataavläsning efter ansökan från åklagaren. Det är underförstått att en svensk åklagare utan särskilt stöd i lagen får begära rättslig hjälp utomlands i den utsträckning som den andra staten tillåter det, vilket följer redan av 1 kap. 7 §.

Bestämmelsens *andra stycke* klargör att underrättelse till enskild inte alltid aktualiseras. När åtgärden verkställs i en annan stat ska den statens regler om underrättelse tillämpas, jfr 2006/07:133 s. 59. Det är endast när avläsning eller upptagning sker i Sverige som bestämmelsen i lagen om hemlig dataavläsning om underrättelse till enskild ska tillämpas.

I *tredje stycket* framgår att när det är fråga om hemlig dataavläsning som avser kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter så får åklagaren på motsvarande vis och enligt de förutsättningar som gäller vid hemlig avlyssning av elektronisk kommunikation begära tekniskt bistånd från en annan stat. Det som gäller enligt 4 kap. 26 § för sådant bistånd

gäller således även för bistånd med hemlig dataavläsning i de fallen, se vidare prop. 2004/05:144 s. 204 f. och 2011/12:55 s. 140.

4 kap.

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.

I paragrafen regleras när hemlig dataavläsning får verkställas gränsöverskridande utan hjälp från den andra staten. Övervägandena finns i avsnitt 11.2.3.

Bestämmelsen klargör att samma sak ska gälla beträffande tillstånd från annan stat till gränsöverskridande hemlig dataavläsning när åtgärden avser avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter som gäller för tillstånd till gränsöverskridande hemlig avlyssning av elektronisk kommunikation, se vidare prop. 2004/05:144 s. 208 f. och 2011/12:55 s. 141.

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

18 kap.

19 §

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

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig 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 vad som anges i andra stycket följer av 7 kap. 3 § första stycket 1, 4 § 1–8 och 5 § 3 tryckfrihetsförordningen samt 5 kap. 1 § första stycket och 3 § första stycket 1 yttrandefrihetsgrundlagen.

I paragrafen regleras vilka tystnadsplikter som har företräde framför rätten att meddela och offentliggöra uppgifter enligt 18 kap. offentlighets- och sekretesslagen. Övervägandena finns i avsnitt 10.12.3.

I andra och tredje styckena har hemlig dataavläsning tagits med i förteckningarna avseende åtgärder där tystnadsplikten, enligt de bestämmelser som framgår av respektive stycke, inskränker rätten att meddela och offentliggöra uppgifter. I tredje stycket har också hemlig rumsavlyssning lagts till som en sådan åtgärd för att rätta till ett tidigare förbiseende. I övrigt är paragrafen oförändrad.

Enligt ett förslag i en lagrådsremiss ska 5 kap. 3 § första stycket yttrandefrihetsgrundlagen flyttas till 5 kap. 4 § första stycket 1 i samma grundlag den 1 januari 2019, se lagrådsremissen Ändrade mediegrundlagar den 22 juni 2017. Någon ändring har dock inte föreslagits i förevarande bestämmelse med anledning av den aviserade lagändringen.

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.

I paragrafen regleras vilka tystnadsplikter som har företräde framför rätten att meddela och offentliggöra uppgifter enligt särskilda regler i annan lagstiftning. Övervägandena finns i avsnitt 10.12.3.

Ett tillägg görs i den förteckning som klargör när tystnadsplikten har företräde framför rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Tillägget utgörs av att den nya punkten 5 förs in sist i förteckningen. Innebörden av punkten är att den som avses i 30 § första stycket lagen om hemlig dataavläsning inte får meddela eller offentliggöra uppgifter som hen har fått del av eller tillgång till och som hänför sig till angelägenhet som avser användning av hemlig dataavläsning, dvs. sådana uppgifter för vilka tystnadsplikt råder.

13.5 Förslaget till lag om ändring i lagen (2017:000) om europeisk utredningsorder

1 kap.

2 §

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.

I paragrafen regleras vilka åtgärder enligt svensk rätt som utgör utredningsåtgärder enligt lagen. Övervägandena och förslag finns i avsnitt 11.2.4.

Ett tillägg avseende hemlig dataavläsning görs i punkt 6 i bestämmelsens förteckning, vilken förklarar vilka inhemska åtgärder som utgör utredningsåtgärder enligt lagen. Genom tillägget klargörs således att hemlig dataavläsning utgör en utredningsåtgärd 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 §§ *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.

I paragrafen framgår vissa förfaranderegler. Övervägandena och förslag finns i avsnitt 11.2.4.

I *första stycket* läggs hemlig dataavläsning till bland de utredningsåtgärder, som även i övrigt utgörs av andra hemliga tvångsmedel, i *andra punkten* som kräver domstolsprövning innan åklagaren kan utfärda en utredningsorder. Således klargörs att huvudregeln för att utredningsorder om hemlig dataavläsning ska få utfärdas är att domstolen har lämnat tillstånd till åtgärden.

I *andra stycket* regleras undantag från första stycket. Ett tillägg görs där för att klargöra att när det är tillåtet med interimistiska åklagarbeslut om tillstånd till hemlig dataavläsning enligt 14 § lagen om hemlig dataavläsning så är det också möjligt med ett sådant

beslut om utfärdande av en utredningsorder om hemlig dataavläsning. Det innebär att åklagaren interimistiskt kan utfärda utredningsorder om hemlig dataavläsning enligt 2 § första stycket 1–3 samt 5 och 6 lagen om hemlig dataavläsning men inte beträffande avläsning eller upptagning av rumsavlyssningsuppgifter.

Hemlig dataavläsning

2 kap.

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.

I bestämmelsen, som är ny, anges vilka särskilda regler i lagen om hemlig dataavläsning som ska tillämpas när en utredningsorder för hemlig dataavläsning har utfärdats i Sverige. Övervägandena och förslag finns i avsnitt 11.2.4.

Bestämmelserna i 3 och 5 §§ innebär att samma förutsättningar (1–5, 11 och 12 §§ lagen om hemlig dataavläsning) och förfarande (13–15 §§ och 16 § första stycket samma lag) gäller för att utfärda en utredningsorder av detta slag som när en motsvarande åtgärd vidtas i Sverige. Enligt förevarande paragrafs *första stycke* ska bestämmelserna i 16 § andra stycket, 22 § och 23§ första stycket lagen om hemlig dataavläsning i de fallen tillämpas. Det motsvarar helt vad som enligt gäller enligt 19 § för hemlig kameraövervakning och hemlig rumsavlyssning fast med hänvisningar till lagen om hemlig dataavläsning i stället för till rättegångsbalken. När det gäller tillämpningen av bestämmelsen hänvisas därför till prop. 2016/17:218 s. 256.

I andra och tredje styckena finns särskilda bestämmelser som gäller när det är fråga om en utredningsorder för hemlig dataavläs-

ning avseende avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter. Bestämmelserna motsvarar genom hänvisningar vad som gäller för en utredningsorder om hemlig avlyssning av elektronisk kommunikation enligt 17 och 18 §§, dock med hänvisning till lagen om hemlig dataavläsning i stället för till rättegångsbalken. Se vidare prop. 2016/17:218 s. 254 f.

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 14 § lagen (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*.

I paragrafen regleras frågor om interimistisk beslutanderätt för åklagaren beträffande erkännande och verkställande av en utredningsorder. Övervägandena finns i avsnitt 11.2.4.

I bestämmelsen görs ett tillägg som innebär att åklagaren, liksom är fallet vid övriga hemliga tvångsmedel utom hemlig rumsavlyssning, får meddela interimistiskt beslut att erkänna en utredningsorder för hemlig dataavläsning. Hänvisningen sker till 14 § lagen om hemlig rumsavlyssning vilket innebär att erkännande och verkställighet av en utredningsorder får ske interimistiskt för hemlig dataavläsning enligt 2 § första stycket 1–3 samt 5 och 6 lagen om hemlig dataavläsning men inte beträffande avläsning eller upptagning av rumsavlyssningsuppgifter.

Hemlig dataavläsning

3 kap.

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 verkställbarhetsförklaring, får verkställighet ske först efter det att domstolen har fastställt förklaringen. Vid verkställighet enligt 34 § 2 tillämpas första och andra styckena.

I paragrafen, som är ny, regleras vad som gäller för verkställighet av en utredningsorder för hemlig dataavläsning. Övervägandena finns i avsnitt 11.2.4.

Bestämmelsens första och andra stycke motsvarar vad som gäller för verkställighet av en utredningsorder för hemlig kameraövervakning och hemlig rumsavlyssning enligt 37 §, se kommentaren till den bestämmelsen i prop. 2016/17:218 s. 287. Innebörden av *första meningen i första stycket* är att upptagningar eller upptagningar inte behöver granskas på samma vis som om det hade varit fråga om verkställighet av hemlig dataavläsning efter ett svenskt tillstånd till åtgärden enligt lagen om hemlig dataavläsning. Det hänger samman med att det är den brottsbekämpande myndigheten i den stat där utred-

ningsordern har utfärdats som har kunskaperna om vilka uppgifter som är relevanta för den pågående utredningen. Därför tillämpas i stället den statens bestämmelser om granskning. Undantaget från granskningsskyldigheten gäller emellertid inte sådan granskning som t.ex. avser att avbryta åtgärden om avlyssningsförbud råder eller uppgifterna är skyddade enligt beslagsförbudsregeln, se 21 och 22 §§ lagen om hemlig dataavläsning och jämför kommentaren till 36 § i prop. 2016/17:218 s. 286. I första styckets *andra mening* finns en regel som i huvudsak motsvarar det som föreslås ska gälla enligt 4 kap. 28 c § tredje stycket andra meningen lagen om internationell rättslig hjälp i brottmål, se kommentaren ovan till den bestämmelsen. Skillnaden mot den bestämmelsen är bestämmelserna som reglerar när överlämnande av upptagningar och uppteckningar får ske (38 och 40 §§ förevarande lag). Beträffande dessa bestämmelser se prop.2016/17:218 s. 287 och 288 f.

I *andra stycket* sker en hänvisning till att det som gäller enligt 36 § andra stycket ska gälla beträffande underrättelse till enskild. Bestämmelserna i 27 kap. 31–33 §§ rättegångsbalken, till vilka den angivna bestämmelsen hänvisar och föreskriver vissa avsteg ifrån, blir vid hemlig dataavläsning tillämpliga först genom en hänvisning i 23 § andra stycket den lagen. För att tydliggöra att 27 kap. 31–33 §§ rättegångsbalken ska tillämpas enligt bestämmelserna i lagen om hemlig dataavläsning, se t.ex. 25 § den lagen, görs i förevarande bestämmelse en hänvisning till 23 § andra stycket lagen om hemlig dataavläsning. I övrigt är ingen annan tillämpning av avsedd än vad som gäller vid hemlig kameraövervakning eller hemlig rumsavlyssning.

I *tredje och fjärde styckena* finns särskilda bestämmelser om vad som gäller när det är fråga om hemlig dataavläsning för kommunikationsavlyssnings-, kommunikationsövervaknings- och lokaliseringsuppgifter. Genom hänvisningar och bestämmelsens ordalydelse tillämpas då motsvarande som vid verkställighet av utredningsorder för hemlig avlyssning av elektronisk kommunikation, se vidare prop. 2016/17:218 s. 284 ff. Hänvisningar sker till dock till lagen om hemlig dataavläsning i stället för till rättegångsbalken. Innehållet i de hänvisade bestämmelserna är dock motsvarande.

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.

I paragrafen, som är ny, finns dels bestämmelser om underrättelse till en annan medlemsstat, dels förutsättningarna för att tillåta en annan medlemsstats avläsning på svenskt territorium, vem som är behörig att pröva tillståndsfrågan och tidsfrister. Övervägandena finns i avsnitt 11.2.4.

Enligt bestämmelsen ska det som gäller enligt lagen om europeisk utredningsorder för hemlig avlyssning av elektronisk kommunikation gälla när hemlig dataavläsning avser avläsning eller upptagning av kommunikationsavlyssnings-, kommunikationsövervaknings- eller lokaliseringsuppgifter. Se därför kommentarerna till befintliga bestämmelser i prop. 2016/17:218 s. 299 ff.

Särskilda yttranden

Särskilt yttrande av experten Anne Ramberg

Integritet - en rättighet som åtnjuter skydd

Genom Lissabonfördraget blev Europeiska unionens stadga om de grundläggande rättigheterna rättsligt bindande. Stadgan har samma rättsliga status som fördragen. I en gemensam förklaring anger medlemsstaterna att stadgan bekräftar de grundläggande rättigheter som garanteras av Europakonventionen (skyddet av den personliga integriteten och privatlivet regleras i artikel 8) och som följer av de konstitutionella traditioner som är gemensamma för medlemsstaterna. Det kan i det sammanhanget konstateras att den personliga integriteten och privatlivet dessutom åtnjuter skydd enligt artikel 12 i FN:s deklaration om de mänskliga rättigheterna och i FN:s konvention om medborgerliga och politiska rättigheter, Europarådets resolution från 1970, liksom i Europadomstolens praxis, EU-domstolens praxis samt i regeringsformen.

Att skyddet för den personliga integriteten och privatlivet upprätthålls är såväl ett enskilt intresse, som ett samhällsintresse. Övervakning genom hemliga tvångsmedel innebär ett integritetsintrång för den enskilde. Men, övervakning utgör samtidigt ett intrång i de rättsstatliga och demokratiska värden som den personliga integriteten ska skydda. Personlig integritet utgör ett villkor för att människor ska kunna utöva sina demokratiska rättigheter och därmed en förutsättning för det demokratiska samhället. Ett samhälle, där den personliga integriteten beskärs, riskerar att förlora sin demokratiska värdegrund, som bygger på allas fria och kritiska deltagande i debatten. Denna värdegrund förutsätter att människor i allmänhet inte upplever sig övervakade och registrerade. Skyddet är också en gräns för statens maktutövning och kan därför inte uppvägas av kontroll.

Inskränkningar i rättighetsskyddet

Det finns emellertid, under vissa i konventioner och lag angivna villkor, möjlighet att göra inskränkningar i rättighetsskyddet. En grundläggande förutsättning är att intrånget måste vara nödvändigt i ett demokratiskt samhälle. Ett behov måste föreligga och åtgärden måste förväntas bli effektiv. Därtill måste den vara proportionerlig i förhållande till syftet. Dessa krav följer av EU:s stadga om de grundläggande rättigheterna, Europakonventionen, regeringsformen och tydlig praxis från EU-domstolen och Europadomstolen för mänskliga rättigheter. Det innebär att en avvägning, mellan det befogade kravet på effektiv brottsbekämpning och upprätthållande av rättstrygghet för medborgaren, å den ena sidan och det lika befogade kravet på upprätthållandet av den enskildes rättssäkerhet och integritet å den andra, måste göras. Denna avvägning kan komma att utfalla olika vid skilda tidpunkter.

Hemliga tvångsmedel skulle ur ett brottsbekämpningsperspektiv kunna användas utan begränsning, inte bara vid brottsutredning, utan också i preventivt underrättelsesyfte. Det är lätt att se nyttoeffekter, såväl i det enskilda fallet, som generellt. Det är emellertid inte liktydigt med att det föreligger ett reellt behov av sådana åtgärder. Till detta anknyter problemet att effektiviteten är svår att definiera och mäta, något som i sin tur medför svårigheter i proportionalitetsavvägningen. En obegränsad användning av hemliga tvångsmedel är därför inte förenligt med grundläggande rättigheter skyddade i lag och konventioner.[1]

Krav på analys av behov, effektivitet och proportionalitet

Inledningsvis vill jag i detta sammanhang hänvisa till vad Advokatsamfundet tidigare anfört i yttrande rörande behovs-, effektivitets- och proportionalitetsprincipen vid hemlig dataavläsning och andra

[1] Se Advokatsamfundets remissyttrande den 30 oktober 2012 över betänkandet *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44), den 18 maj 2009 över delbetänkandet *En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen* (SOU 2009:1), samt den 30 januari 2007 över betänkandet *Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.* (SOU 2006:98), liksom den kritik som Lagrådet anförde i sitt yttrande såväl den 13 maj 2014 (prop. 2013/14:237) som den 28 mars 2017 avseende fortsatt giltighet av en tidsbegränsad bestämmelse i inhämtningslagen.

tvångsmedel, vilket alltjämt äger giltighet.[2] När det gäller frågan om det finns ett behov av att införa hemlig dataavläsning delar jag utredningens analys och slutsats att det, på de av de brottsbekämpande myndigheterna anförda skälen, föreligger ett behov som inte kan tillgodoses på annat sätt än genom hemlig dataavläsning. Till grund för denna slutsats lägger jag det faktum att lagstiftaren genom t.ex. inhämtningslagen, preventivlagen och i rättegångsbalken under vissa förutsättningar godtagit hemlig informationsinhämtning i underrättelseverksamhet och under förundersökning. Mycket av den information som med hjälp av nuvarande hemliga tvångsmedel tidigare kunnat inhämtas har dock av i utredningen redovisade skäl kommit att reduceras väsentligt. Således finns ett behov av att tillåta hemlig dataavläsning.

Jag delar likaså utredningens bedömning att hemlig dataavläsning skulle vara effektiv, i det enskilda fallet, då en sådan åtgärd skulle komma att användas. Det har emellertid från de brottsbekämpande myndigheternas sida samtidigt understrukits att hemlig dataavläsning i likhet med hemlig rumsavlyssning är tekniskt mycket komplicerad och mycket resurskrävande. Detta har uppgivits innebära att hemlig dataavläsning, i likhet med hemlig rumsavlyssning, endast skulle komma att användas i mycket begränsad utsträckning. I ljuset av det stora behov som uppges föreligga på grund av att en stor mängd information som tidigare kunde inhämtas med befintliga hemliga tvångsmedel, av en rad olika skäl, inte längre är tillgänglig, ifrågasätter jag om tvångsmedlet hemlig dataavläsning för närvarande skulle vara effektivt i strikt mening. Till detta kommer att risken finns att de personer och miljöer som skulle komma att bli föremål för hemlig dataavläsning snabbt skulle utveckla tekniker för att förhindra att informationsinhämtningen genom dataavläsning, på samma sätt som skett med traditionell avlyssning, skulle ge effektivt resultat. Detta sagt kan jag godta utredningens analys och slutsats när det gäller effektiviteten.

Jag delar dock inte utredningens analys och slutsatser när det gäller proportionalitetsavvägningen. Proportionalitetsprincipen är en erkänd rättsprincip i Sverige och i Europa. Den är lagfäst bland annat

[2] Se Advokatsamfundets remissyttrande den 30 september 2005 över promemorian *Tvångsmedel för att förebygga eller förhindra allvarlig brottslighet* (Ds 2005:21). Se även Advokatsamfundets remissyttrande den 28 november 2005 över delbetänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* (SOU 2005:38).

i regeringsformen, polislagen, rättegångsbalken, liksom i Europakonventionen och EU:s rättighetsstadga. Den följer därtill av Europadomstolens och numera EU-domstolens praxis. Principen äger generell giltighet vad gäller avvägningen mellan allmänna och enskilda intressen. Den betyder att statens metoder ska vara proportionerliga i förhållande till det berättigade ändamål som den avser att uppnå. I all synnerhet gäller detta i fråga om viktiga principer till skydd för den enskilde. När det allmänna intresset kolliderar med det grundläggande integritetsskyddet är statens handlingsutrymme särskilt begränsat. I en rättsstat ska den enskilde åtnjuta skydd mot statens maktutövning. Proportionalitetskravet innefattar en sådan begränsning. EU-domstolen bekräftade detta såväl i ogiltigförklarandet av datalagringsdirektivet som i den s.k. Tele2-domen.[3] Domstolen fastslog här att unionsrätten inte alltid tillåter intrång i privatlivet, ens om syftet i sig är godtagbart. Det krävs mer. Det krävs att åtgärden är nödvändig och att den vid en övergripande bedömning ryms inom statens handlingsutrymme. Min slutsats är därför att utredningens förslag om införande av hemlig dataavläsning inte är proportionerligt. Sammanfattningsvis finner jag utifrån principiella utgångspunkter inte utredningens förslag vara godtagbart.

Rättssäkerheten i teknikens våld

I den digitala utvecklingen har teknikimperativet blivit styrande. Det leder till en maktförskjutning från riksdagen till regeringen och rättstillämparen.[4] Vidden av integritetsintrånget kan nämligen utvidgas utan att lagstiftningen förändras. Det blir en s.k. tillämpningsglidning. Polisens basstationstömningar är ett sådant exempel. Detsamma gäller olika molntjänster. Teknikutvecklingen riskerar därmed att leda till att legalitetskravet åsidosätts. I detta hänseende är särskilt bestämmelserna i 17 och 19 §§ i den föreslagna lagen om hemlig dataavläsning av intresse.

[3] Se EU-domstolens avgörande den 8 april 2014 i de förenade målen C-293/12 och C-594/12 samt EU-domstolens dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15.
[4] Se Markus Naarttijärvi, *För din och andras säkerhet – Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel*, 2013, Skrifter från juridiska institutionen vid Umeå universitet, nr. 29.

Hemlig dataavläsning erbjuder i det närmaste obegränsade tekniska möjligheter att övervaka människor i realtid. De avgränsningar som utredningsförslaget anvisar utgör dock enligt min mening inte tillräckligt skydd varken för den enskildes rättssäkerhet eller integritet. De stora avgränsnings- och tillämpningsproblem som den föreslagna bestämmelsen i 5 § innebär erfordrar en vidare analys. Härutöver finns behov av ytterligare utredning. Ett sådant exempel är hur det överhuvudtaget ska vara praktiskt möjligt att kunna tillämpa begränsningarna i 4 § tredje stycket i den föreslagna lagen om hemlig dataavläsning.

Som historien under senare tid visat tillkommer lagstiftning inte sällan för ett ändamål, men utvidgas efter en tid till att omfatta andra ursprungligen inte avsedda ändamål. Exemplen är många. När ett tvångsmedel eller annan övervakning väl har införts, är det jämförelsevis enkelt att utvidga tillämpningsområdet allt eftersom. Förslaget att ge de brottsbekämpande myndigheterna tillgång till vad som inhämtas genom signalspaning är bara ett av många exempel. Detsamma gäller när hemlig tvångsmedelslagstiftning införs ”på prov” och efter en tid regelmässigt blir permanentad. Risken för ändamålsglidning är uppenbar och kontrollen riskerar till följd av den komplicerade tekniken att bli inget annat än en chimär.

Särskilt om Säkerhetspolisens särskilda uppdrag att förhindra brott

Intrånget i den personliga integriteten grundar sig vid underrättelseverksamhet inte på någon misstanke mot en enskild person, utan på riskbedömningar om brottslig verksamhet någon gång i framtiden. Tidigare krävdes att det fanns särskild anledning anta att en specifik person skulle kunna göra sig skyldig till de uppräknade brotten. Utgångspunkten nu är i stället nyttan som inhämtningen kan ha för den preventiva verksamheten. Inhämtningen är inte som tidigare kopplad till vissa brott utan till visst straffvärde. Enligt inhämtningslagen får uppgifterna hämtas in om de är av särskild vikt för att förebygga, förhindra, eller upptäcka brottslig verksamhet för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Sådana bedömningar riskerar, i en annan politisk kontext än den som vi lever i idag, att grundas på allt från etnicitet, religiös inriktning, sexuell läggning till politisk inriktning. Att i underrättelseverksamhet tillåta preven-

tiva metoder på det sätt som lagstiftningen numera medger är redan det ett avsteg från sedan lång tid erkända och tillämpade rättsstatliga principer. De brottsbekämpande myndigheternas (utöver Säkerhetspolisen) behov får i underrättelseverksamheten, anses tillgodosett genom befintlig lagstiftning och de förslag som nyligen presenterats i delbetänkandet av Utredningen om datalagring och EU-rätten, *Datalagring – brottsbekämpning och integritet* (SOU 2017:75). Att härutöver tillåta hemlig dataavläsning i underrättelsesyfte är därför enligt min mening inte proportionerligt när det gäller de brottsbekämpande myndigheterna i allmänhet. När det gäller Säkerhetspolisen kan enligt min mening dock en annan bedömning göras.

Terrorism och IT-attacker är exempel på reella hot mot vårt samhälle och den demokratiska rättsstaten. Säkerhetspolisen har härvidlag ett särskilt ansvar att förhindra att terrorattentat och andra allvarliga brott mot rikets säkerhet äger rum. Detta uppdrag skiljer sig på ett avgörande sätt från den öppna polisens. Säkerhetspolisens uppdrag tar därför till övervägande del sikte på underrättelseverksamhet i syfte att förhindra allvarliga brott. Detta framgår bland annat av användningen av preventiva tvångsmedel. Det är i princip endast Säkerhetspolisen som använder sig av denna möjlighet. Den öppna polisen har enligt uppgift från regeringens skrivelse till riksdagen endast vid ett fåtal tillfällen erhållit domstols tillstånd enligt preventivlagen.[5] Lagstiftaren har dock inte velat göra åtskillnad mellan Säkerhetspolisen och den öppna polisen, när det gäller möjligheterna till tvångsmedelsanvändning. Det tycker jag är olyckligt. Om hemlig dataavläsning överhuvudtaget ska kunna uppfylla kraven på proportionalitet måste, enligt min mening, tvångsmedlet exklusivt förbehållas Säkerhetspolisen vid misstanke om mycket allvarlig brottslighet som utgör hot mot rikets säkerhet och som har ett straffminimum eller förväntat straffvärde på fängelse fyra år eller mer.[6] Detta erfordrar dock ytterligare analys och utredning.

[5] Se Regeringens skrivelse 2016/17:69 *Redovisning av användningen av hemliga tvångsmedel under år 2015*.
[6] Se Advokatsamfundets remissyttrande den 30 oktober 2012 över betänkandet *Hemliga tvångsmedel mot allvarliga brott* (SOU 2012:44) och det särskilda yttrande jag avgav i samband med den utredningen.

Materiella synpunkter på lagstiftningen

Jag vill utöver vad som anförts ovan, även framhålla några materiella synpunkter på den föreslagna lagstiftningen.

Hemlig dataavläsning är enligt förslaget ett eget hemligt tvångsmedel som ska beslutas av domstol och införas under en begränsad tid. Avsikten är dock att det inte ska gå längre, när det gäller den information som ska kunna inhämtas, än vad som är fallet med befintliga tvångsmedel. Hemlig dataavläsning är emellertid ett tvångsmedel som enligt min mening innebär särskilda integritetskränkningar för den enskilde och som i flera hänseenden går betydligt längre än övriga hemliga tvångsmedel. Mot denna bakgrund anser jag att detta tvångsmedel, om det införs, bör vara sekundärt till övriga tvångsmedel och tillstånd av domstol endast aktualiseras efter att det visat sig att ett redan beslutat tvångsmedel inte gett avsett resultat. Först i ett sådant skede bör hemlig dataavläsning kunna komma ifråga.

Eftersom det är av största vikt att hemlig dataavläsning används med stor restriktivitet och endast efter nogsamt uppställda rättsliga förutsättningar, anser jag även att den uppräkning av uppgiftstyper som föreslås kunna inhämtas genom hemlig dataavläsning i bestämmelsen i 2 §, måste förtydligas genom att det i de angivna punkterna uttryckligen hänvisas till de lagbestämmelser som reglerar dessa tvångsmedel. Det kan finnas risk för att det annars skapas alternativa rekvisit för tillämpning av dessa hemliga tvångsmedel och därmed även en utvidgning av tillämpningsområdet. Lagtekniskt innebär då förslaget att tillåtligheten och omfattningen av hemlig dataavläsning görs beroende av den s.k. inhämtningslagen, preventivlagen och rättegångsbalken. Genom att vidta ändringar i dessa lagar kommer tillämpningen av hemlig dataavläsning därigenom automatiskt att kunna utvidgas. Det är emellertid inte heller en lämplig ordning. Frågan bör ytterligare analyseras och lösningen måste tydligt framgå i lagen om hemlig dataavläsning.

När det gäller de särskilda begränsningar mot hemlig dataavläsning som föreslås i 11 §, undantas advokater från åtgärder enligt 2 §. Detta är en självklarhet och innebär ett upprätthållande av gällande rättsstatliga principer. Avlyssning eller övervakning ska aldrig kunna vidtas avseende elektronisk kommunikation som sker mellan en advokat och dennes klient. Det är i detta sammanhang viktigt att

understryka att den förtroliga kommunikationen mellan en advokat och en klient och advokatens i rättegångsbalken fastslagna tystnadsplikt är ett klientprivilegium och därmed finns för att i första hand skydda klientens intresse av sekretess (se NJA 2010 s. 122 och justitierådet Stefan Lindskogs särskilda yttrande i denna fråga).

De särskilda förbuden mot att använda hemlig dataavläsning mot bl.a. advokater har även direkt samband med de föreslagna bestämmelserna om beslagsförbud och avlyssningsförbud (21 och 22 §§). Beslagsförbudet i 27 kap. 2 § RB är direkt kopplat till frågeförbudet i 36 kap. 5 § RB. Det är därför viktigt att den rättsliga motiveringen för beslags- och avlyssningsförbudet även tillämpas i fråga om den allmänna förbudsbestämmelsen i 11 §.

Skyddet för advokatens verksamhet framgår även av bestämmelsen om tillträdestillstånd i 12 §. Det rör sig här om mycket långtgående åtgärder av integritetskränkande art som innebär möjlighet att kunna installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Enligt bestämmelsens andra punkt anges att ett tillträdestillstånd inte får avse en plats som stadigvarande används eller särskilt är avsedd att användas för verksamhet som bedrivs av advokater. Enligt min uppfattning är kravet på ”särskild anledning att anta” att informationssystemet kommer att finnas på platsen och att det inte räcker med ett allmänt antagande, utan att det måste krävas någon faktisk omständighet som med viss styrka talar för att det kommer att finnas där i vart fall någon gång under tillståndstiden, alltför vagt formulerat. Kravet bör skärpas ytterligare.

I sista stycket i 2 § framgår att det ska vara möjligt att hindra överförda meddelanden från att komma fram. Oaktat liknande reglering avseende hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § andra stycket rättegångsbalken, får detta enligt min mening anses vara ett långtgående komplement till övervakning som kommer att kunna utföras genom hemlig dataavläsning. Ett sådant förfarande ställer därför särskilda krav på förekomsten av effektiva rättsmedel för det fall ett sådant, felaktigt, myndighetsförfarande skulle föranleda en enskild ekonomisk eller personlig skada (se artikel 13 Europakonventionen).

De grundläggande förutsättningar som måste vara för handen för att hemlig dataavläsning ska kunna ske anges i 3 §. Dock framgår av denna bestämmelse att det är tillräckligt att göra en proportionalitetsprövning innan ett beslut fattas om hemlig dataavläsning.

Bestämmelsen bör enligt mitt förmenande kompletteras med krav på nödvändighet och effektivitet, dvs. även uppfylla den s.k. behovs- och ändamålsprincipen, för att detta tvångsmedel ska kunna aktualiseras.

I bestämmelsen i 6 § anges förutsättningarna för hemlig dataavläsning utanför en förundersökning. Även om kriteriet ”påtaglig risk” är detsamma som i preventivlagen, finns risk för att det i fråga om ett så pass långtgående tvångsmedel som dataavläsning utgör ett alltför oklart och vidsträckt kriterium. Enligt min uppfattning bör det krävas att det föreligger en ”uppenbar risk”. Vidare torde lokutionen ”en person” innebära att det inte uppställs något krav på kunskap om namnet på den person som kan komma i fråga för hemlig dataavläsning. Dock torde det även innebära att också annan person än den som misstänks för brott skulle kunna komma att omfattas av tvångsmedlet (t.ex. en familjemedlem som bor på annan adress än den misstänkte, jfr 12§). Detta förefaller vara att gå väl långt och bestämmelsen bör uttryckligen ta sikte på en viss person, även om det inte uppställs krav på misstanke om ett specifikt brott.

I bestämmelsen i 13 § anges att prövning av hemlig dataavläsning sker av rätten på ansökan av åklagare (dock med undantagsmöjligheten i de fall det kan anses vara ”fara i dröjsmål” enligt 14 §, då åklagaren interimistiskt får fatta beslut om hemlig dataavläsning och där rätten sedan skyndsamt ska pröva om det finns skäl för åtgärden). Eftersom detta överensstämmer med det tillståndssystem som finns för andra hemliga tvångsmedel, utöver inhämtningsfallen (10 §), är detta en lämplig ordning även för hemlig dataavläsning och innebär i förhållande till inhämtningsfallen en stärkt rättssäkerhet genom att Polismyndigheten eller Säkerhetspolisen inte själv får fatta beslut, utan att detta måste göras av en domstol. Dessutom tycks den föreslagna ordningen innebära att det ankommer på åklagare att i det enskilda fallet pröva om förutsättningar för hemlig dataavläsning föreligger, efter att den brottsbekämpande myndighet som vill utföra åtgärden har ansökt om det, vilket jag anser vara positivt. Härtill kommer att det i 29 § anges att SIN ska underrättas om en prövning har skett rörande hemlig dataavläsning, vilket också är en systemkonform och rättssäkerhetsfrämjande ordning.

Vidare konstaterar jag att den möjlighet som åklagare har att i brådskande fall besluta om hemlig dataavläsning enligt 14 §, ställer viktningen mellan effektiv brottsbekämpning och rättssäkerhet

ytterligare i fokus. Att ett så pass långtgående beslut som att besluta om hemlig dataavläsning ska ligga på åklagare, vilken sedermera kan komma att utgöra part i ett efterföljande brottmål, kan ifrågasättas utifrån rättssäkerhetsskäl. Detta gäller även om den föreslagna ordningen är densamma som gäller i fråga om hemlig avlyssning och övervakning av elektronisk kommunikation och hemlig kameraövervakning enligt 27 kap. 21 a § andra stycket RB, liksom enligt 6 a § preventivlagen. Det kan alltså ifrågasättas om ett så integritetskränkande tvångsmedel som hemlig dataavläsning innebär, ska kunna beslutas av en brottsbekämpande myndighet.[7] Att stadga att uppgifter som inhämtats på felaktig grund inte får användas i en efterföljande brottsutredning utgör inte ett tillräckligt skydd för den enskilde. Sammantaget anser jag att domstol alltid ska ansvara för prövning av hemlig dataavläsning. I vart fall bör kravet på att det ska föreligga risk för ”fördröjning av väsentlig betydelse” skärpas väsentligt.

Överlag anser jag att förslagen i betänkandet i flera avseenden innebär att alltför mycket inflytande över den hemliga dataavläsningen, såväl i fråga om form som innehåll, överlämnas till de brottsbekämpande myndigheterna.

I 18 § regleras teleoperatörernas medverkan i samband med verkställigheten av hemlig dataavläsning. Det föreslås ingen lagfäst skyldighet för operatörerna att medverka vid verkställigheten av den hemliga dataavläsningen, utan det är fråga om frivillig medverkan. Skrivningarna i betänkandet förutsätter dock att operatörerna kommer att samarbeta med de brottsbekämpande myndigheterna på frivillig grund. Detta är med beaktande av förbudet mot lagstiftning genom motiv direkt olämpligt. Det finns goda argument för såväl en medverkansskyldighet som en medverkansmöjlighet. Enligt min uppfattning måste det dock tydligt framgå om operatörernas medverkan ska bygga på en laglig skyldighet eller om den ska vara helt frivillig. Att såsom nu lagstifta kring en medverkansmöjlighet på frivillig grund, men underförstått uttala att operatörerna måste medverka för att den hemliga dataavläsningen ska kunna bli effektiv, är inte en god lagstiftningsordning. Vidare framgår det inte av bestämmelsen vilken form av bistånd som avses, även om det i för-

[7] Jfr Advokatsamfundets tidigare yttranden i denna fråga, bl.a. yttrandet över betänkandet *Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.* (SOU 2006:98).

fattningskommentaren nämns vissa typer av åtgärder som operatörerna kan komma att tillfrågas om bistånd med. Det finns därför risk för att det kan uppstå praktiska problem i samband med förfrågningar från de verkställande myndigheterna om samverkan med teleoperatörerna.

I bestämmelsen i 20 § slås vissa aktsamhetskrav fast; olägenhet eller skada får inte förorsakas utöver vad som är ”absolut nödvändigt”. Vidare anges att ett tekniskt hjälpmedel som använts vid hemlig dataavläsning ska tas bort, avinstalleras eller göras obrukbart ”så snart det kan ske” efter att tiden för tillståndet gått ut eller tillståndet hävts. Jag anser att tidskravet bör skärpas ytterligare, till ”omedelbart” eller ”i direkt anslutning till”, för att minimera risken för att uppgifter inhämtas efter att tillstånd löpt ut eller hävts.

Särskilt yttrande av experterna Johan Dahl, Susanne Hedberg, Kurt Alavaara, Per Lagerud, Lisbeth Tjärnkvist, Bengt Lindholm, Mats Ljungqvist och Hans Harding

Vi står bakom utredningens förslag om införande av en lag om hemlig dataavläsning. Denna lagstiftning är nödvändig för att de brottsbekämpande myndigheterna ska kunna upprätthålla ett effektivt arbete med att förebygga, bekämpa, utreda och lagföra allvarlig brottslighet och brott mot Sveriges säkerhet.

För att kunna förbereda och sedan verkställa hemlig dataavläsning kommer det i praktiken att krävas främst personella och tekniska resurser från de brotts-bekämpande myndigheterna. Men en annan central framgångsfaktor i detta arbete är att de operatörer som tillhandahåller allmänt tillgängliga elektroniska kommunikationsnät – och som därmed förfogar över den tekniska och elektroniska infrastrukturen – underlättar verkställigheten av hemlig dataavläsning. Utredningen har därför övervägt en *skyldighet* för dessa operatörer att på olika sätt medverka vid verkställigheten av hemlig dataavläsning, men stannat vid att föreslå en *möjlighet* till detta.

Vi menar emellertid att endast en möjlighet, och därmed valfrihet, för operatörerna att medverka inte är tillräcklig. Att, som det framställs i avsnitt 10.12.2, förlita sig på att operatörer kommer att medverka på grund av något djupt känt samhällsansvar är tyvärr nog bara fromma förhoppningar. Vår långa erfarenhet säger att operatörernas medverkan i sådant fall skulle bli högst godtycklig och att flera operatörer kan förväntas vägra att samarbeta med de brottsbekämpande myndigheterna vid hemlig dataavläsning.

För att hemlig dataavläsning i alla avseenden ska bli ett reellt och effektivt verktyg i brottsbekämpningen kommer det i vissa fall att vara en förutsättning att operatörer är skyldiga att medverka, helst med tydliga och kännbara sanktioner om de vägrar.

Kommittédirektiv 2016:36

Hemlig dataavläsning

Beslut vid regeringssammanträde den 12 maj 2016

Sammanfattning

En särskild utredare ska undersöka om bestämmelser om hemlig dataavläsning bör införas i svensk rätt för att säkerställa att de brottsbekämpande myndigheterna kan upprätthålla sin förmåga att bekämpa brott. Utredaren ska bl.a.

- ta reda på vilket behov av hemlig dataavläsning som finns,
- undersöka om hemlig dataavläsning skulle vara en effektiv metod för att bekämpa terrorristbrottslighet 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.

Uppdraget ska redovisas senast den 13 november 2017.

Förutsättningarna för att bekämpa brott har förändrats

Under senare år har den ökande internationaliseringen i kombination med teknikutvecklingen och en tilltagande internetanvändning inneburit att kriminaliteten delvis har ändrat karaktär. Internet erbjuder lättillgängliga kontaktytor för brottsplanering inom och utom landets gränser och utgör bl.a. en etablerad plattform för våldsbejakande extremism och terrorismpropaganda. Viss typ av kriminalitet, t.ex. barnpornografibrott, har internet som brottsplats. Utvecklingen innebär att även förutsättningarna för att förhindra brott och säkra bevis för begångna brott har förändrats radikalt. Uppgifter om elektronisk kommunikation och andra elektroniska spår är i dag helt nödvändiga för brottsbekämpningen.

Samtidigt har teknik- och kommunikationsutvecklingen under de senaste åren begränsat det praktiska användningsområdet för hemlig avlyssning av elektronisk kommunikation (hemlig avlyssning). Hemlig avlyssning används av brottsbekämpande myndigheter för att komma åt innehållet i kommunikation mellan individer. Nuvarande lagstiftning tillåter hemlig avlyssning av såväl traditionell telefoni som internetbaserad kommunikation, t.ex. ip-telefoni, e-post och sociala medier. Eftersom internetbaserad kommunikation mellan individer allt oftare krypteras när den skickas från avsändare till mottagare får myndigheterna emellertid ofta bara tillgång till krypterad information inom ramen för ett tillstånd till hemlig avlyssning. För leverantörer av internetbaserade tjänster finns det, till skillnad från för leverantörer av traditionell telefoni, inte någon skyldighet att anpassa sina tekniska system så att de kan lämna ut kommunikation som de krypterar i sina nät till brottsbekämpande myndigheter i klartext. De brottsbekämpande myndigheterna har inte någon egen möjlighet att dekryptera kommunikation i realtid. Det är inte heller realistiskt för myndigheterna att bygga upp och underhålla en sådan teknisk förmåga i förhållande till de olika operatörernas system.

Det finns andra tekniska svårigheter med att avlyssna internetbaserad kommunikation inom ramen för ett tillstånd till hemlig avlyssning. Det beror framför allt på att enskilda personer enkelt kan köpa anonymiseringstjänster som skyddar deras identitet, ip-adress, på nätet så att kommunikationen blir helt anonym. Teknikutvecklingen har också medfört att det inte längre är självklart att en viss ip-

adress motsvarar en enskild abonnent. Flera abonnenter kan dela på en och samma adress vilket medför att ip-adressen inte är synonym med den misstänktes identitet på nätet. Den stora mängden krypterad information på nätet innebär också att det kan vara svårt för brottsbekämpande myndigheter att identifiera vad som är kommunikation mellan individer i det samlade flödet.

En effektiv brottsbekämpning förutsätter att de brottsbekämpande myndigheterna har ändamålsenliga verktyg för att bekämpa brott. Flera länder tillåter att de brottsbekämpande myndigheterna använder sig av hemlig dataavläsning som metod. I Danmark har hemlig dataavläsning använts sedan 2002. I Finland möjliggör relativt ny lagstiftning hemlig dataavläsning. Också Tyskland använder sig av en sådan metod. De olika länderna har reglerat metoden på olika sätt. Norge arbetar för närvarande med ett lagförslag om hemlig dataavläsning som ska presenteras för Stortinget. Viktiga lärdomar kan dras av hur andra länder till exempel har valt att avgränsa vilka brott som verktyget får användas för och hur överskottsinformation ska hanteras.

Beredningen för rättsväsendets utveckling (BRU) föreslog 2005 att hemlig dataavläsning skulle införas som ett nytt tvångsmedel i svensk rätt (SOU 2005:38). Som bakgrund till förslaget anfördes bl.a. att den organiserade brottsligheten alltmer söker sig till kommunikationsformer som är säkrare än telefoner, utnyttjar modern teknik och använder internet som ett arbetsredskap i verksamheten. Möjligheten att kommunicera på ett relativt anonymt och säkert sätt (främst frågan om kryptering) framhölls vid sidan av globaliseringen och mobiliteten som stora utmaningar som den internetrelaterade brottsligheten ställer upp för rättsväsendet. Beredningen bedömde det helt nödvändigt att de brottsbekämpande myndigheterna skulle ha möjlighet att använda effektiva arbetsmetoder, inte minst med anknytning till internet, för att den kvalificerade brottsligheten med dess struktur, inriktning och tillvägagångssätt skulle kunna bekämpas (SOU 2005:38, s. 360). Förslaget kritiserades av många remissinstanser och har inte lett till lagstiftning. Den huvudsakliga kritiken gällde att det föreslagna tvångsmedlets effektivitet och integritetseffekter inte ansågs tillräckligt klarlagda. Dessutom ifrågasatte flera remissinstanser om beskrivningen av teknikutvecklingen var rättvisande och därmed om behovet av åtgärder var så tungt vägande att det motiverade ett nytt tvångsmedel.

På motsvarande sätt som BRU redovisade Utredningen om vissa hemliga tvångsmedel några år senare att det vid den kartläggning av tillämpningen av vissa hemliga tvångsmedel som utredningen genomfört hade framkommit att personer inom den organiserade brottsligheten ägnar stor möda åt att anpassa sin kommunikation så att myndigheterna inte ska kunna avlyssna den. Utredningen konstaterade att krypterade telefonitjänster används liksom e-post och att det finns exempel på hur gemensamma mejlkonton utnyttjas för att undgå att meddelanden sänds mellan konton (SOU 2012:44, s. 765).

Det är avgörande att de brottsbekämpande myndigheterna upprätthåller sin förmåga att bekämpa brott. Teknik- och samhällsutvecklingen innebär att det nu finns anledning att på nytt undersöka om hemlig dataavläsning bör införas som ett straffprocessuellt tvångsmedel. Vid en sådan bedömning måste det säkerställas att grundläggande rättigheter respekteras och att intrång i enskildas integritet minimeras.

Uppdraget att undersöka om hemlig dataavläsning bör införas som ett nytt straffprocessuellt tvångsmedel

Det finns inte någon fastställd definition av hemlig dataavläsning. Som utgångspunkt för en analys kan begreppet definieras som 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 används för kommunikation och därigenom få besked om hur utrustningen används i realtid och vilken information som finns i den. Detta kan t.ex. ske genom att en hård- eller mjukvara placeras, antingen fysiskt eller elektroniskt, via en eller flera trojaner, i en användares tekniska utrustning.

Enligt 2 kap. 6 § regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om intrånget sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Överväganden om att införa regler om hemlig dataavläsning i svensk rätt fordrar en avvägning mellan å ena sidan samhällets behov av en effektiv brottsbekämpning och å andra sidan den enskildes rätt till integritet i förhållande till staten. Bara om hemlig dataavläsning bedöms vara en proportionerlig åtgärd kan den tillåtas. För att det ska vara möjligt att göra den avvägning som behövs måste det

inledningsvis fastställas om det finns ett reellt behov av hemlig dataavläsning som metod i brottsbekämpningen eller om den brottsbekämpande förmågan kan upprätthållas med mindre integritetskänsliga metoder. Hur stort behovet av hemlig dataavläsning kan bedömas vara beror bl.a. på hur den moderna brottsligheten ser ut och samhällsutvecklingen i övrigt. Den tekniska utvecklingen och de förändrade förutsättningar för kommunikation som den medfört behöver särskilt uppmärksammas. Endast under förutsättning att behovet är tungt vägande och grundligt redovisat kan det ligga till grund för fortsatta överväganden om att införa metoden.

Nästa fråga blir i vilken utsträckning hemlig dataavläsning kan förväntas vara en effektiv metod för brottsbekämpning i förhållande till behovet. Svaret på den frågan är i stor utsträckning beroende av hur metoden tekniskt kan utformas. Undersökningen ska utgå från de tekniska möjligheter som finns och beakta de svårigheter vid verkställighet som kan förutses. Frågan hur bearbetning av information som inhämtas genom metoden kan förväntas gå till kommer att ha betydelse liksom hur myndigheterna ska skaffa den tekniska förmåga som krävs för att använda metoden. Risken för att de personer som begår brott anpassar sitt beteende för att komma runt de nya övervakningsverktygen och hur det skulle påverka effektiviteten behöver beaktas. Även frågan om vilka resurser metoden förutsätter bör belysas.

Behovet och den förväntade effekten behöver vidare bedömas utifrån olika brott. Hemlig dataavläsning skulle kunna vara en effektiv metod för att bekämpa terroristbrottslighet. Det kan även finnas andra allvarliga brott som hemlig avlyssning av elektronisk kommunikation får användas mot och som är svåra att utreda utan tillgång till hemlig dataavläsning.

Behovet och den förväntade effekten behöver också belysas utifrån olika syften med åtgärden. Straffprocessuella tvångsmedel kan användas både i syfte att förhindra och att utreda brott. Behovet kan skilja sig mellan dessa användningsområden. Exempelvis har behovet av att kunna använda hemlig rumsavlyssning i preventivt syfte bedömts vara mindre än motsvarande behov för andra hemliga tvångsmedel (prop. 2013/14:237 s. 101). Hemlig avlyssning kan användas både för att förhindra och utreda brott medan hemlig rumsavlyssning enbart är tillåtet för att utreda brott inom ramen för en förundersökning. Behovet av den tänkta åtgärden kan också vara

olika för olika brott. För effekten av tvångsmedlet är det vidare av betydelse vilka beviskrav som ska ställas på tvångsåtgärdens betydelse för det fastställda ändamålet med åtgärden.

Varje befogenhet för staten att bereda sig tillgång till information om medborgarna leder till ingrepp i den personliga integriteten. Ramarna för intrånget bestäms av hur befogenheten avgränsas och utformas i lag. En behörighet för brottsbekämpande myndigheter att i realtid hemligt läsa information i och från datorer och andra tekniska utrusningar, t.ex. mobiltelefoner, skulle potentiellt kunna innebära ett mycket omfattande intrång i enskildas privatliv. Vid överväganden om hemlig dataavläsning måste därför integritetseffekterna beskrivas noga. Det måste så långt det är möjligt redogöras för hur skyddet för den personliga integritetens kärnområden, dvs. sådant som rör individen och dennes personlighet, skulle påverkas av hemlig dataavläsning, bl.a. risken för att andra personer än den som är föremål för tvångsåtgärden påverkas. Regleringen av bland annat hur överskottsinformation får användas och hur tillsyn ska utföras spelar en viktig roll i denna bedömning. Behovet och den förväntade nyttan av att kunna använda hemlig dataavläsning för de olika syftena där ett behov har identifierats måste vägas mot det förväntade integritetsintrånget av en sådan användning. Även frågor om hur metoden skulle påverka enskildas egendomsskydd när det gäller tekniska utrustningars lagringsutrymme (eventuella begränsningar i överföring av datamängd och kapacitet) och kostnader för enskilda behöver beaktas.

Oavsett hur avgränsningen mellan integritets- och effektivitetshänsyn utfaller är det ett ovillkorligt krav att de bestämmelser som föreslås uppfyller högt ställda krav på rättssäkerhet. Det finns därför anledning att noga analysera vilka kvalifikationskrav som är nödvändiga för tillämpningen, hur beslutsordningen bör se ut, hur efterhandskontroll och övrig tillsyn bör fungera, hur underrättelseskyldighet till enskilda bör utformas, hur jurisdiktionsreglerna kan upprätthållas och hur användningen av överskottsinformation ska regleras.

Utredaren ska

- ta reda på vilket behov de brottsbekämpande myndigheterna har av att hemligt i realtid bereda sig tillgång till information i datorer och andra tekniska utrustningar för att effektivt kunna fullgöra sin uppgift, bl.a. i förhållande till övriga metoder för att bekämpa

brott inklusive övriga (hemliga) tvångsmedel, och vid analysen särredovisa Åklagarmyndighetens, Ekobrottsmyndighetens, Polismyndighetens, Säkerhetspolisens och Tullverkets behov,

- undersöka vilka möjligheter som modern teknik kan ge de brottsbekämpande myndigheterna att i realtid i hemlighet läsa information i datorer och andra tekniska utrustningar och vilka begränsningar som följer av tekniken och av möjligheten att använda motmedel mot en sådan åtgärd,
- kartlägga och med beaktande av eventuell sekretess beskriva hur en sådan metod kan förväntas verkställas och avbrytas eller avslutas inklusive de operativa svårigheterna med detta,
- analysera i vilken utsträckning det kan bidra till en effektiv brottsbekämpning att ge brottsbekämpande myndigheter befogenhet att i realtid i hemlighet läsa information i datorer och andra tekniska utrustningar,
- undersöka vilket integritetsintrång detta skulle medföra för enskilda och beskriva vilka avgränsningar som behövs,
- utifrån en avvägning mellan effektivitets- och integritetsskäl ta ställning till om de brottsbekämpande myndigheterna bör ges möjlighet att använda hemlig dataavläsning för att bekämpa terroristbrottslighet och andra allvarliga brott, som i dag ger möjlighet till hemlig avlyssning av elektronisk kommunikation,
- avgöra de närmare förutsättningarna för en sådan användning bl.a. i fråga om syfte, tillämpningsområde och rättssäkerhetsgarantier i enlighet med Europakonventionen och den praxis som Europeiska domstolen för de mänskliga rättigheterna har utvecklat,
- ta ställning till i vilken utsträckning åtgärden ska kunna användas i det internationella rättsliga samarbetet, och
- lämna förslag till författningsändringar eller andra förändringar oavsett vad analysen föranleder.

Vid utarbetandet av lagförslag ska utredaren så långt som det är möjligt välja en teknikneutral reglering. Uppgifter i utredningen ska redovisas med beaktande av eventuell sekretess. Utredaren är fri att

lämna sådana närliggande förslag till författningsändringar som bedöms vara nödvändiga.

Ekonomiska konsekvenser

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för staten, kommuner och landsting och konsekvenserna i övrigt av förslagen. Om förslagen förväntas leda till kostnadsökningar för staten, kommuner och landsting, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska också redovisa i vilken utsträckning resursutnyttjandet i rättsväsendet kan bli effektivare genom förslagen.

Lagstiftning i andra länder

Utredaren ska redovisa gällande rätt och eventuellt pågående arbete i övriga nordiska länder samt de övriga länder som bedöms vara relevanta för utredningsuppdraget och i övrigt göra de internationella jämförelser som utredaren bedömer befogade.

Samråd och redovisning

Utredaren ska vid genomförande av uppdraget inhämta upplysningar från företrädare för berörda myndigheter och organ, särskilt Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden, Post- och telestyrelsen och Sveriges advokatsamfund.

Utredaren ska också hålla sig informerad om och beakta sådant arbete inom Regeringskansliet samt inom EU och andra internationella forum som är relevant för uppdraget. Utredaren ska särskilt uppmärksamma det pågående arbetet inom ramen för utredningen om moderna regler om beslag och husrannsakan (dir. 2016:20) och samordna sina bedömningar med den utredningen i den utsträckning det behövs.

Uppdraget ska redovisas senast den 13 november 2017.

(Justitiedepartementet)

Brottsbekämpande myndigheters behovsbeskrivningar

Under utredningsarbetet har experterna från de brottsbekämpande myndigheterna av utredningen ombetts redogöra för det behov som de anser föreligger av att få använda hemlig dataavläsning. Utredningen har löpande fått in behovsbeskrivningar, vilka efter frågor, påpekanden och synpunkter från utredningen har kompletterats i olika avseenden. I denna bilaga redovisas, i enlighet med direktivens krav på särredovisning av Åklagarmyndighetens, Ekobrottsmyndighetens, Polismyndighetens, Säkerhetspolisens och Tullverkets behov, de behovsbeskrivningar som utredningen fått in från experterna såsom samlade och slutliga dokument.

Säkerhetspolisen

Säkerhetspolisens behovsbeskrivning avseende hemlig dataavläsning

Inledning

Samhällsutvecklingen har inneburit en mycket hög grad av digitalisering. Den utvecklingen fortsätter i rask takt. I stort sett alla använder idag elektronisk kommunikation i såväl privat- som arbetslivet. Nya tekniska lösningar utvecklas hela tiden.

De personer som ägnar sig åt brottslig verksamhet ligger ofta i framkant när det gäller att utnyttja de möjligheter som ges. Man är högst medveten om vilka legala och praktiska begränsningar som finns för de brottsbekämpande myndigheterna och anpassar sina modus i syfte att försvåra eller omöjliggöra för myndigheterna att få fram information.

Samtidigt som många idag ger offentlighet åt sitt privatliv på sociala medier har integritetsskydd blivit ett naturligt inslag i utvecklingen av de digitala tjänster som gemene man använder. Integritetsskyddet medför bl.a. att såväl innehållet i kommunikation som lagrad information skyddas och gör att personer kan agera dolt och anonymt.

Det nu sagda innebär en mycket stor utmaning för de brottsbekämpande myndigheterna, och för lagstiftaren.

Kryptering

Den tekniska utvecklingen leder till ökad och bredare användning av elektroniska tjänster som är skyddade och säkra. I stort sett samtliga appar och program som används för kommunikation är konstruerade på det sättet. Det har fått till följd att värdet av att använda flera av dagens tvångsmedel har minskat markant över tid. Exempelvis ger hemlig avlyssning av elektronisk kommunikation (HAK) idag långt färre uppgifter än tidigare, främst beroende på att de som kommunicerar har skyddat innehållet med kryptering eller använder tjänster som ger anonymitet. Konsekvensen kan bl.a. bli att miss-

tankar varken kan bekräftas eller avfärdas och att utredningar måste läggas ned, med följd att den brottsliga verksamheten kan fortsätta.

Kryptering kan medföra att innehållet i kommunikationen, lagrad information (t.ex. i hårddiskar, telefoners inbyggda minnen, USB-minnen och enskilda filer) och uppgifter om kommunikationen (trafikuppgifter) inte går att komma åt och att användarna förblir anonyma. De tjänster som finns på marknaden är lättillgängliga och användarvänliga och skapar allvarliga hinder i det brottsbekämpande arbetet. Det är av yttersta vikt att myndigheternas förmåga att bekämpa brottslighet med hjälp av hemliga tvångsmedel upprätthålls genom att problemen med bl.a. kryptering får en lösning.

Den kommunikation som en användare har med olika tjänster, som exempelvis Skype, Twitter, Instagram, Viber, FaceTime, WhatsApp, Signal, iMessage och Facebook, eller med andra användare av tjänsten, är vanligtvis krypterad. Det är också möjligt att skapa en krypterad tunnel eller länk (VPN) över internet där kommunikation kan ske skyddat punkt-till-punkt. Hemlig avlyssning eller övervakning av elektronisk kommunikation ger då mycket begränsad information. Därför är sådana kommunikationssätt mycket vanliga i kriminella kretsar, oavsett vilken brottslighet det rör sig om. Detsamma gäller krypterade VoIP-tjänster (Voice over IP), som Skype, Viber, Google talk, Signal och Wickr. Även vanliga kommersiella bolag (t.ex. hotell, resebolag, banker, restauranger, affärer och hyrbilsfirmor) liksom myndigheter använder kryptering (SSL, https:) i sin kommunikation med kunderna och allmänheten.

Vid kryptering försvinner också möjligheten att identifiera samtalsparterna via rösten eller andra ljud. Även om de brottsbekämpande myndigheterna alltså vet att ett samtal har ägt rum, kan det bli svårt att dels identifiera hittills okända personer, dels knyta personer till ett specifikt samtal. Sådana uppgifter är många gånger avgörande för att nå framgång i utredningar.

Som nämndes är det inte bara kommunikationen i sig och uppgifter om kommunikationen som krypteras. Även den information som lagras kan skyddas. Dessutom kan kryptering ske i flera ”lager” samtidigt, dvs. samma information skyddas av flera krypteringar. Det kan röra kryptering av en enskild fil, kryptering av tjänsten som överför filen och kryptering i den tunnel eller länk som används.

Verktygen för kryptering är numera standard för alla att använda. Ofta ingår de som en del i operativsystemen, t.ex. IOS (Apple) och

BitLocker (Microsoft), och kräver endast enkla handgrepp hos användaren.

Anonymisering

Vid sidan av kryptering finns problemet med att brottslingar har som modus att göra sig anonyma på internet. Det kan ske på många olika sätt. Exempelvis kan man använda sig av anonyma förbetalda kontantkort eller koppla upp sig på trådlösa nät (WiFi-nät), t.ex. på restauranger, flygplatser, tågstationer, köpcentrum och hotell. På marknaden finns även anonymiseringstjänster, alltså internettjänster som ger användare möjligheten att skicka e-post, besöka webbplatser eller genomföra andra aktiviteter på internet anonymt. Tjänsterna fungerar vanligtvis så att användarens IP-adress byts mot en anonym sådan, vilket dessutom kan ske i flera led.

Svårigheterna för de brottsbekämpande myndigheterna blir än större när krypterings- och anonymiseringstjänster används samtidigt. Ett sådant exempel är Darknet, vilket är ett virtuellt nätverk där det behövs speciell mjukvara, konfiguration eller behörighet för åtkomst. Darknet är allmänt känt som en plats där nästan all illegal näthandel med t.ex. vapen, droger och barnpornografi förekommer. En specifik tjänst som regelmässigt används vid kriminalitet är TOR (The Onion Router).

Ytterligare ett sätt att försvåra upptäckten av brottslig verksamhet är att använda sig av flera olika bärartjänster vid samma kommunikationstillfälle (t.ex. mobilnät, WiFi-nät, fasta bredbandsnät och företagsnät) och på så sätt ”fragmentera” sin kommunikation. Exempelvis kan användaren från sin utrustning utnyttja sociala medietjänster, VoIP och e-post samtidigt via olika bärartjänster.

Realtidsaktiviteter

I princip är alltid innehållet i kommunikationen och lagrad information intressant. Ett problem i sammanhanget är att de befintliga tvångsmedlen inte ger tillgång till uppgifter som varken kommuniceras till eller från utrustningen eller lagras i denna. Det ligger i sakens natur att möjligheten att få uppgifterna löpande i realtid många gånger kan vara helt avgörande för att identifiera brottsplaner, för-

hindra att brott fullbordas, avvärja överhängande fara, verkställa tvångsmedel och säkra bevis. Det som bl.a. kan vara av mycket stort värde är realtidsuppgifter om att utrustningen faktiskt används, om att tangentbord används, om innehållet i dokument eller meddelanden som skrivs, om inloggningsuppgifter, om att lagring sker på extern media t.ex. usb-minne, om att filer öppnas och om att program startas.

De uppgifter som varken kommuniceras eller lagras kan behövas före, under och efter verkställighet av tvångsmedel, som gripande, husrannsakan och beslag. De kan ge information om att en person finns på en viss plats vid en viss tidpunkt, om inloggningsuppgifter och om vilka lagringsmedia som ska eftersökas. Uppgifterna kan också behövas för att visa minneanteckningar eller annan tillfälligt upprättad dokumentation och för att se att en person redigerar kontaktlistor eller bilder, samt för att se om någon förändrar en säkerhetslogg eller öppnar ett dokument eller ett program vid givet tillfälle. Att öppna program kan innebära att personen sätter utrustningen i ”flygläge” och förbereder meddelanden för att senare snabbt kunna kommunicera.

Radering

Problemen bottnar i att kriminella personer är mycket medvetna om säkerheten. Det finns tydliga brottsmanualer på internet som används för att undvika att de brottsbekämpande myndigheterna får tillgång till uppgifter. Det gäller bl.a. hur raderingsprogram ska användas. Programmen gör att informationen försvinner så snart personen vill det, och den kan senare inte återskapas. Detsamma gäller nyare hårddiskar, där tekniken gör att den information som är raderad eller överskriven inte kan återskapas. Samma problem uppstår när de kriminella har som modus att slänga eller förstöra den utrustning som använts.

Lokalisering

I dagsläget har de brottsbekämpande myndigheterna möjlighet att få tillgång till positionen på en elektronisk kommunikationsutrustning genom hemliga tvångsmedel (HAK, HÖK och IHL). Lokaliserings-

uppgifter är ofta av fundamental betydelse i utredningarna för att klargöra var misstänka personer och deras utrustning har befunnit sig vid olika tidpunkter.

De kriminella är väl medvetna om att utrustning som kopplas upp mot kommersiella mobilnät kan positioneras. Ett problem i dag är att de lokaliseringsuppgifter som operatörerna lämnar vid tvångsmedlen många gånger är allt för oprecisa och kan avse ett relativt stort geografiskt område, i synnerhet i glesbygd. Ett annat problem är att om personen utnyttjar trådlösa nät (WiFi) så saknas ofta lokaliseringsuppgifter. Ett sätt att överhuvudtaget få sådana uppgifter eller i vart fall få mer precisa skulle vara att aktivera och utnyttja GPS-mottagaren som är inbyggd i utrustningen.

Identifiering

Även andra funktioner som kan aktiveras skulle kunna vara mycket värdefulla i utredningsarbetet. När det gäller kommunikation som sker genom textmeddelanden, alltså utan att ljud eller bild används, kan det vara mycket svårt att knyta någon till kommunikationen. Det kan vara fråga om fall där myndigheterna vet att någon i en viss krets av personer använder utrustningen, t.ex. i en familj, ett företag eller en organisation, utan att kunna binda en viss användare till kommunikationen, eller fall där användaren är helt okänd. De funktioner som då skulle vara aktuella att aktivera är kameran, för att ta en bild av personen, eller mikrofonen, för att kunna identifiera denne genom rösten. I båda fallen kan det också ges information om miljön där utrustningen finns.

Verkställighet av tvångsmedel

Kameran och mikrofonen skulle också kunna aktiveras som en ren verkställighetsåtgärd för hemlig kameraövervakning eller hemlig rumsavlyssning. De kriminella är generellt mycket medvetna om hur de brottsbekämpande myndigheterna får använda tvångsmedlen, inte minst de begränsningar som finns när åtgärderna ska verkställas. Det leder till att man använder vissa modus i kriminaliteten. Bland annat utnyttjar man det faktum att tillstånden måste vara knutna till viss förutbestämd plats. Därför väljer man att t.ex. ha möten på platser

som inte går att förutse från myndigheternas sida eller platser där tvångsmedlen inte får eller fysiskt kan verkställas. Man lämnar t.ex. inte en lokal obevakad, man växlar platser för möten och man vistas i geografiska områden som är svåra för andra att smälta in i. Kameran skulle också kunna användas för att säkerställa miljön inför framtida tvångsmedel, som gripande, husrannsakan och beslag.

Problemens omfattning

De problem som beskrivs är lätta att ”kvantifiera”. De förekommer i praktiken i någon form i samtliga ärenden som Säkerhetspolisen har och ger därmed fundamentala problem i brottsbekämpningen. Ofta är det först i verkställighetsstadiet som problemen visar sig, t.ex. när ett HAK-tillstånd verkställs. Problemen medför också att tvångsmedel inte ens begärs för att det bedöms vara utsiktslöst att åtgärden skulle resultera i något konkret.

Det är väl känt bland personer som ägnar sig åt grov brottslighet hur man ska agera för att utföra brotten och undgå upptäckt. Ett exempel på det är att man använder anonyma abonnemang och ny elektronisk utrustning under enstaka samtal för att därefter slänga eller förstöra SIM-kortet och utrustningen. Ett sådant agerande är mer regel än undantag och medför stora problem för de brottsbekämpande myndigheterna. Ett annat liknande exempel är raderingsprogrammen eller de nyare hårddiskarna som bl.a. genom brottsmanualer på internet blivit mer eller mindre standard vid vissa typer av brottslighet, särskilt den som innefattar barnpornografi. Den teknikutvecklingen fortsätter i rask takt och utgör ett stort och växande problem för myndigheterna.

Ovan nämndes att lokaliseringsuppgifter är av fundamental betydelse i utredningarna. Användningen av trådlösa nät (WiFi) är numera mycket stor i samhället. Att den användningen ger problem i brottsbekämpningen är väl känt av kriminella och utnyttjas i stor omfattning. Även detta är ett växande problem. Det ska också tilläggas att i flera utredningar som Säkerhetspolisen har haft har lokaliseringsuppgifterna från operatörerna varit allt för oprecisa för att vara avgörande när det gäller att knyta en person till en viss plats.

Behovet av att aktivera kamera eller mikrofon för identifiering har uppkommit eftersom teknikutvecklingen har inneburit att en stor

del av kommunikationerna i dagsläget sker genom textmeddelanden i någon form. Den utvecklingen kommer att fortsätta.

Effektiva alternativ saknas

Ett alternativt sätt att få fram information kan vara att Säkerhetspolisen får uppgifter genom fysisk spaning, från andra personer än den misstänkte, från myndigheter i andra länder eller från leverantörer av internettjänster. Detta är dock av flera skäl inga effektiva vägar, och i många fall inte ens möjligt. Syftet med kryptering och anonymisering är ju att skydda information. Tekniska lösningar byggs just för att komma runt insyn från myndigheter och andra. I vissa situationer kan också hemlig rumsavlyssning vara ett alternativ, dvs. att man får uppgifter genom att man fångar talet, i vart fall avseende en av samtalsparterna, innan det krypteras t.ex. vid ett Skypesamtal. På motsvarande sätt skulle även hemlig kameraövervakning i vissa lägen vara ett alternativ. Ett problem med båda tvångsmedlen är att tillstånden måste knytas till en viss plats och, när det gäller kameraövervakning, att det saknas laglig möjlighet att installera kameran i bostad.

Framgång för brottsbekämpningen förutsätter i praktiken att den misstänkte begår misstag i sin informationshantering. I något enstaka fall finns det också möjlighet för myndigheterna att skräddarsy en teknisk lösning eller att använda särskilda program för att knäcka lösenord (Brute force). Detta är dock mycket tids- och resurskrävande. Det finns heller inga garantier för framgång.

Det är oerhört otillfredsställande att framgång i utredningar om grov brottslighet kopplad till nationell säkerhet ska bygga på tur, särskilt som tur är väldigt sällan förekommande.

Exempel

Säkerhetspolisen ger nedan ett antal exempel på situationer där de nuvarande hemliga tvångsmedlen inte på långa vägar möter de behov som finns inom brottsbekämpningen. Exemplen bygger alla på verkliga situationer men har modifierats för att undvika att avslöja sekretessbelagda uppgifter.

Exemplen visar på de olika problem som hemlig dataavläsning kan lösa. Det är främst fråga om kryptering, anonymisering, realtidsaktiviteter, radering, lokalisering, identifiering och svårigheter att verkställa hemlig kameraövervakning och rumsavlyssning. Med stor sannolikhet kan hemlig dataavläsning även ge annan värdefull information i utredningarna utan att det särskilt påpekas i exemplen nedan. Exemplen är formulerade utifrån att det finns ett huvudsakligt problem där hemlig dataavläsning kan vara till hjälp.

Typfall 1

Säkerhetspolisen har information om att fem personer kan vara i färd med att planera terrorattentat i Sverige. De fem männen bor på visst avstånd från varandra och använder elektronisk kommunikation i kontakten mellan dem. Vid verkställighet av HAK hör Säkerhetspolisen hur personerna pratar med varandra om alldagliga saker men också att de ibland säger att ”vi tar Skype”. Det kan starkt misstänkas att man då pratar om de brott som planeras. Eftersom Skype, liksom t.ex. Twitter, Viber och Facebook, är en krypterad tjänst, kan Säkerhetspolisen inte få del av innehållet i kommunikationen.

Hemlig dataavläsning (HDA) skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information och om utrustningens position (GPS) både historiskt och i realtid.

Typfall 2

En privatperson tar kontakt med Säkerhetspolisen och informerar om att han blivit kontaktad av en man via en social medietjänst på internet. Så småningom har det framgått att mannens avsikter med kontakten har varit att få hjälp med information som bedöms vara av betydelse vid attentatsplanering mot Sverige. Vid kontakter med internetoperatören framgår att kontot som mannen använt vid kontakten tillhör en för Säkerhetspolisen känd person. Vid spaning får Säkerhetspolisen fram att personen använder en smartphone. Säkerhetspolisen får information om abonnemanget som mannen har men inga uppgifter om hans kommunikation. Säkerhetspolisen

misstänker att mannen utnyttjar trådlösa nät (WiFi) för att kommunicera anonymt.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning (smartphone), som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas.

Typfall 3

Vid en förundersökning framkommer information om att man från såväl den autonoma miljön som vit makt-miljön ”mobiliserar” inför en större händelse som är av intresse för båda sidor. Stämningen är så hatisk att det finns farhågor om att grovt våld kommer att användas. Vid den förundersökning som inleds försöker Säkerhetspolisen kartlägga de individer som kan vara inblandade. Det visar sig att man från båda sidor undviker att ha fysiska möten. I stället sker all kontakt via krypterade sociala medietjänster eller andra egenutvecklade slutna forum.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som de misstänkta kommunicerar med skulle kunna fastställas.

Typfall 4

Efter ett fullbordat terroristattentat utomlands får Säkerhetspolisen information från sin motsvarighet i det aktuella landet att någon av gärningsmännen har haft kontakt med flera IP-adresser som sannolikt är kopplade till en mobiltelefon i Sverige. Efter att information inhämtats från den aktuella operatören kan IP-adresserna knytas till en viss mobiltelefon, som har ett anonymt abonnemang. Genom uppgifter från HÖK kan innehavaren av mobiltelefonen

identifieras som en person med koppling till terroraktörer i Sverige. Vid avlyssning av telefonen visar det sig att den används endast för krypterad IP-baserad kommunikation.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas. Det gäller även i vilken miljö den misstänkte finns när han kommunicerar.

Typfall 5

Efter att ett terroristbrott fullbordats i Sverige står det klart att gärningsmannen måste ha haft hjälp av andra för att utföra dådet. Vid kartläggning av gärningsmannens kommunikationer framkommer att han haft ett flertal kontakter via internet med personer både i Sverige och utomlands. Säkerhetspolisen ser en uppenbar risk för att ytterligare attentat kan komma att genomföras inom en snar framtid och behöver få kontroll på vilka de övriga personerna är. Gärningsmannens datorer och telefoner tas i beslag. Undersökningen av föremålen visar att gärningsmannen strax före attentatet har haft kontakt med en IP-adress. När HÖK verkställs avseende den IP-adressen framkommer att kommunikation sker med andra IP-adresser såväl i Sverige som utomlands. En av IP-adresserna kan knytas till en sedan tidigare känd anhängare av våldsbejakande islamistisk extremism. När HAK verkställs visar det sig att den personens kommunikation är krypterad.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han kommunicerar.

Typfall 6

Säkerhetspolisen får information om att en gruppering inom vit makt-miljön planerar att bränna ner en flyktingförläggning på en mindre ort. En förundersökning om förberedelse till grov mordbrand inleds. Vid verkställighet av HAK kommer det fram att de misstänkta använder sig av Facebook men också motsvarande typ av tjänst i Ryssland. Man har också skapat egna slutna forum där endast särskilt betrodda medlemmar har fått inloggningsuppgifter. Samtliga kommunikationstjänster är krypterade.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som de misstänkta kommunicerar med skulle kunna fastställas liksom i vilken miljö de misstänkta finns när de kommunicerar.

Typfall 7

Flera personer lämnar information om att det inom ett slutet forum pågår en ”hatkampanj” mot de politiker som står bakom Sveriges flyktingpolitik. Flera av de inblandade har uttryckt en vilja att spränga lokaler där centrala statsledningen finns, och man har också efterfrågat vapen och sprängämnen. HAK har inte kunnat ge någon ytterligare information till utredningen eftersom all kommunikation är krypterad.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som de misstänkta kommunicerar med skulle kunna fastställas liksom i vilken miljö de misstänkta finns när de kommunicerar.

Typfall 8

Flera personer har lämnat information till Säkerhetspolisen om att två bröder, 17 och 19 år gamla, har radikaliserats snabbt. Deras närstående är mycket oroliga för att de kan agera okontrollerat. En av bröderna har haft kontakt med personer som kommer från samma bostadsområde och som befinner sig i Syrien för att slåss för IS. Bröderna har själva uttalat att de vill kriga för IS oavsett var i världen det sker. Vid verkställighet av HAK framkommer att en stor del av brödernas kommunikation, både med varandra och med andra, går via krypterade sociala medietjänster. Dessutom har bröderna kontakt med IP-adresser som vid kontroll visar sig innehas av mindre resebyråer utomlands. En av Säkerhetspolisens hypoteser är att bröderna försöker få stridstränade personer från Syrien att komma hem för att begå terroristbrott i Sverige. Eftersom kommunikationen med resebyråerna är krypterad går det inte att få klarlagt vad bröderna har för avsikt med kontakterna.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras.

Typfall 9

Säkerhetspolisen har konstaterat att en lägenhet används av flera personer som är kända i terrorkretsar. En förundersökning om stämpling till terroristbrott pågår och domstolen har beslutat om HAK avseende de misstänktas telefoner. Vid ett tillfälle under avlyssningen uttalar en av de misstänkta att han har information i sin dator men att den är krypterad och säker. Säkerhetspolisen bedömer att den informationen skulle kunna vara av mycket stort värde i förundersökningen och överväger att göra husrannsakan i lägenheten där datorn finns. En sådan kan dock inte ske öppet, eftersom det skulle riskera att spoliera utredningsresultatet. I lägenheten bor en familj där någon av familjemedlemmarna alltid är hemma, dvs. lägenheten är aldrig tom. Det finns med andra ord ingen möjlighet att i detta läge av utredningen komma åt informationen i datorn.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information och om aktiviteter som inte kommuniceras eller lagras.

Typfall 10

Säkerhetspolisen har via finanspolisen fått information om att en person, som sedan tidigare är känd av Säkerhetspolisen i terrorsammanhang, har blivit rapporterad av en bank för misstänkt penningtvätt. Uppgifterna från finanspolisen gör att misstankarna mot personen stärks och en förundersökning rörande finansiering av terroristbrott inleds. Uppgifter inkommer från banken, som visar att den misstänkte har överfört pengar till bankkonton utomlands. Vem som är innehavare av de utländska kontona framgår däremot inte. Den misstänktes kontakter med banken har uteslutande skett via internet och en specifik IP-adress har använts. Den misstänkte har avslutat kontot. Banken har ingen uppgift om att den misstänkte har bytt bank. Vid verkställighet av HAK framgår att den misstänkte kommunicerar med en IP-adress som innehas av en bank utomlands. Det är omöjligt att få uppgifter från banken. Eftersom kommunikationen med banken är krypterad går det inte att få fram vad kommunikationen rör.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras och om lagrad information.

Typfall 11

Vid övervakning av en känd underrättelseofficer upptäcker Säkerhetspolisen att hon har svårförklarliga kontakter med en person som vid kontroll visar sig vara anställd vid ett stort teknikföretag som levererar materiel till en myndighet inom det svenska försvaret. Efter kontakt med den aktuella myndigheten står det klart att mannen arbetar med teknik som direkt kan kopplas till verksamhet som rör rikets säkerhet. En förundersökning om grovt spionerі inleds. Vid

verkställighet av HAK går det att dra slutsatsen att hårddisken i mannens dator är krypterad. Det framkommer dessutom att en del av hans kommunikation sker via en applikation som inte är känd sedan tidigare och som är krypterad.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han kommunicerar.

Typfall 12

Vid verkställighet av HAK mot kända underrättelseofficerare framkommer att de undviker att prata om i sammanhanget känsliga saker i klartext över telefon. Det enda man säger efter att ha ringt upp varandra är ”WhatsApp”. Av sammanhanget är det lätt att dra slutsatsen att all konspiratorisk kommunikation sker via den tjänsten, där överföring av både tal och bild är krypterad.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om den miljö där de misstänkta finns när de använder utrustningen.

Typfall 13

Säkerhetspolisen misstänker att en viss person med tillgång till kvalificerat hemlig information har värvats som agent av en utländsk underrättelseofficer. Personen har bl.a. vid ett flertal tillfällen besökt det aktuella landet utan att berätta om det för sin arbetsgivare. Arbetsgivaren misstänker, efter att ha granskat säkerhetsloggar, att mannen sannolikt har kopierat hemliga uppgifter. Vid verkställighet av HAK framgår att kommunikationen till och från hans mobiltelefon och dator är krypterad.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustningar, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 14

En serie grova dataintrång sker mot flera myndigheter som hanterar mycket känsliga uppgifter med bäring på rikets säkerhet. Det är oklart vem eller vilka som står bakom brottsligheten, men intrången är till sin karaktär sådana att en förundersökning om grovt spionerі inleds. Intrången kan spåras till en server som finns i Sverige. Vid undersökning av servern framgår att den ofta kontaktas från en specifik IP-adress och att kommunikationen är krypterad. Vid kontroll med operatören fastställs att IP-adressen är hemmahörande hos ett mindre bolag inom IT-branschen. Det går däremot inte att fastställa vem som är användare eller vilket innehåll kommunikationen har. Säkerhetspolisen bedömer att bolaget inte kan kontaktas för upplysningar utan att utredningen röjs.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i bolagets utrustning, som kan ge information bl.a. om vilka som kommunicerar, innehållet i kommunikationen innan det krypteras och om lagrad information.

Typfall 15

Säkerhetspolisen har fått information om att en viss namngiven person har sagt till flera bekanta att hans högsta önskan är att dö och att han vill resa till Syrien, kriga för IS och bli martyr. Säkerhetspolisen vet sedan tidigare att han har försökt att resa till Syrien men stoppats av utländska gränskontrollmyndigheter. Om han inte kommer iväg så vill han göra något i Sverige och har börjat söka efter vapen och sprängämnen på internet, både i Sverige och utomlands.

Säkerhetspolisen kan genom spaning konstatera att han har tillgång till mobiltelefoner, och han har setts använda en bärbar dator, typ Ipad. En förundersökning om förberedelse till terroristbrott har inletts. När HAK-tillståndet ska verkställas går det att se att han kommunicerar i stor omfattning men det går inte att få fram med vem eller vilka och inte heller vilka websidor han besöker. Kommunikationen är krypterad. Kontroll av de IP-adresser som den misstänkte kommunicerar med leder inte utredningen vidare eftersom det sannolikt rör sig om TOR-kommunikation.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på de personer och den utrustning den misstänkte kommunicerar med (exempelvis användarID i en viss app, e-postadress, ljud, bild m.m.) skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 16

Efter information från en uppgiftslämnare driver Säkerhetspolisen en förundersökning om spionerі. En person misstänks för att ha kommit över uppgifter som omfattas av sekretess med hänsyn till rikets säkerhet. Det går dock inte att säga från vilken myndighet uppgifterna kommer. Det sannolika är att personen agerat från sin dator för att komma över uppgifterna. Vid verkställighet av HAK framgår att uppgifterna är krypterade och att gärningsmannen sannolikt nyttjar TOR, vilket gör att det inte går att fastställa vilken myndighet som blivit föremål för intrånget.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras och om identiteten på den utrustning den misstänkte kommunicerar med (exempelvis IP-adress, e-postadress m.m.), dvs. vilken eller vilka myndigheter det är fråga om.

Typfall 17

Säkerhetspolisen får information från en säkerhetstjänst i annat land att en person med diplomatisk immunitet misstänks ägna sig åt flyktingspionage och att han har kontakter med en kvinna i Sverige. En förundersökning om olovlig underrättelseverksamhet inleds. Det visar sig vid HAK att kvinnan ofta kommunicerar med en utländsk IP-adress och att kommunikationen är krypterad. Säkerhetspolisen misstänker att hon har kontakt med sina svenska uppgiftslämnare via den adressen.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position och om vilka den misstänkta kommunicerar med (exempelvis användarID i en viss app, e-postadress, ljud, bild m.m.). Även identiteten på personer som den misstänkta kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkta finns när hon använder utrustningen.

Typfall 18

Personer inom vit makt-miljön planerar att mörda en tongivande vänsteraktivist. Säkerhetspolisen får information om att det i gruppen finns personer med mycket hög teknisk kompetens. All kommunikation inom gruppen är krypterad. Bl.a. lämnar medlemmarna information till varandra i en krypterad molntjänst. Alla datorer som medlemmarna har är krypterade. Det visar sig under förundersökningen att molntjänsten finns i Sverige men det går inte att fastställa vilka datorer som har kontakt med tjänsten.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras och om lagrad information. Om det tekniska hjälpmedlet installeras i molntjänsten kan det ge information om det finns fler personer i gruppen än vad som är känt och om identiteten på annan utrustning som kommunicerar med tjänsten.

Typfall 19

Säkerhetspolisen har information om att en grupp män brukar hålla möten med muslimska ungdomar i en föreningslokal i ett utsatt område. Informationen säger att gruppen försöker rekrytera ungdomarna att åka till Syrien och ansluta sig till IS. Det finns indikationer på att en för Säkerhetspolisen känd anhängare av islamistisk extremism är gruppens ledare. Vid verkställighet av HAK visar det sig att operatören inte längre lagrar historiska uppgifter om inkommande samtal till den misstänktes mobiltelefon med anledning av EU-domstolens förhandsbesked i december 2016 om s.k. datalagring. Dessutom är realtidskommunikationen krypterad.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information (t.ex. kontaktlista och samtalslogg), om utrustningens position, om identiteten på de utrustningar den misstänkte kommunicerar med (exempelvis IP-adress, e-postadress m.m.) och om aktiviteter som inte kommuniceras eller lagras. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 20

En yngre man med kopplingar till vit makt-miljön blir misstänkt för grov allmänfarlig ödeläggelse genom att ha utlöst en sprängladdning vid en flyktingförläggning. Säkerhetspolisen misstänker att han har medhjälpare. Vid spaning kan det konstateras att den misstänkte använder både mobiltelefon och Ipad. Efter kontakt med operatörerna visar det sig att information om hans IP-adress och lokaliseringsuppgifter inte har lagrats med anledning av EU-domstolens förhandsbesked i december 2016 om s.k. datalagring.

HDA skulle ge möjlighet att fysiskt installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i kommunikationen innan det krypteras, om lagrad information, om utrustningens position samt om identiteten på de utrustningar den misstänkte använder själv och dem han kommunicerar med (exem-

pelvis IP-adress, e-postadress m.m.). Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 21

Genom bl.a. spaning mot en känd underrättelseofficer drar Säkerhetspolisen slutsatsen att hon har lyckats värva en agent i Sverige. Agenten är dock hittills okänd. Misstanken är att när underrättelseofficeren kommunicerar med agenten sker det genom att hon utnyttjar trådlösa nät (WiFi), främst på olika restauranger och ibland på hotell.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i underrättelseofficerens utrustning, vilket ger möjlighet att klarlägga identiteten på dem hon kommunicerar med, utrustningens position, vilka trådlösa nät hon använder och i vilken miljö den misstänkta finns när hon använder utrustningen.

Typfall 22

Vid förundersökning rörande försök till mordbrand riktat mot ett kommunalråd är misstanken att brottet utförts av personer inom den autonoma miljön, varav en är identifierad. Säkerhetspolisen har information om att ett e-postkonto har använts för kommunikation inom gruppen före, under och efter brottet. Det har skett på så sätt att personerna har skrivit meddelanden till varandra. För att undvika att avslöja kontakten mellan personerna och vilken information de ger till varandra, har meddelandena aldrig skickats iväg från kontot. I stället har de sparats som utkast och därigenom funnits tillgängliga för alla som haft lösenord till kontot.
HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som kan ge information bl.a. om innehållet i den personens kommunikation med e-postkontot innan det krypteras och om inloggningsuppgifter. Med hjälp av de uppgifterna kan ett tekniskt hjälpmedel för HDA installeras i e-postservern för att ge information om vilka utrustningar som har kommunikation med det aktuella e-postkontot.

Typfall 23

Vid Säkerhetspolisen bedrivs en förundersökning om förberedelse till terroristbrott där en man misstänks för att på internet samla in information om bombtillverkning och försöka köpa komponenter. Det finns uppgifter om att han håller på att sammanställa en ”terrorinstruktion” som ska spridas och att han inte är ensam i planeringen. Han kan ha medhjälpare som hittills är okända för Säkerhetspolisen. Vid verkställighet av HAK har det framkommit att hans kommunikation med andra liksom hans tekniska utrustning (dator och smartphone) är krypterade.

HDA skulle ge möjlighet att installera tekniskt hjälpmedel, som bl.a. registrerar tryckningar på tangentbordet, vilket ger tillgång till lösenord och den text den misstänkte skriver i realtid samt andra aktiviteter som inte kommuniceras eller lagras. Säkerhetspolisen skulle samtidigt kunna få information om innehållet i kommunikationen innan det krypteras, om lagrad information, t.ex. kontaktlista, samtalslogg och innehållet i dokument som skrivs eller har skrivits, och om utrustningens position. Även identiteten på personer som den misstänkte kommunicerar med skulle kunna fastställas, liksom i vilken miljö den misstänkte finns när han använder utrustningen.

Typfall 24

En svensk man, som tidigare lagförts för terrorrelaterade brott i annat land, har kommit tillbaka till Sverige. Säkerhetspolisen får upp ögonen för hans aktiviteter i ett ärende som rör terrorfinansiering. Säkerhetstjänsten i det andra landet uppger att den misstänkte tidigare haft som modus att radera informationen i telefon och dator. För detta har han använt särskilda program som innebär att uppgifterna inte kan återskapas. Det innebär att efter ett eventuellt beslag kommer informationen inte att finnas kvar och inte heller kunna återskapas.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustningar som kan ge information bl.a. om innehållet i kommunikationen, om lagrad information innan den raderas och om aktiviteter som inte kommuniceras eller lagras.

Typfall 25

Efter ett fullbordat terroristattentat i ett av våra grannländer får Säkerhetspolisen information om att en av de misstänkta gärningsmännen dagarna före dådet har haft kontakt med ett svenskt mobiltelefonnummer. Det rör sig om ett anonymt kontantkort. Misstanken i Sverige rör medhjälp till terroristbrott. Vid verkställighet av HÖK visar det sig att utrustningen inte används för vanliga telefonsamtal utan att den har varit uppkopplad mot internet vid ett flertal tillfällen.

HDA skulle ge möjlighet att installera ett tekniskt hjälpmedel så att utrustningens position blir klarlagd. Samtidigt kan åtgärden ge möjlighet att med hjälp av telefonens kamera och mikrofon identifiera personen som använder utrustningen.

Typfall 26

En teleoperatör lämnar information till Säkerhetspolisen om att en av dess anställda kan misstänkas för att lämna ut väldigt känslig teknisk information till främmande makt. Informationen har inte direkt bäring på rikets säkerhet men är av mycket stort värde för det aktuella bolaget i konkurrenshänseende. En förundersökning om grovt företagsspionerі inleds. Domstolen beslutar bl.a. om hemlig rumsavlyssning och hemlig kameraövervakning. Det visar sig att någon i mannens familj i stort sett alltid finns hemma i villan. Dessutom är det omöjligt att sätta upp en kamera riktad mot bostaden. Domstolens beslut bedöms inte kunna verkställas.
De beslutade tvångsmedlen skulle kunna verkställas genom att ett tekniskt hjälpmedel för HDA installeras i den misstänktes dator. På det sättet kan datorns inbyggda mikrofon och kamera användas.

Typfall 27

Efter ett brandattentat mot en moskébyggnad bedrivs en förundersökning om terroristbrott mot en skäligen misstänkt person. Mannen förekommer sedan tidigare i terrorsammanhang och mycket talar för att han inte är ensam gärningsman. Säkerhetspolisen bedriver fysisk

spaning mot honom och kan konstatera att han har många kontakter som han träffar på caféer på bostadsorten. Spanarna ser att mannen använder en smartphone och bedömer att det inte är möjligt att komma så nära samtalsparterna att det går att uppfatta vad som sägs. Ibland är det inte ens möjligt att se vilka personer han träffar. Domstolen beslutar om hemlig rumsavlyssning och hemlig kameraövervakning och anger som platser i tillståndet vissa caféer som han tidigare besökt. Tyvärr visar det sig när tvångsmedlen ska verkställas att han hela tiden väljer nya platser för sina möten. Domstolens beslut bedöms inte kunna verkställas.

De beslutade tvångsmedlen skulle kunna verkställas genom att ett tekniskt hjälpmedel för HDA installeras i den misstänktes smartphone. På det sättet kan mobiltelefonens inbyggda mikrofon och kamera användas.

Tullverket

Tullverkets behovsbeskrivning avseende hemlig dataavläsning under förundersökning

Bakgrund

Inledningsvis lämnas en kort bakgrundsbeskrivning av Tullverkets användning av hemliga tvångsmedel i myndighetens brottsbekämpande verksamhet.

Sedan den 1 januari 2007 bedriver Tullverket verksamhet med hemliga tvångsmedel i egen regi och i egna lokaler. Dessförinnan fick myndigheten ta hjälp av polisen för att kunna genomföra dåvarande hemlig teleavlyssning respektive hemlig teleövervakning. I dagsläget genomför Tullverket hemliga tvångsmedel både centralt och lokalt inom Samordnad teknisk inhämtning (STI). Här hanteras merparten av de hemliga tvångsmedel som regleras av 27 kap. rättegångsbalken, dvs. hemlig avlyssning av elektronisk kommunikation (HAK), hemlig övervakning med elektronisk kommunikation (HÖK) samt hemlig kameraövervakning (HKÖ). Genomförande av tillstånd till hemlig rumsavlyssning (HRA) har hittills skett med bistånd av polisen (nuvarande NOA). Genom STI förbereder Tullverket att med egen teknik och egna resurser genomföra HRA i vissa fall under 2017.

Nämnda hemliga tvångsmedel (inkl. s.k. postkontroll) används i ärenden med misstanke om grova brott, företrädesvis grov narkotikasmuggling, men även grov smuggling av alkohol, cigaretter, dopning och vapen. Förundersökningar i dessa ärenden sker alltid under ledning av en åklagare och bedrivs på tullkriminalavdelningar placerade inom Kompetenscenter gränsskydd (KCG) i Stockholm, Göteborg, Malmö och Umeå. Avdelningarna samarbetar med STI både centralt (i Stockholm) och lokalt (i Stockholm, Göteborg, Malmö och Umeå). Bedrivandet av denna verksamhet regleras dels genom föreskrifter (TFS 2014:7), dels genom olika interna styrdokument.

Tullverkets behov av hemlig dataavläsning

Fram till och med 2008 fungerade det tillfredsställande för den brottsbekämpande verksamheten i Tullverket att använda främst HAK och HÖK, ibland i kombination med en HKÖ i förundersökningar rörande misstanke om grova brott. Användningen av HRA i dessa förundersökningar är dock mer begränsad. Det finns flera orsaker till detta. Att använda HRA är resurskrävande och tekniskt komplicerat, och Tullverket har hittills varit beroende av hjälp från polisen för att kunna genomföra en buggning. Förutsättningarna för att använda HRA är nu på väg att ändras så att Tullverket ska kunna hantera tvångsmedlet med mindre användning av polisens teknik och personella resurser än tidigare.

Den tekniska utvecklingen inom kommunikationsområdet sker allt snabbare, samtidigt som dess användare i allt högre grad blivit medvetna om kravet på säkra lösningar för att skydda sin kommunikation. De personer som är inblandade i kriminell verksamhet utgör inget undantag i detta avseende, snarare tvärtom. Här går utvecklingen extra snabbt. Som ett alternativ till att använda billiga telefoner eller kontantkort som slängs efter en användning, nyttjas allt oftare en mer avancerad kommunikationsutrustning där all information krypteras innan den sänds iväg. Därmed går det inte längre att använda den information som inhämtats med tillstånd till HAK, eftersom detta tvångsmedel enbart fångar upp de krypterade meddelandena utan att ge tillgång till innehållet. Lösningen på problemet är att den brottsbekämpande verksamheten får tillgång till ett nytt hemligt tvångsmedel i form av hemlig dataavläsning (HDA).

För att Tullverket ska kunna bedriva förundersökningar med misstanke om grova brott som blir framgångsrika och ger resultat i form av fällande domar i domstol, behöver myndigheten få tillgång till information som är okrypterad. Ett behov som Tullverket delar med övriga myndigheter med brottsbekämpande verksamhet riktad mot grov organiserad brottslighet.

Tullverket behöver få tillgång till HDA vid misstanke om brott av den högre svårhetsgraden (grovt, synnerligen grovt), enligt bestämmelserna i lagen (2000:1225) om straff för smuggling (smugglingslagen, SL). Aktuella brott enligt smugglingslagen för användning av HDA är närmast grov narkotikasmuggling och synnerligen grov narkotikasmuggling (6 § tredje och fjärde styckena SL), grov smugg-

ling enligt 5 § SL (t.ex. alkohol, dopningsmedel) och grovt tullbrott enligt 8 § (t.ex. cigaretter). Med undantag för HRA som enbart får tillämpas vid misstanke om grov eller synnerligen grov narkotikasmuggling, kan övriga hemliga tvångsmedel tillämpas vid misstanke om grov smuggling eller grovt tullbrott. För att Tullverket ska kunna beivra sådan brottslighet som både är välplanerad, välorganiserad och flitig användare av olika typer av kommunikationsmedel, krävs bra verktyg. HDA är ett sådant verktyg som krävs, i synnerhet i de fall kommunikationen i form av meddelanden, filer, mappar etc. i utrustningen, är krypterad.

För att tillgodose Tullverkets behov av effektiva verktyg för att bekämpa grov organiserad brottslighet är det önskvärt att brottskatalogen för användning av HDA omfattar brott vars straffvärde överstiger fängelse i två år, dvs. grova brott. Om det förstnämnda inte anses genomförbart, anser Tullverket att straffvärdet för att få använda HDA bör utgå från brott vars straffvärde är minst fängelse i två år, dvs. grov narkotikasmuggling eller brott av högre svårhetsgrad.

Tullverket har behov av att kunna använda HDA för att inhämta information som är krypterad oavsett typ av kommunikationsutrustning. Beroende på typ av utrustning och hur tillståndet är utformat, kan HDA ge tillgång till all form av krypterad information inkl. ljud och bild. Sådan tillgång innebär att det kan säkerställas av att den som använder en persondator, läsplatta (ipad), notebook, mobiltelefon eller motsvarande kommunikationsutrustning, är den eller de personer som misstänks för det aktuella brottet.

Nämnda kommunikationsutrustningar är också i högsta grad mobila. Telefonhytterna är sedan länge borttagna och mobiltelefonen har ersatt fast telefoni. Datorerna är inte längre stationära utan lätta och bärbara. Detsamma gäller för ipad och notebook och liknande teknisk utrustning. I motsats till kravet för tillstånd till HRA eller HKÖ, bör därför tillstånd till HDA inte vara begränsat till en plats.

Misstänkta gärningsmän byter ständigt utrustning (t.ex. kastar bort billiga mobiler eller slänger sim-kort efter en användning). Detta tillsammans med den höga mobiliteten gör det svårt att koppla en misstänkt person till den kommunikationsutrustning som anges i tillståndet (t.ex. ip-adress, abonnemang etc.). För att säkerställa att HDA används för teknisk utrustning, som i sin tur används av den som är misstänkt för brott, bör tillstånd till HDA kopplas till person.

För att bli ett effektivt tvångsmedel som både är teknikneutralt och anpassningsbart, bör HDA kunna användas i kombination med andra hemliga tvångsmedel, som HDA + HAK och HÖK, HDA + HRA för ljud och HDA + HKÖ för bild (genom kameran i datorn).

Två aktuella exempel från Tullverkets STI-verksamhet på ärenden som inte gått att driva vidare på grund av kryptering.

– Ett nyligen avslutat ärende gällde storskalig smuggling av narkotika (cannabis och kokain), från Spanien via Nederländerna till Sverige och Norge. De misstänkta i ärendet använde sig till stora delar av samtal och meddelanden via krypterade appar, bl a Skype, Viber, Messenger och Facebook.

  Ärendet drevs i nio månader med tillstånd till hemliga tvångsmedel i form av HAK, HKÖ och HRA, men utan framgång. Under denna tid gjordes mindre beslag i ärendet, vilket påvisade att det kommer in narkotika i landet. Det finns teorier om hur och när narkotikan kommer in, men detta har inte gått att styrka med hjälp av befintliga hemliga tvångsmedel.

– I ett pågående ärende bedrivs förundersökning med hemliga tvångsmedel mot en organisation som misstänks smuggla in omfattande mängder kokain till Sverige från Sydamerika. De misstänkta huvudmännen använder flertalet mobiltelefoner, varav många s.k. smartphones. Den ene huvudmisstänkta har sju mobiltelefoner inkopplade. Den trafik som kan avlyssnas med tillstånd till HAK och HÖK bedöms som mycket ringa. De misstänkta huvudpersonerna har vid flertalet tillfällen setts prata i mobiltelefon, men inga samtal har kommit in via systemet för HAK.

Användningen av dagens hemliga tvångsmedel har sina begränsningar, dels genom att viss information sänds krypterad, dels genom kravet på specifika tekniska uppgifter (t.ex. telefonnummer, adress), samt genom att tillstånd till vissa tvångsmedel är knutna till en geografisk plats.

Tillstånd till HAK och HÖK är knutet till uppgift om en specifik teknisk utrustning i form av ett telefonnummer eller annan adress eller till en viss elektronisk kommunikationsutrustning kopplad till

den misstänkte. Tillgång till sådan information har på senare år försvårats genom att den sänds krypterad.

Tillstånd till HRA ger enbart åtkomst till ljud och ställer krav på en teknisk installation som genomförs fysiskt på en viss plats, inom- eller utomhus. Kravet på en specifik plats i kombination med att det kan vara svårt att identifiera vem som säger vad i utrymmet som är föremål för avlyssningen, samt vad som sägs på grund av ohörbarhet, medför svårigheter att använda buggning. Dessutom är det resurskrävande då tvångsmedlet kräver omfattande fysisk spaning.

Tillstånd till HKÖ ger enbart tillgång till bild och information om vem eller vilka personer som befinner sig på en viss plats, men ingen information om vad som sägs på denna plats. För att få tillgång till både ljud och bild kan tillstånd meddelas både för HRA och HKÖ för en viss plats. Medgivandet är dock i flera avseenden begränsat. Tillstånd till dessa tvångsmedel är kopplat till ett tillträde till platsen för installation (tillträdestillstånd) och får inte avse någons stadigvarande bostad, dvs. inte heller den misstänktes bostad.

De brottsbekämpande myndigheterna ligger mer än tio år efter den tekniska utvecklingen. Rent generellt kan konstateras att teknikutveckling varken är ond eller god men att den påverkar. Den accelererande tekniska utvecklingen inom området kommunikation med en mångfald av sociala medier gynnar inte bara allmänheten, utan även brottsligheten. Den senare tycks ligga i framkant när det gäller att dra nytta av den senaste nyheterna på området, inklusive möjligheten att kunna kommunicera på ett säkert sätt – utan risk för att bli avlyssnade.

Problemet med bland annat krypterad information fanns redan för drygt tio år sedan. Redan då framfördes farhågor rörande den s.k. IT-relaterade brottsligheten och dess möjligheter till anonymitet och säkerhet (främst kryptering), som tillsammans med globaliseringen och mobiliteten utgjorde stora utmaningar för rättsväsendet (SOU 2005:38 s. 51). Sedan dess har utmaningarna bara blivit flera. Mobiltelefonerna bli allt smartare och därmed mer mångsidiga, olika typer av kommunikationsutrustning har blivit allt vanligare, likaså sociala medier i olika former där användaren erbjuds anonymitet och säkra lösningar i form av olika krypteringsmetoder. Betalning görs med bitcoin, en ny typ av valuta baserad på kryptoteknik, där betalning sker direkt mellan användare utan mellanhänder, vilket gör det svårare att spåra transaktioner mellan köpare och säljare. Allt detta

underlättar för kriminaliteten, men försvårar för de brottsbekämpande myndigheterna att bekämpa den grova organiserade brottligheten.

Även om problemet med kryptering kan lösas rent tekniskt, så kvarstår fortfarande problemen med hög mobilitet i förhållande till nuvarande krav på specifika tekniska uppgifter för tillstånd till HAK. Motsvarande gäller för kravet på plats för tillstånd till HKÖ och HRA. Dagens olika typer av kommunikationsutrustningar är tekniskt avancerade. Samma utrustning kan ofta samtidigt användas för flera olika ändamål, dvs. både för skrift, tal och bild (t.ex. pc eller mobiltelefon). Ett tillstånd till HDA kan, beroende på hur det utformas, täcka samtliga (eller enbart enstaka) behov. I kombination med att ett tillstånd till HDA riktas mot person och görs oberoende av plats, ökar förutsättningarna för att detta kan bli det verktyg som de brottsbekämpande myndigheterna behöver för att nå framgång i sitt arbete med att bekämpa grov kriminalitet.

Inledande problembeskrivning

Att i stort sett all tillgänglig information numera är krypterad medför:

- Minskad tillgång till information om brottsplaner
- Försvårande av kartläggning och planering av tillslag
- Svårigheter att koppla ihop använt datamedium med misstänkt person
- Längre förundersökningstider
- Låsta (krypterade) beslag
- Svårare bevisläge
- Resurskrävande utredningar
- Högre utredningskostnader
- Nedlagda förundersökningar
- Bortval av förundersökningar
- Färre brottsmisstänkta som åtalas och döms i domstol
- Ökad tillgång till narkotika i samhället.

Enligt STI medför den frekventa användningen inom kriminella organisationer av olika mobiltelefoner, datorer och andra elektroniska kommunikationsutrustningar som byts ut, byter ägare osv. att det försvårar för Tullverket att få kännedom om *vem* som använder *vilken* utrustning vid *vilket* tillfälle. Den omfattande användningen av datatrafik i olika sociala medier gör det svårare för den brottsbekämpande verksamheten att kartlägga de misstänkta personernas brottsliga planering. Inte minst gäller detta för det övre skiktet i dessa kriminella nätverk som, trots stora och dyra satsningar i dessa förundersökningar, är svåra att kartlägga och utplåna. Detta eftersom personer som misstänks tillhöra det övre kriminella skiktet i en organisation eller nätverk inte alltid är fysiskt närvarande vid ett tillslag, t.ex. av ett narkotikaparti eller en kurir.

Tekniken i de hemliga tvångsmedel som används idag är i vissa fall kostsam att köpa in, tidskrävande och svår att montera och har brister i den tekniska kvalitén. Detta gäller främst kameror för hemlig kameraövervakning och avlyssningsutrustning för hemlig rumsavlyssning. För det senare försämras ljudkvaliteten av att det är lätt att störa sådan avlyssningsutrustning med radio, tv eller annan ljudkälla. Att granska ljud och bild i efterhand från dessa tvångsmedel är tidskrävande, vilket medför längre förundersökningstider och högre kostnader.

I takt med att användningen av olika datamedier stadigt ökar i kriminella kretsar har det blivit allt svårare för den brottsbekämpande verksamheten att slå ut organisatörerna och nätverken som systematiskt organiserar och finansierar brottslig kriminell verksamhet. Detta medför i sin tur att Tullverket inte får kunskap om inkommande leveranser av t.ex. narkotika. Vi får heller inte information om kontakter eller samtal mellan misstänkta personer som kan vara avgörande för att kunna planera och genomföra ett tillslag vid rätt tillfälle och på rätt plats. I vissa fall beror Tullverkets framgångar i ett ärende snarare på de misstag som görs av de misstänkta, än med hjälp av tillräckligt bra tekniska hjälpmedel.

Den brottsutredande verksamheten inom Tullverket anger att i kriminella kretsar är det numera *välkänt* att de brottsbekämpande myndigheterna använder hemliga tvångsmedel, *vilka* dessa är och *hur* de används. De kriminella nätverken har anpassat sitt beteende efter denna kunskap. Idag är det sällsynt att brottsmisstänkta personer pratar om nära förestående eller pågående brott i sina telefoner.

Under senare år, från ca 2010 och framåt, har Tullverket fått allt svårare att lyckas med sina utredningsärenden trots användningen av hemliga tvångsmedel. Nuförtiden får vi ytterst lite information från de traditionella hemliga tvångsmedlen, eftersom de misstänkta har övergått till att kommunicera via krypterade media som exempelvis Wickr, Viber, Skype, WhatsApp, Facetime, Superspot m.fl. Bara under 2016 har detta problem ökat kraftigt. Vi har även sett att man använt sig av krypterade Blackberry-telefoner. Här använder man sig inte av standardkrypteringen utan har specialombyggda telefoner utan mikrofon, för att endast kunna texta meddelanden till varandra.

Brottsutredningen har haft ärenden där alla nu gällande hemliga tvångsmedel har använts, inklusive hemlig rumsavlyssning, utan att problemet med att informationen i ärendet är krypterad har gått att lösa.

Krypterad information är idag vanligt förekommande i alla typer av projekt (förundersökningar) där Tullverkets brottsutredning använder hemliga tvångsmedel. Exempel på detta är att man per telefon säger att man går över till annan media som Skype, Viber, WhatsApp etc, då man ska prata ”ostört”. Informationen går då inte att avlyssna eftersom den är krypterad. I beslagtagen media använder man sig ofta av någon form av kryptering för att skydda sin information.

Konsekvensen av att merparten av den information som eftersöks är krypterad blir dels att vi inte kan beslagta narkotika och gripa misstänkta, dels att förundersökningarna måste läggas ned, samt att ingen kan åtalas eller dömas för det misstänkta smugglingsbrottet. I de fall det trots bristen på relevant information har varit möjligt att beslagta narkotika och lagföra misstänkta personer så har det oftast varit fråga om personer i den ”nedre delen” av nätverket som har lagförts. De misstänkta huvudmännen går då fria.

Dessa personer befattar sig sällan med narkotikan och det enda sättet att kunna binda dem till brottet är genom att kunna uppvisa den kommunikation som föregått mellan misstänkt huvudman och kuriren, i samband med planering och genomförande av brottet. I bästa fall blir resultatet att vi lyckas gripa och lagföra kuriren och någon i nätverket som skickas ut för att möta upp kuriren. Däremot saknas bevisning för kunna lagföra huvudman, mottagare eller leverantör.

I en utredning av ett nätverk där man inte använder krypterad kommunikation, jämfört med det motsatta, uppskattas tidsåtgången från det att ärendet startas till dess att ett tillslag kan genomföras till 1 – 2 månader. Efterföljande brottsutredning går dessutom snabbt när det finns bra bevisning i de avlyssnade samtalen som inte är krypterade.

Är kommunikationen i ärendet däremot krypterad arbetar man ofta minst sex månader upp till ett år, innan det slutar med att man oftast måste lägga ned ärendet utan att ha få något resultat i form av beslag och lagföring av misstänkta personer. I dessa fall har man även använt hemliga tvångsmedel, inklusive hemlig rumsavlyssning, på personer i nätverket runt omkring den huvudmisstänkte, utan resultat.

Problemet med krypterad information måste få en lösning, annars riskerar både Tullverket och övriga brottsbekämpande myndigheter att komma ännu längre efter i den tekniska utvecklingen. Hemlig dataavläsning innebär en möjlighet för myndigheterna att kunna begränsa inhämtningen av information till sådan som är väsentlig för utredningen, och därmed säkra bevisning samt förkorta förundersökningstiden.

Tullverkets IT-forensiker delar den problembild som har framförts av forensiker i andra brottsbekämpande myndigheter. Våra forensiker undersöker samma typ av objekt eller enheter (t.ex. mobiltelefoner, datorer och annan elektronisk utrustning), och den data som ska analyseras är oftast skyddad på något sätt. En fråga som allt oftare återkommer vid varje beslagstillfälle är: ”– Hur väl skyddad är informationen?”

Mobiltelefoner, i synnerhet Apples IOS version 9 och uppåt samt iPhone och iPad, är alltid är krypterade och därmed omöjliga att få åtkomst till information utan tillgång till låskoden. Antalet försök att mata in låskoden är dessutom begränsat. Även Android erbjuder numera användaren möjligheten att kryptera innehållet. För Android kan det vara problematiskt att få åtkomst till innehållet utan låskoden, även om informationen inte är krypterad. Detta eftersom antalet försök att mata in låskoden även här är begränsat. Datorer från Apples har inbyggd kryptering (Filevault2) som enkelt kan aktiveras av användaren.

Utöver beslagtagna krypterade enheter så förekommer även krypterad kommunikation i Tullverkets ärenden. Krypteringen kan ske med s.k. appar i mobilen, eller med hjälp av en krypterad webb-

posttjänst, t.ex. Countermail. Tullverket kan inhämta information om e-post från operatören. Men den information som levereras av operatören är då oftast krypterad. För att kunna dekryptera meddelandena behövs ett lösenord eller s.k. nycklar. Operatören har inte tillgång till dessa lösenord eller nycklar, då de sparas i datorn. Med hjälp av hemlig dataavläsning bör det vara möjligt att kunna ”avlyssna” inmatningarna för att för att fånga upp lösenordet, som sedan kan användas för att dekryptera meddelandena.

Idag finns det flera kostnadsfria programvaror på marknaden som gör att användaren både kan kryptera och dölja sina aktiviteter, vilket försvårar och även helt förhindrar för en IT-forensiker att få tillgång till den eftersökta informationen.

Tullverkets IT-forensiker kan inte själva installera mjukvara eller kamerautrustning för inspelning av lösenord i en dator. För att göra detta möjligt krävs fysisk tillgång till datorn, eller att det på annat sätt görs möjligt att installera mjukvara som tillåter övervakning av datorns system. Tillgång till hemlig dataavläsning ger en sådan möjlighet.

Problemens omfattning

Omfattningen av problemet med krypterad information bygger i dagsläget inte på faktiska siffror utan mer på en uppskattning. Inom STI uppskattas att ca 90 procent av all trafik som inhämtas med hjälp av hemlig avlyssning är krypterad, vilket medför ett stort informationsbortfall i de enskilda ärendena.

Antalet beslag av olika typer av enheter som är krypterade varierar kraftigt beroende på var i landet beslagen görs. Högsta andelen krypterade enheter finns i storstadsområdena som Stockholm, Göteborg och Malmö. Den lägsta andelen återfinns i norrlandsregionen där kryptering förekommer i ca 10 procent av beslagen. Inom storstadsområdena uppskattar man att ca 50 – 80 procent av de beslag som görs av olika objekt är krypterade. Merparten av dessa beslag består av mobiltelefoner, s.k. smartphones, som är låsta. För att få tillgång till informationen i telefonen behövs ett lösenord.

Antalet ärenden på årsbasis (januari 2015 – december 2016) där hemliga tvångsmedel har använts i utredningsverksamheten varierar mellan de olika huvudorterna (Stockholm, Göteborg och Malmö).

Här har det varit svårt att få fram exakta uppgifter. Enligt uppgift har brottsutredningen i Stockholm haft ca tio ärenden med hemliga tvångsmedel (oktober 2015 – oktober 2016), varav tre av dessa ärenden har försvårats eller varit omöjliga att driva vidare på grund av krypterad information. Under en något längre period (januari 2015–december 2016) har brottsutredningen i Göteborg startat 19 ärenden med hemlig avlyssning och hemlig övervakning av elektronisk kommunikation. Av samtliga ärenden har endast två varit framgångsrika med hjälp av hemliga tvångsmedel. Sju av ärendena har inte lyckats alls på grund av att kommunikationen gått via krypterade medier. I ytterligare sju ärenden framgår det inte lika tydligt att kommunikationen är krypterad, men i dagsläget är det sannolikt att det är så. Två av ärendena pågår för närvarande, men bevisläget ser mycket svårt ut eftersom all brottplanering görs upp via krypterade medier.

Alternativa lösningar på problemen

För att få tillgång till information i beslag av mobiltelefoner, datorer etc. som är låsta, dvs. krypterade, krävs tillgång till *lösenord* (nycklar). Vid tillslag i samband med husrannsakan är det därför viktigt att det finns IT-forensiker på plats som kan säkra volatil data (ung. föränderlig överföring), och eventuella lösenord på plats när datorn är igång. Sådana tillslag kräver någon form av överraskningsmoment för att minimera risken att den misstänkte hinner stänga av datorn. I annat fall blir det svårt att få ett framgångsrikt resultat i dessa ärenden om inte den misstänkte väljer att samverka och uppger lösenord.

I samband med förhör har *utredaren* en nyckelroll när denne träffar den misstänkte och då har möjlighet att bygga upp ett förtroende dem emellan, som på sikt kan medföra att misstänkte lämnar uppgift om lösenord. Mer erfarna kriminella vet dock att man inte uppger sin kod för förhörsledaren.

Det finns metoder för att ”*tvinga upp*” låsta datorer (s.k. bruteforce). Metoderna är dock ganska tidsödande och används därför oftast inte i en pågående brottsutredning. En annan möjlighet är att ha en dator som är avsedd för dekryptering. Datorn kan endast knäcka lättare lösenord men metoden är precis som nämnda bruteforce, tidskrävande att använda.

Utan tillgång till informationen i beslagtagna enheter och då även samtal sker via krypterade kommunikationsmedel, är man hänvisad till den information man kan få fram genom telefonlistor från HÖK eller via HRA. När det gäller det senare har kriminella personer snabbt anpassat sig till tvångsmedlets möjligheter enligt gällande bestämmelser, och framför allt till dess begränsningar. Det händer ofta att möten och känsliga samtal undviks för att inte riskera eventuell s.k. buggning i förutsägbara rum eller bilar. Istället genomförs mötena flexibelt och oannonserat på allmänna och öppna platser. För att bli ett mer effektivt tvångsmedel bör beslut om HRA vara riktat mot misstänkt person och utan krav på plats. Åtgärder som kräver en ändring av nuvarande bestämmelser på området.

Det förekommer att de misstänkta trots allt inte använder sig av kryptering eller att krypteringen inte fungerar. Misstänkta personer kan också bli stressade och göra *misstag*, något som dock blir mer och mer ovanligt.

En arbetsmetod som kan tillämpas för att undvika att driva tidsödande utredningar som inte leder till framgång med anledning av användningen av krypterad information, är att göra *bortval*. De mest rutinerade kriminella känner till hur myndigheterna arbetar och kommunicerar därför alltid via krypterade kanaler. Under 2016 har Tullverkets brottsutredning av den anledningen och i avsaknad av tillgång till hemlig dataavläsning, medvetet valt att inte starta upp ett par ärenden.

En annan arbetsmetod är att arbeta med ”*underhuggarna*” i de kriminella nätverken. I bästa fall kan man på så sätt beslagta narkotika och gripa kuriren samt den person som skickas för att möta kuriren. Men man kommer fortfarande inte åt huvudmannen och övriga organisatörer i nätverket.

Ytterligare en arbetsmetod för att komma åt problemet med krypterad kommunikation är att använda *informatörs- och undercoververksamhet*, det senare används inte av Tullverket. Dessa arbetsmetoder är dock otillräckliga och inte heller alltid lämpliga att använda. Det löser inte heller problematiken att med få tillgång till krypterad information i beslagtagen datamedia som exempelvis datorer och mobiltelefoner.

Typfall

Exempel på ärenden under perioden 2015–2016

– I ett ärende med misstänkt narkotikasmuggling kommunicerades via Viber samt i specialkrypterade Blackberrytelefoner, vilket medförde att tillgången till information i utredningen var mycket begränsad. Traditionella telefoner användes också, men då utan att väsentlig information röjdes. De misstänkta huvudmännen i ärendet hade många möten utan förvarning. Dessa möten framkom inte av de samtal eller sms som avlyssnades. Det var därför mycket svårt att kunna göra prioriteringar i ärendet. Vissa personer dök alltid upp utan förvarning, förmodligen efter kommunikation på Viber. Det fanns vetskap om att stora narkotikaaffärer gjordes upp och man arbetade under lång tid med ärendet. Trots detta gick det inte att få fram någon vital eller avgörande information om dessa affärer, och man tvingades att avsluta ärendet utan resultat.

– I ett ärende som drevs i form av ett projekt gällande misstanke om storskalig smuggling och hantering av dopningsmedel hade den misstänkte huvudmannen en dator som var krypterad med Truecrypt (2015). I ett försök att knäcka lösenordet togs hjälp av andra myndigheter men det misslyckades och den misstänkte huvudmannen åtalades inte för sin inblandning. Däremot åtalades de övriga i grupperingen då deras datorer lyckades bli säkrade påslagna, vilket medförde att man kom förbi krypteringen.

– Ett gripande av en person som misstänks ha varit Sveriges största säljare av nätdroger under 2015. Vid gripandet hade denne, förutom flera krypterade datorer, även tillgång till krypterad webbpost (Countermail) som han använde i sin verksamhet. Lösenordet till ett av den misstänktes krypterade e-postkonton säkrades. Detta utgjorde sedan grunden till att denne dömdes för närmare 3 000 försäljningar. Däremot lyckades man inte knäcka lösenordet till den misstänktes huvudsakliga e-postkonton, som högst sannolikt innehöll bevis för ännu fler försäljningar.

– Kokainsmuggling från Latinamerika och Spanien (2015). Ärendet resulterade i beslag av narkotika samt gripande av olika kurirer. Däremot gick huvudmannen fri. Denne övergick till att kom-

municera via ”WhatsApp”, och då det inte gick att binda honom till de olika narkotikapartierna på annat sätt, så kunde han inte lagföras för misstänkt narkotikasmuggling.

– Uppstart i mars 2016 av ett ärende som handlade om misstänkt smuggling av kokain till Sverige från Europa. Ärendet fick läggas ner i juni utan resultat. Genom hemlig avlyssning av elektronisk kommunikation framkom att de misstänkta personerna i ärendet kommunicerade via Viber och Skype.
– Uppstart i juni 2016 av ett ärende om misstänkt smuggling av amfetamin från Holland till Sverige, samt smuggling av vapen. Avslutades i oktober utan att ärendet kommit framåt. Anledningen till detta var att de misstänkta personerna i ärendet kommunicerade via krypterade kanaler.
– I ett pågående ärende som handlar om misstänkt smuggling av stora mängder narkotika och vapen kommuniceras det huvudsakligen på WhatsApp, Snapchat och Instagram. Valet av stängda kommunikationsvägar gör att det i nuläget ser svårt ut att nå framgång i ärendet.

Varför hemlig dataavläsning?

Hemlig dataavläsning är det verktyg som Tullverket behöver för att få tillgång till den kommunikation som vi för bara ca sex år sedan kunde ta del av, något som den tekniska utvecklingen nu i alltför hög grad förhindrar.

Kriminella kretsar använder i allt större omfattning information som är krypterad i sin kommunikation. Om utvecklingen fortsätter som hittills kommer det att bli allt svårare för Tullverket att driva ärenden mot grupperingar och nätverk inom den grova organiserade brottsligheten.

Bristande bevisföring försvårar för Tullverket att knyta misstänkta huvudmän och andra nyckelpersoner till den misstänkta smugglingen. Det blir också svårare att påträffa varor som vi misstänker kommer att smugglas in i landet eller som misstänks redan tidigare ha smugglats in i landet. Det kan även försvåra för oss att kunna styrka att tillgångar som t.ex. påträffas vid en husrannsakan

kommer från brottslig verksamhet, vilket i sin tur leder till minskade möjligheter att kunna förverka brottsvinster.

Att bristen på bevisning även leder till att vi tvingas välja bort eller i förtid avsluta sådana ärenden är naturligtvis inte bra ur ett samhällsperspektiv. Organisatörerna för den grova narkotikasmugglingen blir då aldrig lagförda och kan på så sätt fortsätta med sin drogverksamhet, utan att bli nämnvärt påverkade av de åtgärder som myndigheten försöker vidta för att stoppa inflödet av narkotika till landet.

Med tillgång till hemlig dataavläsning kan Tullverket arbeta mer effektivt med att bekämpa den grova organiserade brottsligheten. För att kunna slå ut och lagföra aktörerna i kriminella nätverk måste vi få tillgång till den information som vi missar idag när brottsmisstänkta personer kommuniceras både inom och utom nätverken. Det är mycket svårt att nå framgång i dessa ärenden eftersom merparten av kommunikationen sker via krypterade kanaler. Även de beslag som görs av t.ex. mobiltelefoner och datorer är numera i allt större omfattning krypterade med olika standardprogram. Att kunna ta del av innehållet i dessa beslag är i stort sett omöjligt utan tillgång till lösenord (nycklar).

Konsekvensen av bristen på tillgång till information, blir att narkotikan i bästa fall kan beslagtas på gränsen, men några andra misstänkta personer än möjligen kuriren kommer inte att kunna gripas och lagföras i ärendet. Under vissa omständigheter kan det även vara svårt att bevisa att kuriren haft kännedom om narkotikan, vilket medför att inte heller kuriren kan lagföras för brottet.

Användningen av hemlig dataavläsning innebär en högre teknisk säkerhet vid inhämtningen, vilket förbättrar bevisläget, i synnerhet gällande huvudmän och andra nyckelpersoner i kriminella nätverk. Tvångsmedlet gör det även möjligt att förkorta utredningstider, vilket minskar utredningskostnaderna. Att inhämta uppgifter med hjälp av hemlig dataavläsning bör därmed bli mer rättssäkert och kostnadseffektivt, jämfört med inhämtning med hjälp av nuvarande hemliga tvångsmedel.

Ytterligare problembeskrivning i vissa avseenden

Identifiering av misstänkt

En avgörande framgångsfaktor i operativa projekt är att kunna identifiera misstänkta. Med anledning av den frekventa användningen av anonyma kontantkort finns det idag ett stort behov av att kunna använda HDA för att identifiera en misstänkt person genom att kunna aktivera mobiltelefonens kamera, mikrofon eller gps. Svårigheten att kunna identifiera personer i samband med misstanke om brott, innebär i vissa fall att Tullverket tvingas avstå från att begära inkoppling av ett hemligt tvångsmedel.

Exempel: En narkotikakurir har gripits vid gränsen. I dennes mobiltelefon hittas telefonnummer till en person som misstänks vara mottagare av narkotikan. Möjligheten att kunna installera ett tekniskt hjälpmedel med stöd av HDA i mottagarens telefon som ger tillgång till kamera och gps är ett effektivt sätt att kunna identifiera hur mottagaren ser ut med hjälp av en bild , samtidigt som man får reda på var denne befinner sig geografiskt.

Lokalisering av misstänkt

Det finns ett stort behov av att kunna positionera misstänkta personer i operativa spaningsinsatser. Möjligheten att kunna ta del av historiska och lagrade WiFi i telefonen som leder till lokalisering av misstänkta kan bli avgörande, t.ex. för beslut om husrannsakan och vid senare lagföring.

Användningen av HDA kompenserar här bristerna i operatörernas datalagring. Med anledning av EU-domstolens dom om datalagring innehåller uppgifterna från operatörerna inte någon detaljerad information om var den person som är misstänkt för brott finns eller har funnits under en viss intressant tidpunkt. För att kunna binda den misstänkte till brottsplatsen och brottstillfället är det viktigt att få fram mer detaljerade uppgifter om den misstänktes positionering, än t.ex. en mast som visar 360 grader.

Exempel: I ett pågående tullkriminalprojekt finns en misstänkt som är mycket försiktig med att överhuvudtaget använda sin telefon. Den misstänkte bor i ett s.k. ”särskilt utsatt område” i en storstad och är mycket misstänksam av sig och därför svår att spana fysiskt på. För att kunna fånga upp den misstänkte behövs positionsangivelser. Verktygen för nuvarande teknik är alldeles för grova, vilket innebär att det nästan är omöjligt att hitta den misstänkte. Med stöd av HDA ges möjlighet att kunna installera ett tekniskt hjälpmedel i den misstänktes mobiltelefon för att få tillgång till gps-funktionen, vilket i sin tur gör det möjligt att kunna spåra och hitta den misstänkte.

Ytterligare förutsättningar för

- hemlig rumsavlyssning (HRA)

Tullverket använder ytterst sällan HRA i sina ärenden. Anledningen är inte att det saknas behov av att kunna använda tvångsmedlet, utan på att det är mycket svårt att få utrustningen på plats. En smartphone innehåller bl.a. en mikrofon. I de fall som den misstänkte använder en smartphone finns därmed möjlighet att kunna använda HRA i mobiltelefonen med stöd av HDA. Ur ett integritetsperspektiv bör detta vara ett bättre alternativ för den enskilde, då risken för att utomstående (som inte är misstänkta för brott) spelas in och avlyssnas minskar väsentligt om informationen inhämtas via en mobiltelefon med stöd av HDA. Detta bör i sin tur även minska mängden överskottsinformation.

Exempel (fordon): För att kunna montera in utrustningen för HRA i ett fordon krävs en lång förberedelsetid. Det faktum att misstänkta personer också ofta byter bil, medför att det sällan är någon idé att begära tillstånd till HRA i ett specifikt fordon under pågående spaning. Att med stöd av HDA kunna installera ett tekniskt hjälpmedel i den misstänktes mobiltelefon för att avlyssna vad som sägs via telefonen, ger större möjligheter att få tillgång till den efterfrågade informationen, och utan krav på att installationen måste göras i ett särskilt fordon i samband med en pågående spaningsaktivitet.

Exempel (bostad): Montering av utrustning i en bostad kräver flera veckors förspaning innan det är möjligt att verkställa ett beslut om HRA. När utrustningen sedan är på plats är det ett omfattande arbete att ta hand om all överskottsinformation, då alla ljud i lägenheten spelas in och därefter måste gås igenom noggrant. Att med stöd av HDA kunna installera ett tekniskt hjälpmedel i den misstänktes mobiltelefon för att avlyssna vad som sägs via telefonen, ger större möjligheter att få tillgång till den efterfrågade informationen i det enskilda samtalet mellan misstänkta personer, samtidigt som mängden överskotts-information begränsas.

Exempel (offentlig plats): I ett projekt erhölls tillstånd till HRA på offentlig plats, som var en avgränsad plats där misstänkta personer brukade träffas. Dessa möten bestämdes ofta endast en kort tid innan de ägde rum. Något som medförde logistikproblem, då en annan myndighet som bistod Tullverket med installation av den tekniska utrustningen, måste kunna ställa upp på kort varsel. Att med stöd av HDA kunna installera ett tekniskt hjälpmedel i den misstänktes mobiltelefon för att avlyssna vad som sägs via telefonen, ger större möjligheter att få tillgång till den efterfrågade informationen i det enskilda samtalet mellan misstänkta, samtidigt som mängden överskottsinformation begränsas.

– hemlig kameraövervakning (HKÖ)

HKÖ används framförallt vid platser som är svårspanade och där den misstänkte har möten som bedöms vara viktiga i brottsplaneringen. Ett flertalet gånger har HKÖ dock inte kunnat verkställas, då det har varit svårt att hitta ett bra ställe att montera kameran på.

Att med stöd av HDA kunna installera ett tekniskt hjälpmedel i den misstänktes mobiltelefon för att få tillgång till kameran i telefonen, ger möjlighet att kunna se och även identifiera vem den misstänkte har möte med, utan att vara bunden till en specifik plats eller bra monteringsmöjligheter för en fjärrstyrd kamera.

Realtidsövervakning av teknisk utrustning

I tullkriminalens projektverksamhet har Tullverket erfarit ett arbetssätt som används av kriminella; de lägger meddelanden i s.k. utkast, dvs. skriftiga meddelanden som skrivs i realtid men som inte skickas.

I samband med provokativa åtgärder och tillslag är behovet stort av att i realtid kunna avläsa dokument som delas löpande mellan misstänkta, i egna chattrum eller motsvarande ”sfärer” för realtidskommunikation.

Att med stöd av HDA kunna installera ett tekniskt hjälpmedel i den misstänktes kommunikationsutrustning, skulle ge möjlighet att få tillgång till sådan realtidskommunikation.

Problembeskrivning; undersökningar av beslag

Sammanställning

Utifrån ett antal frågor som har ställts till Tullverkets forensiker via en kontaktperson, har följande sammanställning gjorts av de svar som inkommit. Tullverkets forensiker är placerade inom tullkriminalverksamheten och finns på fyra orter i landet; Stockholm, Göteborg, Malmö och Umeå. Bifogad sammanställning utgår från svaren från två av dem, varav en storstad i söder (Malmö) och en mindre stad i norr (Umeå) som får representera Norrland. Övriga två storstäder (Stockholm och Göteborg) har dessvärre inte svarat.

Frågor & svar

1. Hur vanligt förekommande är det med raderingsprogram?
Av svaret från storstad framgår att raderingsprogram verkar vara vanligast förekommande i datorer. Särskilt i utredningsärenden gällande köp eller försäljning av illegala produkter (anm. införselreglerade varor) på internet. I övriga ärendetyper är det inte så ofta förekommande. Det vanligaste programmet man har kommit i kontakt med är CCleaner.

Enligt uppgift från Norrland har uppskattningsvis runt 60 procent av alla beslag någon typ av raderingsprogram, och om ett raderingsprogram har körts så är den informationen borta och går inte att återskapa. Det blir allt vanligare att det på olika sidor på internet

finns rekommendationer att använda raderingsprogram och kryptering.

2. Förekommer det att man i samband med en undersökning upptäcker att alla uppgifter på informationsbäraren (mobil, dator etc.) är borta?
Enligt uppgift från storstad går det inte att få fram någon information då en *mobiltelefon* har återställts. Detta gäller både innan telefonen tas i beslag eller fjärråterställd, om inte flygplansläge har aktiverats. På *datorer* däremot finns alltid något spår kvar. Mängden information är dock beroende på borttagningsmetod, samt hur mycket datorn har använts vid eventuell borttagning, formatering eller ominstallation. Erfarenheten för Norrland är att detta har hänt vid ett flertal tillfällen, och då främst på mobiltelefoner som inte har nätverksisolerats.

Följdfråga till fråga 2: I hur stor utsträckning av antalet undersökta beslag (uttryckt i procent), har bortfall av uppgifter upptäckts under de tre senaste åren?
Enligt storstad är det svårt att uppskatta antalet misstänkta återställningar, men gör en grov uppskattning för *mobiler* på ca tio stycken de tre senaste åren. Kan dock inte göra en uppskattning för datorer. Norrland gör en uppskattning på ett bortfall av uppgifter i 5–6 procent av antalet undersökta beslag.

3. Har användningen av raderingsprogram ökat, minskat eller ligger på samma nivå?
Uppfattningen hos både storstad och Norrland är att användarnas kunskaper kring anti-forensiska metoder[1] har ökat. Enligt storstad är ökningen dock inte extrem, vilket kan bero på olika brottstyper. Tullverket har inte ärenden där man utreder brott som exempelvis dataintrång, där de misstänkta besitter sådan kompetens. I brottsutredningar rörande narkotikasmuggling och olika typer av narkotikabrott förekommer dock anti-forensiska verktyg och kryptering.

[1] Begreppet anti-forensiska metoder är ett generellt begrepp som används för att beskriva olika programvaror och metoder som försvårar för brottsbekämpande myndigheter att få tillgång till uppgifter (t.ex. kryptering och radering). Begreppet förekommer i forum som t.ex. Flashback.

4. Hur ser ni på risken för att kriminella framöver kan komma att – i större utsträckning än idag – installera raderingsprogram som försvårar arbetet för forensiker?
Både storstad och Norrland bedömer risken som mycket stor, dels för att raderingsprogrammen blir mer lättillgängliga och enklare att använda, dels för att:

- verktygen blir lättare att hantera,
- information om anti-forensiska metoder sprids,
- myndigheters IT-forensiska metoder diskuteras på det nationellt kända internetforumet Flashback, och det finns en forumstråd där de ska samla förundersökningsprotokoll.

5. En uppgift som framkommit i HDA-utredningen är att dagens hårddiskar i sig är så bra på att radera/skriva över att det inte går att återskapa information vid undersökning av beslag. Vad är er erfarenhet av detta? Stämmer det?
Enligt både storstad och Norrland gäller detta främst de nya hårddiskarna (SSD) som har en funktion som innebär att data skrivs på olika platser på hårddisken. Därmed minimeras risken att gammal data skrivs över. Funktionen innebär också att data flyttas runt för att det ska bli jämnt ”slitage” på minnespositionerna. Dessa SSD-diskar blir allt vanligare eftersom de är mycket snabbare än traditionella skivdiskar.

Tullverkets behovsbeskrivning avseende hemlig dataavläsning i underrättelseverksamhet

Bakgrund

Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i den brottsbekämpande myndigheternas underrättelseverksamhet (den s.k. inhämtningslagen, IHL), trädde i kraft den 1 juli 2012. Med stöd av denna lag får Tullverkets underrättelseverksamhet inhämta uppgifter om elektronisk kommunikation från berörda operatörer. Inhämtningen som sker i hemlighet avser uppgifter om elektronisk kommunikation i form av samtalslistor samt lokaliseringsuppgifter (dvs. visst geografiskt område), avseende

elektroniska kommunikationsutrustningar (t.ex. mobiltelefon eller dator), i *dåtid* eller i *realtid*.

För att Tullverket ska kunna inhämta dessa uppgifter krävs inte misstanke om ett specifikt brott utan enbart misstanke om ”brottslig verksamhet”. Åtgärden ska dock vara av *särskild vikt*, i syfte att förebygga, förhindra eller upptäcka sådan brottslighet, dvs. underrättelseverksamhet. Kravet på särskild vikt är en behovsbedömning som innebär att det ska finnas andra uppgifter (t.ex. källinformation), som gör det möjligt att bedöma den förväntade betydelsen för syftet med inhämtningen. Därtill krävs att skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som utsätts för åtgärden, dvs. proportionalitetsprincipen ska tillämpas vid beslut om inhämtning.

För att Tullverket ska få inhämta uppgifter med stöd av inhämtningslagen krävs vidare att den misstänkta brottsliga verksamheten innefattar brott med *minst två års fängelse i straffskalan*. För Tullverkets del motsvarar det angivna straffvärdet brotten grov narkotikasmuggling eller synnerligen grov narkotikasmuggling[2].

Tullverkets uppdrag

Tullverkets uppdrag i dess brottsbekämpande verksamheten från riksdag och regering, är att förebygga, förhindra och utreda brott[3]. Den brottskatalog som Tullverket arbetar med är dock begränsad i jämförelse med motsvarande kataloger inom Polismyndigheten respektive Säkerhetspolisen. Gemensamt för dessa myndigheter är att de samverkar med varandra mot den organiserade brottsligheten och de grova brotten.

För att Tullverket ska kunna fullgöra sitt uppdrag för att förebygga och förhindra brott, dvs. underrättelseverksamhet, behöver myndigheten information och uppgifter. Behovet av information och uppgifter kan variera beroende på typ av brottslighet och vilka aktörer som är inblandade. För att samla information och uppgifter används olika arbetsmetoder som exempelvis fysisk respektive inre

[2] 6 § tredje och fjärde styckena lagen (2000:1225) om straff för smuggling (smugglingslagen).
[3] Förordning (2016:1332) om instruktion för Tullverket och Regleringsbrev för budgetåret 2017 avseende Tullverket.

spaning, tips från allmänheten och kontakter med anmälare och tipsare. Insamlad information och uppgifter bearbetas, analyseras och byggs på, i syfte att få fram ett tillräckligt underbyggt underlag för att kunna inleda förundersökning med misstanke om brott.

I detta arbete är det av yttersta vikt att Tullverket även får tillgång till uppgifter om elektronisk kommunikation i form av trafik- och lokaliseringsuppgifter, både i realtid och i dåtid (historiska uppgifter). Tullverkets tillgång till sådana uppgifter regleras av bestämmelserna i inhämtningslagen.

Rätten att få tillgång till dessa uppgifter som finns hos olika teleoperatörer, mängden uppgifter samt operatörernas lagringsskyldighet för brottsbekämpande ändamål har ifrågasatts av EU-domstolen i ett förhandsavgörande den 21 december 2016 i de förenade målen C-203/15 och C-698/15.

Tullverkets behov av hemlig dataavläsning i underrättelseverksamhet

Tullverkets möjligheter att kunna inhämta uppgifter med stöd av bestämmelserna i inhämtningslagen är begränsade, dels av de uppgifter som faktiskt får inhämtas med stöd av lagen (1 § 1 – 3 IHL), dels av kravet på ett straffvärde på minst två års fängelse för det brott som omfattas av den misstänkta brottsliga verksamheten (2 § 1 IHL). För Tullverkets del avser detta enbart brotten grov narkotikasmuggling och synnerligen grov narkotikasmuggling enligt smugglingslagen.

Precis som inom förundersökningsverksamheten så försvåras Tullverkets underrättelsearbete av att kriminella aktiviteter numera i allt högre grad sker i olika typer av sociala medier. Kriminella personer använder också många olika oregistrerade kontantkort i s.k. buslurar eller fullurar, som är mobiltelefoner av äldre modell, men som ändå i vissa fall klarar att hantera sociala medier, t.ex.”WhatsApp”.

Mer avancerade kriminella personer med en god ekonomi har dock råd med dyra mobiltelefoner och datorer. I kombination med ett högt säkerhetsmedvetande har dessa personer även lättare att undvika spårbarhet (p.g.a. kryptering, raderingsprogram etc.), vilket fått till följd att Tullverkets underrättelsearbete har försvårats eller till och med inte gått att genomföra. Färre antal framtagna underrättelseärenden leder i sin tur till minskat antal inledda förunder-

sökningar och färre antal misstänkta personer som kan lagföras för grova brott.

Att genomföra kartläggning av stora kriminella nätverk som misstänks syssla med storskalig smuggling och som fungerar som välorganiserade företag, kräver både resurser och lämpliga ”verktyg”. För Tullverkets del saknas idag sådana verktyg. Hemlig dataavläsning kan, som ett självständigt hemligt tvångsmedel, vara ett sådant verktyg.

Bestämmelserna i inhämtningslagen är direkt kopplade mot vissa bestämmelser i LEK som reglerar operatörernas lagringsskyldighet för brottsbekämpande ändamål, samt skyldighet att på begäran från brottsbekämpande myndigheter tillhandahålla dessa uppgifter. Dessa skyldigheter inbegriper s.k. telefonlistor, realtidsuppgifter och s.k. basstationstömning (eller masttömning).

Kommunikation som sker via sociala medier omfattas inte av bestämmelserna i LEK och FEK. Uppgifterna i sådan kommunikation är skyddade på olika sätt, t.ex. genom kryptering, krav på lösenord etc. För att få tillgång till uppgifterna finns ett stort behov för Tullverket som brottsbekämpande myndighet i underrättelseverksamhet att, precis som inom ramen för en förundersökning, kunna använda hemlig dataavläsning som ett självständigt hemligt tvångsmedel vid inhämtning av uppgifter enligt inhämtningslagen. Utifrån den lagens nuvarande utformning verkar detta dock inte vara möjligt, då det av förarbetena framgår att inhämtningslagen inte omfattar de brottsbekämpande myndigheternas möjlighet att med egna tekniska hjälpmedel hämta in uppgifter om elektronisk kommunikation (prop. 2011/12:55 s. 120).

Tullverkets rätt att tillämpa bestämmelserna enligt inhämtningslagen är sedan lagens tillkomst begränsad. Tullverket kan enbart inhämta uppgifter från operatörerna vid misstänkt brottslig verksamhet som avser brott med minst två års fängelse i straffskalan. Det högt satta straffvärdet omfattar bara två brott enligt smugglingslagen; grov narkotikasmuggling eller synnerlig grov narkotikasmuggling.

Tullverket har i sin brottsbekämpande verksamhet i uppdrag att förebygga, förhindra och utreda brott, med fokus främst på smuggling av narkotika. Ett uppdrag som väsentligen har försvårats under de senaste tio åren, på grund av den snabba tekniska utvecklingen. Detta har i sin tur påverkat både underrättelse- och utredningsverk-

samheten negativt, genom att det har blivit allt svårare att kunna kartlägga, utreda och lagföra grova brott, däribland grov narkotikasmuggling.

Datalagringsutredningens förslag att begränsa operatörernas lagringsskyldighet för olika trafik- och lokaliseringsuppgifter i kombination med att kriminella aktiviteter i allt större utsträckning sker via sociala medier, försvårar och till och med förhindrar insamling av uppgifter för kartläggning av misstänkt brottslig verksamhet avseende, i detta fallet, grov och synnerligen grov narkotikasmuggling. För att kunna uppfylla sitt uppdrag att bekämpa dessa smugglingsbrott behöver Tullverket bättre ”verktyg”.

Hemlig dataavläsning som tvångsmedel är ett sådant rättsligt verktyg som ger Tullverket möjlighet att kunna undersöka och kartlägga avancerade och tekniskt utvecklade kriminella nätverk. Något som vi idag inte kan göra, i avsaknad av rätt verktyg och ett lagligt stöd för att kunna använda verktyget.

Polisen

Polismyndighetens behovsbeskrivning avseende hemlig dataavläsning under förundersökning

Problem vid hemlig avlyssning av elektronisk kommunikation (HAK)

Polisen har under de senaste åren noterat att de individer som HAK tillämpas mot allt oftare går över till andra kommunikationssätt än telefoni. De sociala samtalen går fortfarande att fånga upp, men om samtalen ska handla om kriminell verksamhet övergår samtalen oftast till exempelvis krypterade kommunikationsappar som WhatsApp, Skype, FaceTime m.fl. Det föreligger ett stort behov av att få tillgång till hemlig dataavläsning (HDA) för att kunna säkra kommunikationen i dessa fall, och på så sätt samla bevis i förundersökningar rörande grova brott. Polisen uppskattar att de senaste tre åren har 90 procent av kommunikationen mellan två parter skett krypterat vid avlyssning rörande internet- eller datatrafik avseende mobila- och fasta bredband.

Alternativet idag är att installera hemlig rumsavlyssning (HRA) i bostäder och fordon för att försöka fånga kommunikationen. Problemet med detta är att man endast hör den ena parten och det blir svårt att få ett sammanhang i samtalen. Ofta är hörbarheten inte heller optimal. Installation av HRA är dessutom en mycket komplicerad metod som ofta kräver lång kartläggning av de misstänkta och deras rutiner, umgänge och familj.

Exempel från förundersökningar med HAK.
Utdrag ur telefonsamtal 2016-10-12:
G: Men vad gäller det?
O: Dom ska genomsöka bostaden
O: Vi får ta det här på telefon....
G: Vi kan inte ta det på telefon....då får du ringa på WhatsApp
O: Ok...

Utdrag ur telefonsamtal 2016-10-11:
G säger att han ringer upp R på den andra.

Detta är två exempel som belyser användningen av krypterad kommunikation där man vill säkerställa att man inte blir avlyssnad.

Vid avlyssning av mobiltelefoner med abonnemang med datatrafik eller av mobilt bredband kan mycket av internet- och datatrafiken inte insamlas då de avlyssnade enheterna kopplats upp mot allmänna trådlösa nätverk på till exempel på flygplatser, restauranger och affärer. Anledningen kan vara antingen att spara dataförbrukning på det mobila abonnemanget eller för att dölja sina förehavanden. Konsekvensen blir att det inte går någon internet-/datatrafik via det avlyssnade mobila abonnemanget, eftersom kommunikationen istället sker via det allmänna trådlösa nätverket. Det är även vanligt att man kopplar upp sig via sitt eget trådlösa nätverk när man befinner sig i sin bostad. Även då går internet-/datatrafiken över till ett nätverk som kan delas av flera familjemedlemmar och blandas in i övrig datatrafik som kan vara film och musik som strömmas till mobiler, surfplattor, spelkonsoller, datorer och tv-apparater vilket gör det svårt att urskilja den trafik som ska avlyssnas och dessutom är ett problem ur integritetssynpunkt.

Idag har i stort sett samtliga appar och program som används för kommunikation inbyggd kryptering. För tio år sedan var endast en bråkdel av internettrafiken krypterad. En tydlig trend är att kryptering byggs in i nya appar och att krypteringen är aktiv utan att användaren behöver vidta någon åtgärd.

Allt fler webbplatser använder SSL-kryptering (Secure Sockets Layer) vilket medför att kommunikationen mellan webbplatsen och den besökande enheten är krypterad. Eftersom det är datatrafik som går via abonnemang som avlyssnas vid HAK får man endast tillgång till krypterad data, som inte går att tolka utan att använda stora dataresurser för dekryptering, om det ens är möjligt att dekryptera inom rimlig tid. Börjar en webbadress med https:// istället för http:// är kommunikationen krypterad med SSL.

Som exempel kan nämnas att man tidigare kunde se vilka bokningar som gjordes på SJ:s hemsida, vilka tåg som eftersöktes. Efter att SJ uppdaterat sin hemsida med SSL går boknings- och sökinformation som användaren gör via krypterad kommunikation, som inte

går att avläsa vid HAK. SSL-kryptering är vanligt förekommande på webbplatser för bokning av flygresor och hyrbilar.

Vid analys av internettrafik, med beslut om HAK, har det visat sig att det är mycket vanligt att misstänkta använder sig av olika VPN-tjänster, ToR och liknande krypterings- och anonymiseringstjänster för att dölja sina förehavanden.

Illegal näthandel (t.ex. vapen, droger, barnpornografi och stulna kreditkort) sker idag nästan uteslutande på Darknet. Tillgång till Darknet sker via det krypterade och anonymiserade ToR-nätverket.

Problem vid analys av beslagtagna databärare

- Kryptering
- Raderings-/rensningsfunktioner

Kryptering av databärare har ökat markant de senaste åren vilket kräver mer resurser och sätter högre krav på planering inför tillslag såsom spaning och offensiv taktik vid själva tillslaget för att hinna fram till en dator innan den stängs av och blir krypterad varvid innehållet blir oläsligt vid en analys.

Ett annat problem som blivit vanligare är raderings- och rensningsprogram som används på datorer. Detta gör att endast den användarhistorik som skrivits efter senaste rensningen finns kvar i databäraren vid beslagstillfället. Om datorn rensats på natten och tillslaget sker på morgonen finns inte mycket användarhistorik kvar i databäraren. Med HDA skulle man kunna fånga upp användarhistoriken löpande innan den raderas. Användarhistoriken kan bestå av till exempel chattar, besökta webbsidor eller filer som har använts. Även inskrivna lösenord kan då återfinnas

Allt som skrivs av användaren vid datorn skickas inte iväg via internet. Till exempel lösenord till en lokalt krypterad fil går inte iväg som ett meddelande, vilket gör att HAK aldrig kommer fånga den informationen.

Det är mer regel än undantag att mobiltelefoner är skyddade av lösenkod eller biometriskt skydd. De ledande tillverkarna av mobiltelefoner har aktiverat kryptering vid leverans. I de fall lösenordet varit känt och mobiltelefonen gått att analysera har chatthistoriken och annan information ändå inte kunnat läsas eftersom appar i

mobiltelefoner använder sig av egen kryptering i stor utsträckning. Det innebär att innehållet i appar inte kan analyseras och information som kan vara av värde i förundersökningen inte kan tillvaratas.

Idag är många beslagtagna datorer och mobiltelefoner krypterade. Det gäller även externa hårddiskar, USB-minnen och enskilda filer i datorerna. I de fall där en beslagtagen enhet är krypterad går den inte att undersöka utan lösenord till dekrypteringsnyckeln. Att dekryptera information, även om man använt relativt enklare former av kryptering, är en tidsödande process. Detta medför att dekrypterad data i vissa fall förlorat sin aktualitet om man lyckas dekryptera materialet.

Vid många tillfällen har det visat sig att misstänkta använder sig av krypterade internetuppkopplingar, som ToR eller VPN. Även beslagen innehåller krypteringar. I de fall där beslaget inte gjorts i öppet och dekrypterat läge har innehållet inte gått att läsa och analysera och eventuellt bevismaterial kan inte tillföras förundersökningen.

Hur kan man gå vidare i ärendet där det finns kryptering? Man kan fråga användaren efter lösenord, vilket oftast inte är någon framgångsfaktor. Det finns attackmetoder för att knäcka lösenord. Ju längre och mer komplicerat lösenordet är desto längre tid tar det att knäcka lösenordet, om det överhuvudtaget är möjligt. När man försökt dekryptera på alla sätt utan att lyckats får man konstatera att dessa delar av beslaget inte blir analyserade och att eventuella bevis går förlorade i förundersökningen. Inte heller omständigheter som talar till den misstänktes fördel kan omhändertas.

Det förekommer ofta även att enstaka filer är låsta med hjälp av lösenord och kryptering, vilket medfört att innehållet inte kunnat analyseras. De filer som innehåller bevis som i görs oläsbara med kryptering och lösenord kan öppnas om man genom HDA kan få del av vilka lösenord som krävs för att dekryptera filen och därmed ta del av innehållet.

Vid ärenden med överbelastningsattacker, så kallade DDoS-attacker, har användaren ofta försökt dölja sina spår med hjälp av kryptering. HDA kan vid förberedelser och under pågående överbelastningsattacker säkra bevis för brottet.

De gärningsmän vars intresse är att samla på bilder och filmer som skildrar sexuella övergrepp på barn vill skydda sitt material. Det

sker vanligtvis genom att lägga bilderna och filmerna på krypterade externa hårddiskar. Lösenorden är oftast komplicerade och gärningsmännen lämnar inte ut sina lösenord.

Gärningsmännen ligger ofta i framkant när det gäller de nya möjligheterna som teknikutvecklingen ger. Man är oftast högt medveten om vilka tekniska och legala begräsningar rättsvårdande myndigheter har. Även om man inte ligger i framkant begränsas våra möjligheter genom att innehållsleverantörerna för internettjänster på senare år implementerat integritetsskydd i sina applikationer som är automatiskt påslagna från början. Vi har tagit del av de kompletterande behovsbeskrivningarna från övriga experter i denna utredning och konstaterar att gärningsmännen använder samma modus för att försvåra utredningsarbetet. Det enda som skiljer är brottsrubriceringarna på de olika myndigheterna. Av den anledningen nöjer vi oss med att komplettera endast några typfall som vi hoppas tillför några ytterligare behovsbilder, istället för att upprepa sådant som redan beskrivits.

Typfall

SSD och TRIM

Ytterligare en försvårande omständighet för brottutredande myndigheter är SSD-diskar (solid-state drive) och flashminnen. Tillsammans med en teknik som kallas TRIM kan filsystemet snabbt återanvända utrymme på hårddisken när filer som funnits där har raderats. TRIM rensar automatiskt den tidigare ytan i bakgrunden utan att användare behöver använda ett rensningsverktyg.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel som kan ge brottsbekämpande myndigheter informationen innan den raderas.

Förberedelse mord

Polismyndigheten har information om att en känd kriminell gruppering planerar en hämndaktion mot en konkurrerande gruppering. Informationen gör gällande att man ska skjuta en framstående med-

lem i den andra grupperingen. I samband med telefonavlyssning i ärendet framgår det att man skriver instruktioner om det planerade brottet i datorn med programmet Anteckningar. Instruktionerna sparas inte på datorn, utan skrivs ut direkt på en skrivare. Detta för att undvika eventuella spår efter lagrade filer.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i de misstänktas utrustning som kan ge information om det som skrivit i Anteckningar innan det skrivits ut och applikationen stängts ner utan att dokumentet sparats.

Grovt sexuellt tvång och grovt utnyttjande av barn för sexuell posering

En av polisen känd person som avtjänat sitt straff är åter igen misstänkt för grovt sexuellt tvång och grovt utnyttjande av barn för sexuell posering mot ett stort antal minderåriga flickor. Personen som dömts ett flertal gånger för liknande brottslighet har efter varje dom blivit bättre på att skydda sig med hjälp av ToR och kryptering. Liksom i många andra groomingärenden använder sig personen även av raderingsprogram efter varje kontakt med sina offer. Genom att återanvända sparade filmer och bilder från tidigare offer kan personen fortsätta med hot och nya groominginspelningar. Dessa sparade filmer och bilder kunde vid tidigare utredningar inte bevissäkras på grund av krypterade lagringsmedia och installerade raderingsprogram. Datorn och lagringsmedia kunde därför inte förverkas och filerna återanvänds i fortsatt brottslighet.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel som kan ge information om var tidigare sparat material finns lagrat samt binda personen till aktuellt brott. Den information som kontinuerligt raderas skulle kunna fångas upp med hjälp av HDA.

Grovt dataintrång och grovt bedrägeri

En kriminell gruppering har under lång tid utarbetat ett sätt att få in skadlig kod i företags affärssystem. Den skadliga koden har gett huvudmannen administratörsrättigheter i systemen i många fall och

genom detta har han kunnat ändra konton för betalningar, genomföra beställningar i företagets namn, få komplett insyn i anställdas epostkonton och därigenom tillgång till lösenord. Efter gripandet av huvudmannen nekar denne till att använt den beslagtagna datorn.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel som kan ge information om vem som brukat datorn vid ett visst tillfälle och om det är huvudmannen som skapat den skadliga koden. Det skulle ge möjlighet till tidigare lagföring och ingripande. Bidra till bra bevisning som skulle göra att man inte behöver invänta huvudbrottet för att få ihop tillräcklig bevisning för lagföring.

Grovt barnpornografibrott

De personer som ägnar sig åt att samla på bilder av barnpornografisk karaktär vill skydda sin samling. Det sker genom att lägga bilderna och filmerna på hårddiskar och på avgränsade ytor som sedan krypteras. Lösenorden är oftast komplicerade och personerna lämnar inte ut dessa. Vissa krypteringsprogram lagrar inte lösenord över huvud taget, utan dessa måste samlas in när de skrivs in av användaren i realtid. I samtliga ärenden på senare tid hos Nationellt it-brottscentrum har det förekommit installerade raderingsprogram på datorn. Ett raderingsprogram suddar ut alla spår av hanteringen av bild- och filmfiler. Det raderar både sökvägar och namn på filer på de lokala lagringsenheterna. Även filernas väg in till datorn raderas. Det går följaktligen inte att se hur eller varifrån filerna har laddats ner till datorn. Det har även förekommit fall där den misstänkte har installerat om hela datorn en gång per månad för att radera alla spår.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel som kan ge information om inloggningsuppgifter, vilket gör att utredningstiderna kan minskas. Det skulle även kunna ge information om vilka andra som sprider barnpornografiska bilder och filmer. Den information som kontinuerligt raderas skulle kunna fångas upp med hjälp av HDA.

Grovt narkotikabrott

Polismyndigheten bedriver en förundersökning rörande grovt narkotikabrott. Huvudmannen misstänks för att driva en marknadsplats på Darknet där säljare och köpare av narkotiska preparat kan mötas. Domstolstillstånd för HAK har getts, men analysen av IP-trafik visar att all kommunikation sker via ToR. Enligt underrättelseinformation administrerar huvudmannen marknadsplatsen helt och hållet från ett krypterat USB-minne med operativsystemet Linux installerat. Vid husrannsakan hos huvudmannen anträffas ett krypterat USB-minne och en dator som saknar hårddisk. Det är sannolikt att datorn har startats från det krypterade USB-minnet och att anslutningen via ToR och marknadsplatsen skett med hjälp av denna. Tyvärr går det inte att styrka brott då det inte går att säkra informationen på det krypterade USB-minnet

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel som kan ge information om innehållet i det krypterade USB-minnet och styrka brottet.

Grova åldringsbrott

Flera fall av grova åldringsbrott har skett i norra delarna av landet. Modus tyder på att det är samma gärningsmän som ligger bakom brotten. Polisen tar kontakt med ett företag som tillhandahåller en söktjänst på internet och hör efter om sökningar gjorts på offrens adresser. Företaget kan bekräfta att så skett på ett par av offrens adresser strax för brottstillfällena. Företaget kan leverera IP-adressen som sökning skett från. Dessvärre visar kontroll att IP-adressen tillhör ett kontant mobilt bredband med okänd abonnent. Teleoperatören levererar inte mastpositioner till rättsvårdande myndigheter, varför det inte går att lokalisera utrustningen som sökningarna skett från eller misstänkt gärningsman.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel som kan ge information utrustningens geografiska position samt misstänkt gärningsman.

Polismyndighetens behovsbeskrivning avseende hemlig dataavläsning i underrättelseverksamhet

Indelande sammanfattning

Polismyndigheten har ombetts av *Utredningen om hemlig dataavläsning* att inkomma med ett yttrande gällande Polismyndighetens behov av hemlig dataavläsning i underrättelsesyfte genom lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (IHL) och anför härmed följande;

- Elektronisk kommunikation är avgörande i Polisens arbete mot den organiserade brottsligheten.
- Polisen har idag inte tillräckliga verktyg för att inhämta elektronisk kommunikation.
- Elektronisk kommunikation är ofta krypterad och är därmed otillgänglig hos telefonoperatörerna.
- Kommunikationen i samhället sker i större utsträckning via datanätet och krypterade chattappar.
- Kriminella söker ständigt sätt att undkomma rättsliga åtgärder och teknikutvecklingen underlättar deras verksamhet.
- It-teknikutvecklingen skapar nya brottsmöjligheter, brottsforum och arenor för brott.
- På internet och på krypterade nätverk finns idag en stor marknad för kriminella varor och tjänster.
- Polisen behöver samma verktyg att verka på internet som i reella världen.
- Lagstiftaren har sedan tidigare bedömt att Polisen ska få inhämta elektronisk kommunikation i underrättelse syfte och lagstadgat det i IHL.
- Hemlig dataavläsning i enlighet med IHL skulle inte förändra vilken typ av uppgifter Polisen har rätt att inhämta utan ge ett verktyg att verkställa den redan lagstadgade inhämtningen.

- Intrånget i den personliga integriteten som hemlig dataavläsning genom IHL skulle innebära står i proportion till den påverkan de brott lagen omfattar har på samhället i stort.

Polisens underrättelseverksamhet

Enligt Polislagen 2§ (1984:387) har Polisen till uppgift att förebygga, förhindra och upptäcka brottslig verksamhet vilket i huvudsak bedrivs vid Polisens underrättelsetjänst som finns verksam på samtliga nivåer i organisationen.

Underrättelseverksamhet är i huvudsak inriktad på att avslöja om en viss, inte närmare specificerad brottslighet, har ägt rum, pågår eller kan antas komma att begås. Till skillnad från Polisens utredande verksamhet fokuserar underrättelseverksamheten inte på enskilda brott, utan på brottslig verksamhet. Utredande verksamhet i form av en förundersökning eller primärutredning är att betrakta som bakåtblickande, då utredningen avser ett specifikt brott som har begåtts. Underrättelseverksamheten är typiskt sett framåtblickande, då den syftar till att upptäcka, förutse och beskriva en viss brottslighet, brottsutveckling eller ett visst fenomen i syfte att förebygga och förhindra.

Det finns vissa brottsområden och kriminella miljöer där underrättelseverksamheten är mer central för det polisiära arbetet. Det handlar främst om brott som vanligtvis inte anmäls till Polisen och som kräver aktiva åtgärder att uppdaga som exempelvis narkotika- eller vapensmuggling. Underrättelseverksamheten är särskilt viktigt i bekämpning av organiserad brottslighet. Dels för att brott sker systematiskt, och genom komplexa brottsupplägg, som kräver kvalificerad kartläggning och analys för att hantera. Dels för att benägenheten att samverka med Polisen är låg vilket ställer högre krav på annan information till grund för brottsbekämpningen, så som elektronisk kommunikation. Dels för att de kriminella vidtar avancerade motåtgärder för att undgå polisiär upptäckt.

Mot bakgrund av de senaste årens utveckling inom marknaden med gratis appar med högre prestanda och utbyggnad av 4G-näten är det troligt att de kriminella i ännu större utsträckning kommer föredra att använda datakommunikation framför traditionell telekommunikation.

Polisen har därav ett behov av hemlig dataavläsning för att möjliggöra inhämtning av information som lagstiftaren avsett att Polisen ska ha rätt att inhämta men som Polisen idag inte kan ta del av då informationen ofta är krypterad och därmed på grund av tekniska skäl inte är tillgänglighos telefonbolagen för den inhämtning som medges i IHL.

Organiserad brottslighet kräver ett aktivt arbeta för att uppdagas

Polisens underrättelsetjänst hanterar främst organiserad brottslighet, vilken till stor del står för den brottslighet som avses i IHL (brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år). Flera av brotten är av sådan art att Polisen måste arbeta aktivt för att upptäcka den. Det kan vara svårt då den många gånger sker i internationell brottssamverkan eller via krypterade forum på internet. Polisen har även liksom Säkerhetspolisen i uppgift att arbeta mot kontraterrorism, ensamagerande och inhemsk extremism där underrättelseverksamheten som kräver en effektiv underrättelseinhämtning.

Motorn i organiserad brottslighet är individer som har förmågan att utveckla sin brottsförmåga och förvalta vinning av brott. Det är även grundläggande för organiserad brottslighet att aktörerna har ett trovärdigt våldskapital som skyddar mot att bli förrådd eller påläggas fiktiva skulder. En våldseskalering har på senare år skett i den kriminella miljön, särskilt kopplat till utsatta områden och skjutvapen eller handgranater används i allt större utsträckning. Vid flera fall har skjutningar och sprängningar skett vårdslöst på allmän plats och inneburit fara eller skadat tredjeman.

Polisen upplever allt större svårigheter att stävja de våldsamma konflikterna i kriminella miljöer. Våldet manar till tystnad vilket ökar behovet av andra typer av information såsom exempelvis elektronisk kommunikation för att verifiera underrättelseinformation. Konfliktaktörerna är därtill väl medvetna om Polisens metoder och skyddar sin kommunikation genom krypretade kommunikationssätt. Många gånger har Polisen en god underrättelsebild gällande konflikterna men saknar verktyg att verifiera underrättelseinformation som kan vara avgörande för Polisen i arbetet att förhindra

nya mord och mordförsök. Behovet av nya insamlingsverktyg, så som hemlig dataavläsning, anses därför i detta avseende vara akut.

Ökningen av det grova våldet inom kriminella kretsar har bidragit till en ökad efterfrågan på vapen. Illegala vapen och handgranatar smugglas till Sverige från exempelvis Balkan. Aktörer i vapenhandeln får ofta kontakt med varandra via internetforum. Vapen kan även beställas på öppna internet eller på det krypterade Darknet och skickas per post.

En stor del av den organiserade brottsligheten kretsar kring handel med narkotika. De senaste åren ses allt mer en öppen narkotikahandel i utsatta områden och narkotika är även viktig inkomstkälla för MC-miljön. Försäljning av narkotika sker även i stor utsträckning på öppna internet och på Darknet. Sverige är främst ett konsumtionsland av narkotika vilket gör att de internationella kopplingarna i narkotikahandeln är högst påtagliga. Flera kriminella nätverk samverkar vanligtvis i distributionskedjan från ursprungslandet till de nationella distributörerna vilket kräver samarbete både inom och utanför Sverige. För att identifiera distributionskedjan och var narkotikan tar vägen krävs omfattande kartläggning som i de allra flesta fallen bygger på elektronisk kommunikation. På samma sätt kartläggs internationella nätverk som ägnar sig åt människohandel för sexuella ändamål, tiggeri eller exploatering i arbete.

På internet och på krypterade nätverk finns en stor marknad för kriminella varor och tjänster. Säkerhetsluckor utnyttjas av kriminella för att genomföra bedrägerier och dataintrång. Komplex cyberbrottslighet riktad mot Sverige sker både innanför och utanför landets gränser. Det utövas i ekonomiskt syfte, vid exempelvis utpressning genom dataintrång, men även som ett led i aktivism eller it-sabotage.

Ett annat brottsområde som utgör en omfattande brottslighet på internet är it-relaterade sexuella övergrepp mot barn. Den tekniska utvecklingen av anonymiseringstjänster och delningsmöjligheter gör det lättare för gärningsmän att få tillgång till, dela bilder och filmer som innehåller sexuella övergrepp. En ökande trend ses gällande att material med sexuella övergrepp mot barn produceras av kriminella aktörer för ekonomisk vinning.

Vidare är penningtvätt utbrett inom organiserad brottslighet och sker gränsöverskridande. Nya betalningsmedel och virtuell valuta är ett sätt att betala utan att använda kontanter, traditionella kreditkort

eller överföringar mellan bankkonton. Ett växande antal onlineplattformar och applikationer erbjuder nya sätt att transferera pengar och genomföra betalningar. Dessa är inte alltid reglerade i samma utsträckning som traditionella tjänsteutförare vilket underlättar penningtvätt.

Nyttjande av kryptering för att undkomma rättsliga åtgärder

De kriminella aktörerna är överlag medvetna om att teknisk bevisning är avgörande för en fällande dom och att inhämtning av uppgifter om elektronisk kommunikation även används av Polisen i underrättelsefasen. Kriminella som aktivt försöker skydda sin kommunikation från Polisen ses ha separata telefoner för kriminella kontakter som exempelvis bara har SIM-kort som kopplar upp via datanätet. Det förekommer även fortsatt att kriminella använder krypterade telefoner så som Blackberry.

Polisen ser att de kriminella har lämnat de traditionella kommunikationsverktygen bakom sig och använder sig numera istället av digitala lösningar såsom chattapplikationer. De kriminella vet att polisen har svårt att komma åt den digitala trafiken. Det gör att de kriminella idag inte på samma sätt som tidigare aktivt behöver anstränga sig för att skydda sin kommunikation utan endast behöver använda krypteringstjänster. Även säkerhet, lönsamhet och flexibilitet spelar stor roll i sammanhanget. Detta i kombination med att brottsligheten många gånger är gränsöverskridande gör att behovet av snabb och säker kommunikation är mycket eftertraktad. I den gränsöverskridande brottsligheten är digitala applikationer ett enkelt sätt att hålla kostnaderna nere.

För aktörer inom människohandel och koppleri är kommunikationen central i kontrollsyfte. De exploaterade måste löpande rapportera in när de har sexköpare på ingång, hur mycket köparen har betalat, beställa transport osv. Genom digitala lösningar, så som krypterade chattar, förenklas denna process avsevärt jämfört med traditionell telefoni och människohandlare och brottsoffer kan hela tiden vara uppkopplade mot varandra. Något som förstärker känslan av kontroll och övervakning av den exploaterade parten. På liknande sätt sker kontroll av kurirer vid vapen och narkotika smuggling.

Polisens möjlighet att inhämta information i enlighet med IHL

En viktig del i polisens underrättelsearbete är att analysera kommunikation mellan kriminella för att identifiera brottssamverkan och binda personer genom kommunikationsutrustning till vissa platser för att utifrån det kunna vidta operativa åtgärder. IHL ger Polisen rätt att i underrättelsesyfte, i hemlighet, inhämta sådan information om det är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Enligt lagen ska informationen kunna inhämtas från den som tillhandahåller ett elektroniskt kommunikationssätt eller en elektronisk kommunikationstjänst. Lagen gör ingen skillnad på om informationen överförts via teleoperatörernas master eller 3G och 4G näten och ifall informationen överförts krypterad eller inte. Idag kan dock teleoperatörerna i Sverige inte se information som går krypterat via datanät vilket innebär att Polisen idag inte kan inhämta sådan information. I praktiken innebär det att dagens verktyg för att verkställa IHL inte är tillräckligt för att inhämta den information som Polisen enligt lag har rätt att ta del av.

Polisen upplever att telefonlistor som inhämtas från telefonbolagen saknar användbar information. Underrättelsetjänsten kan ha en god uppfattning om en persons brottsliga verksamhet och vilket eller vilka telefonnummer denna använder men det saknas bevisning då kommunikationen skett via datatrafik krypterat och därför inte syns i listorna. Vid telefon- och datatömningar i förundersökningar kan detta ofta bekräftas. Då man i tömningarna kan se att den misstänkta haft kriminella kontakter via krypterade kommunikationskanaler via appar eller plattformar på nätet som Polisen i underrättelsefasen inte känt till och kunnat agera utifrån.

Teknikutvecklingen och förändrade förutsättningar för kommunikation

De elektroniska kommunikationssätten är i dag mångfaldiga i jämförelse med tidigare då telefonsamtal och sms via telefonoperatörernas nät, tillsammans med mail, var dominerande. Smartphones, sociala medier och lättillgängliga appar som erbjuder gratis internationella förbindelser har förändrat den sociala interaktionen och kommunikationsmönstret i samhället i stort. Tillflödet av nya digi-

tala kommunikationssätt möjliggör enklare, billigare och krypterad kommunikation mellan människor både inom och utanför Sverige. Ett sådant kommunikationssätt är chattappar som har funktioner som saknas i vanliga sms och som enklare medger gruppchattar. Det gör apparna attraktiva och användandet av krypterade kommunikationssätt är idag lättillgängligt och utbrett. Många gånger är tjänsterna krypterade som standard och att skicka krypterad information behöver därför inte alltid vara ett aktivt ställningstagande. Några exempel på sådana är chattappar är *WhatsApp* och *Viber*. Apparna används inte enbart av de som aktivt söker vägar att skydda sin kommunikation utan av gemene man.

Det förekommer även att kommunikationsutrustning har som standard och är förprogrammerade att företrädelsevis låta kommunikation gå som krypterad datatrafik framför vanlig trafik i telenätet. Ett exempel på det är *Imessage* på Iphone där meddelanden mellan Apple-användare automatiskt sker krypterat via datatrafik.

Utvecklingen går mot att kommunikation krypteras i allt högre utsträckning och att krypterade tjänster erbjuds användaren utan användaren behöver göra någon aktiv krypteringsåtgärd.

Avancerad kryptering, krypterade nätverk och brottsforum på internet

Teknikutvecklingen har inte bara förändrat den organiserade brottslighetens kommunikationsvägar utan även mötesforum- och brottsplatser. Där en överflyttning till internet till viss del skett. Darknet innefattar en dold och krypterad del av internet som kräver särskild programvara för att kunna ansluta till. Det mest kända kryptonätverket är Tor (The Onion Router) som kan användas av vem som helst. Idag kan man ladda ner Tor-applikationer till en vanlig mobiltelefon. Tor krypterar inte bara kommunikationen, nätverket gör även alla användare och platser inom nätverket helt anonyma. Detta har gjort att stora marknadsplatser för illegala varor har kunnat skapas och inte kunnat stängas ner. Idag pågår en öppen handel av en stor mängd illegala varor på Darknet. Det kan handla om vapen, narkotika, gift, bilder på sexuella övergrepp på barn, förfalskad valuta, förfalskade ID-handlingar, hackade konton, hacker programvara med mera.

Utöver den inbyggda krypteringen i Tor så använder de kriminella ytterligare flera lager av kryptering i sin kommunikation mellan varandra. Man använder VPN (virtuellt privat nätverk) för att ansluta till Tor, vilket gör att man inte kan avanonymisera användarna om man skulle ta kontroll över hela Tor-nätverket. Man använder PGP-kryptering för att ytterligare kryptera den skickade informationen, vilket innebär att inte ens den som tillhandahåller marknadsplatsen eller tjänsten på Tor-nätverket kan avkryptera, utan bara den som verkligen är ämnad att ta emot informationen. Man använder kryptovaluta för att anonymt kunna genomföra penningtransaktioner och så vidare. På Darknet finns även ospårbara kryptomailtjänster och chattjänster. Inte ens med rättshjälp kan man få ut någon information i efterhand eftersom man inte ens vet vilket land man skulle skicka en rättshjälp till. Det enda sätt för rättsvårdande myndigheter att idag kunna komma runt krypteringen är att fånga upp informationen innan den krypteras. Hemlig dataavläsning skulle vara en metod för att göra det.

Ett exempel kan ges från ett underrättelseärende Polisen bedrev 2016. Polisen hade underrättelseinformation om att en person i Skåne höll på med omfattande brottslig verksamhet på Darknet. Polisen misstänkte att det handlade om storskalig försäljning av narkotika samt fentanyl på olika marknadsplatser. Verksamheten bedömdes vara så omfattande att de borde vara ett flertal personer inblandade med olika roller i brottsupplägget. Med anledning av detta togs en telefonlista in i enlighet med IHL för att kartlägga nätverket, hitta ytterligare medverkande och kanske få en uppfattning om rollfördelningen. Telefonlistan gav i princip ingen information av värde. En förundersökning kunde så småningom inledas ändå och efter ett tag bedömdes personen vi börjat med vara huvudman. Tillslag och husrannsakan genomfördes och stora mängder narkotika togs i beslag. Först efter analys av dator och en krypterad email som man lyckats hitta lösenordet till kunde man konstatera att det fanns ytterligare en huvudman. De två huvudmännen hade daglig kontakt via den krypterade mailen och återkommande tillfällen via en chattjänst på Tor. De två huvudmännen hade inte haft ett enda fysiskt möte under flera månaders spaning och inte ett enda telefonsamtal eller SMS. Det enda sättet att få kunskap om deras kommunikation i underrättelsefasen hade varit genom hemlig dataavläsning. Tack vare att man i efterhand kunde avkryptera kommuni-

kationen så kunde båda huvudmännen dömas. Båda fick 10 års fängelse. Med hjälp av hemlig dataavläsning hade man kanske inte varit beroende av denna tursamma slump.

Slutdiskussion

De brott som Polisen har rätt att inhämta information kring i enlighet med IHL är grova brott som medför stor påverkan på samhället. Det rör brottslighet som genererar stora summor pengar, som innebär men för enskilda och som påverkar allmänhetens trygghet och tilltro till rättssamhället. Brottsligheten är ofta komplex och karaktäriseras av ständig utveckling där de kriminella anpassar sig till polisens metodik. Det utgör en stor utmaning för polisen och måste bekämpas med ett proaktivt arbetsätt där kunskap om kriminella aktörer är en av förutsättningarna. Möjlighet till underrättelseinhämtning av uppgifter om elektronisk kommunikation är avgörande för att bekämpa den brottslighet som polisen i dag och i framtiden har att bekämpa.

Den utökade användningen av krypterad kommunikation har för polisens del det inneburit att underrättelsearbetet försvårats då inhämtning i enlighet med IHL många gånger varit verkningslös. Detta som tidigare nämnts på grund av att kriminella i mindre utsträckning idag använder okrypterad traditionell telekommunikation som är det Polisen idag rent faktiskt har verktyg till att inhämta genom IHL. Tillsammans med en ökad brottslighet på internet och den avancerade krypteringen som sker på Darknet är det en stor utmaning för Polisen att hantera. För att kunna fullgöra den uppgift Polisen är ålagd att göra enligt Polislagen krävs ändamålsenliga verktyg och att Polisen ges samma möjligheter att agera på internet som i den reella världen. En del i det innefattar verktyg att samla elektronisk kommunikation som går krypterat via datanätet. Hemlig dataavläsning skulle ge Polisen möjlighet att utföra en effektivare brottsbekämpning.

Klarar inte de rättvårdande myndigheterna att hantera den organiserade brottsligheten riskerar den att urholka rättsstaten och i förlängningen det demokratiska samhället. I särskilt utsatta områden anses läget akut. Ett redan sargat förtroende för rättsstaten riskerar där att fördjupas om inte polisen effektivare klarar att stävja den

öppen narkotikahandel och de dödsskjutningar som utvecklats på senare år. Det är därför av stor vikt att säkerställa att de brottsförebyggande myndigheterna kan upprätthålla sin förmåga att bekämpa brott. Med den snabba teknikutveckling som skett har polisen i bekämpningen av allvarlig och organiserad brottslighet kommit att ligga steget efter vilket försvårar både underrättelse- och utredningsarbetet. Det är därför av yttersta vikt att nya metoder ges till polisen för att Polisen även fortsättningsvis framgångsrikt kunna angripa dessa brott.

ÅKLAGARMYNDIGHETEN

Åklagarmyndighetens behovsbeskrivning avseende hemlig dataavläsning

Bakgrund

Införandet av tvångsmedlet hemlig avlyssning av elektronisk kommunikation (HAK) i slutet av 1990-talet (då hemlig teleavlyssning) innebar ett stort steg framåt avseende bevissäkring i brottmål och därmed för brottsbekämpningen i stort. Ungefär i mitten av 2000-talet kunde en ny trend skönjas. Alltfler kommunikationslösningar blev tillgängliga via internet och i takt med att kriminella började använda sig av nya kommunikationssätt har HAK som metod blivit allt mindre betydelsefull. Kriminella personer räknar idag med att deras telefoner kan vara avlyssnade. Det gjorde de även i slutet av 1990-talet, men den avgörande skillnaden är att det då inte fanns så många andra kommunikationsmöjligheter tillgängliga för realtidskommunikation. För att kringgå en eventuell avlyssning kunde kriminella använda sig av kodord eller omskrivningar. Inte sällan var det ändå ganska enkelt för utredarna att förstå vad de avlyssnade pratade om.

I takt med att nya kommunikationslösningar har gjorts tillgängliga, som t.ex. Skype, Viber, WhatsApp, Signal m.fl. har de kriminella i ökande grad i stället övergått till just dessa tjänster. Det största problemet, ur polisens och åklagarens perspektiv, är att dessa tjänster normalt innebär att kommunikationen är hårt *krypterad*. Tjänsterna kan installeras på en kommunicerande enhet, vanligen en dator eller en mobiltelefon, och kan t.ex. användas via anonyma internetuppkopplingar i stället för via mobiloperatörer där abonnemang och telefoner lättare kan knytas till en användare. Enligt uppgift från nationellt IT-brottscentrum är uppåt 90 procent av internetavlyssningen omöjlig att avlyssna på grund av kryptering. Ett annat problem är att även de enheter som används för kommunikation, typiskt

sett mobiltelefoner och datorer jämte externa hårddiskar och annan lagringsmedia, numera är krypterade. Även med dagens kraftfulla dekrypteringsprogram är det i princip omöjligt att knäcka annat än de allra enklaste lösenorden. Detta betyder att det också blir allt svårare att undersöka enheterna inom ramen för beslag.

De befintliga tvångsmedlens effektivitet har i takt med teknikutvecklingen minskat kraftigt de senaste 10 åren. Men samtidigt som den tekniska utvecklingen idag ger de brottsbekämpande myndigheterna stora utmaningar innebär den också möjligheter till nya och effektivare utredningsmetoder.

Behov

Ett samhälle behöver effektivt kunna skydda sig mot kriminalitet, och därmed måste det finnas effektiva metoder att säkra bevis med. Det finns också internationella åtaganden som gör att vi måste upprätthålla en effektiv brottsbekämpning (t.ex. The Financial Action Task Force, FATF). Mot denna bakgrund är det mycket angeläget för de brottsbekämpande myndigheterna att få ett nytt tvångsmedel, vi kallar det HDA i fortsättningen, som möter den teknikutveckling som skett. Behoven, som kan indelas i flera delar, speglar de problem eller hinder för det brottsbekämpande arbetet som teknikutvecklingen har fört med sig.

a) Att omvandla kryptering till klartext

Det tillkommer ständigt nya program och applikationer för kommunikation som bygger på nya krypteringsprinciper. Eftersom kommunikationen kan ske anonymt via internet är det nästan omöjligt att avlyssna kommunikationen även om kommunikationen skulle vara möjlig att dekryptera.

Det mest effektiva sättet att angripa problemet vore HDA som möjliggör att avlyssningen kan ske direkt på de kommunicerande enheterna och som därmed möjliggör att avlyssningen kan ske i själva enheten innan programmet eller applikationen krypterar trafiken. Det kan tilläggas att idag omfattas – till skillnad från t.ex. mobiltelefonoperatörer – inte internetoperatörer, s.k. *Internet service providers* (ISP), av den s.k. anpassningsskyldigheten i 6 kap. 19 §

LEK och därmed inte av skyldigheten att se till att trafiken kan avlyssnas okrypterat.

En fråga man bör ställa sig är varför det idag inte är möjligt att avlyssna en enhet genom att t.ex. installera hårdvara eller att installera en programvara i en dator eller telefon. Detta beror i huvudsak på två omständigheter. Att installera t.ex. hårdvara på en dator eller en telefon innebär att föremålet måste tas i beslag. Enligt nuvarande beslagsregler är det inte möjligt med ”hemliga beslag” på ett sätt som t.ex. motsvarar ”hemlig husrannsakan”. Det senare är möjligt eftersom den som tvångsåtgärden riktas emot inte behöver underrättas förrän detta kan ske utan men för utredningen (28 kap 7 § BrB). Avseende beslag ska den som beslaget riktas mot i stället skyndsamt underrättas om att beslag har skett (27 kap 11 § BrB). Att i stället skicka in programvara i en dator skulle innebära ett dataintrång. Ett beslut från domstol om tillstånd till avlyssning gör inte en sådan åtgärd lovlig. Utgångspunkten är ju att domstolen ger tillstånd till avlyssning av en teleadress, men den sanktionerar inte metoden för avlyssningen som i stället måste följa övrig lagstiftning.

För att möjliggöra en avlyssning av krypterade meddelanden på en misstänkt persons telefon, dator eller liknande genom exempelvis installation av en hård- eller mjukvara fordras alltså även en uttrycklig möjlighet att verkställa denna åtgärd, vare sig detta sker genom intrång i slutet förvar, genom dataintrång eller på annat sätt.

b) En metod för att komma åt lösenord och liknande för att underlätta undersökning av beslag – keylogger

För att komma åt lagrade uppgifter i t.ex. datorer, telefoner eller usbminnen behöver brottsutredande myndigheter i förekommande fall ha tillgång till lösenord.

I princip all hårdvara har någon form av skydd som hindrar vem som helst från att komma in i telefonen eller datorn. Det kan vara ett enklare lösenord som man behöver för att komma in i datorn, t.ex. ett Windows-lösenord eller en pinkod eller ett fingeravtryck för att komma in i telefonen. Detta behöver normalt inte betyda att det är något avgörande problem att komma åt innehållet eftersom det ofta bara handlar om ett enklare åtkomstskydd som det är möjligt att komma runt.

Däremot kan det också finnas ett krypteringsprogram på hårdvaran, t.ex. Truecrypt eller Bitlocker eller inbyggd programvara som i t.ex. IOS (Apple). Med kryptering menar vi i en vidare bemärkelse en särskild programvara med ett lösenord som gör att innehållet på datorn eller mobilen blir krypterat på ett sådant sätt att den enda möjligheten att kunna ta del av informationen där är att presentera rätt lösenord. Idag finns det, starkt förenklat, bara tre saker som gör det möjligt att hitta rätt lösenord.

1. *Brute force*, dvs. att med hjälp av särskilda program och särskilda algoritmer gissa lösenordet. I praktiken är det omöjligt om inte lösenordet är av mycket enkel beskaffenhet.
2. Att den misstänkte frivilligt lämnar ut lösenordet.
3. Att lösenordet kan fås fram på annat sätt, t.ex. att det finns på en lapp i gärningsmannens bostad eller om det kan hämtas ut genom att man söker efter lösenord i datorns internminne om datorn är igång vid ett tillslag.

I praktiken är dessa metoder förenade med olika svårigheter och fungerar kanske i hälften av de fall som vi har. Det betyder att vi därmed i övriga fall inte kommer åt viktig information som skulle kunna utgöra bevisning för brott.

En lösning skulle därmed vara möjligheten att i hemlighet installera en programvara på en dator eller telefon som t.ex. registrerar knapptryckningar, en s.k. *keylogger*. Genom att den skickar knapptryckningarna i en särskild fil så skulle en it-forensiker utifrån en analys får fram det lösenord som den misstänkte slår in på datorn eller telefonen och därmed skulle polisen kunna komma in i en krypterad dator eller telefon som tas i beslag.

c) Tillgång till krypterad information i informationsbärare på distans

I utredningar om grov brottslighet förekommer regelmässigt beslag av informationsbärare av olika slag såsom datorer, mobiltelefoner, usb-minnen etc. När man väl kommer åt informationen i dessa beslag visar sig denna många gånger vara mycket värdefull för utredningen. Det kan röra sig om intressanta uppgifter i själva den information som lagrats där (vad har förmedlats till och från användaren)

eller uppgifter om själva användandet av informationsbäraren (t.ex. när och möjligen var informationsbäraren har varit aktiv). Vid utredningar om brott där den databurna informationen utgör brottslighetens själva mål eller medel är tillgången till denna information omistlig för utredningen.

Möjligheten att med viss programvara radera all möjlig information – vilket även låter sig göra på distans för såväl mobiltelefoner som datorer – gör att en undersökning av en beslagtagen informationsbärare visar vad som finns i denna vid undersökningstillfället men inte nödvändigtvis vad som har funnits där tidigare och om information har tillförts eller tagits bort från informationsbäraren.

Det tycks saknas någon säker statistik på hur ofta förekommande det är att information i datorer/mobiltelefoner m.m. i beslag har raderats. En erfaren it-forensiker vid Region syd uppskattar företeelsen som ökande i ärenden om grov brottslighet och har erfarit det främst i ärenden med väl teknikmedvetna misstänkta som är måna om att dölja sina förehavanden. Enligt denna uppskattning förekommer detta i uppemot vart åttonde ärende.

Vid utredning av pågående brottslighet – vare sig det handlar om narkotikahantering, framställning och spridning av barnpornografi, människohandel, grovt penningtvättsbrott, bedrägeri eller annat – finns ofta ett behov av att kunna ta del av både kommunikation och lagrad information i datamedier löpande och i realtid. Behovet kommer troligtvis att växa, eftersom trenden tycks gå mot att hårddiskar försvinner till förmån för molntjänster och att den information av intresse som befinner sig närmast användaren är datorns eller telefonens arbetsminne (RAM-minnet). Av intresse blir då att ta del av informationen i RAM-minnet alternativt ta sig in i de molntjänster som utnyttjas för lagring av information.

Fördelarna med en möjlighet att under hand och i hemlighet kunna inhämta och kontrollera innehållet i en informationsbärare är flera. En förutsättning för att nå framgång med denna metod är att den utförs i hemlighet.

- Metoden kan användas för att ta ut stickprov i syfte att kontrollera att det t.ex. är rätt dator man är intresserad av, vilket i någon mån kan begränsa omfattningen av tillämpningen av hemliga tvångsmedel för de fall man tagit miste eller datorn bytt användare.

- Genom denna åtgärd kan man under hand på distans plocka ut information som lagras i RAM-minnet för att komma åt lösenord, vilka kan ändras också de på distans, men även se vilken information som datorn har tillgång till för tillfället.
- Löpande undersökningar av innehållet i t.ex. en dator kan tillsammans med fysisk spaning mot den misstänkte knyta den misstänkte till den information som fanns i datorn vid en viss tidpunkt.
- Löpande undersökningar över tid gör det möjligt att säkra bevisning som sedan försvinner på grund av att den misstänkte använder raderingsprogram. Radering kan ske på distans. Även vid ett tillslag kan det finnas möjlighet för en misstänkt person eller dennes medhjälpare att effektuera en radering av information innan informationsbärarens innehåll hunnit säkras av it-forensiker. Radering på distans har erfarits t.ex. i samband med undersökning av beslagtagna mobiltelefoner. Risken för liknande radering är också påtaglig beträffande information som sparas i molntjänster. Utan möjlighet till löpande tömningar av information från en informationsbärare skulle HDA som metod för att få fram lösenord till krypteringsprogram vara verkningslös, om de kriminella kunde omintetgöra en undersökning av ett beslag genom att använda raderingsprogram. Metoden behövs med andra ord för att motverka den givna motåtgärd som de kriminella kan sätta in för att skydda icke raderad information i samband med beslag.
- I samband med tillslag och direkt därpå inledande undersökning av dator kan uppdagas att datorn har en öppen anslutning till en annan dator, t.ex. en filserver som den arbetar mot. Denna dator kan vara omöjlig att lokalisera exakt för undersökning. En husrannsakan på distans skulle då vara den enda möjligheten att säkra information från den datorn.
- När det gäller molntjänster kan det konstateras att det ofta är en tidskrävande uppgift att begära in uppgifter som den misstänkte har i s.k. molntjänster. Genom metoden kan det i särskilda fall vara möjlig att se det material på datorn som vanligtvis ligger i molntjänster som datorn har kopplingar till. Man kan då nämligen från RAM-minnet komma åt information som hämtas in från molntjänster i realtid genom att man läser av informationen

från användarens dator i samband med att de öppnar eller hämtar filer från molntjänsten.

I samband med tillslag och direkt därpå inledande undersökning av dator kan uppdagas att datorn har en öppen anslutning till en annan dator, t.ex. en filserver som den arbetar mot. Denna dator kan vara omöjlig att lokalisera exakt för undersökning. En husrannsakan på distans skulle då vara den enda möjligheten att säkra information från den datorn.

d) Aktivera funktionaliteter i teknisk utrustning

Hemlig rumsavlyssning (HRA) inriktar sig på en misstänkt persons kommunikation med andra och avser installation av avlyssningsutrustning på en specifik plats. Anledningen till att detta tvångsmedel begränsas till en plats synes vara praktisk, eftersom det tidigare inte funnits någon annan möjlighet att tekniskt gå till väga för att fånga upp talet än genom att placera avlyssningsutrustningen i den misstänktes bostad eller på en annan specifik plats där det finns särskild anledning anta att den misstänkte kommer att uppehålla sig. – I detta sammanhang bortses från möjligheterna att avlyssna en telefon genom HAK.

Hemlig kameraövervakning (HKÖ) är inriktad på att övervaka dels den plats där ett brott har begåtts för att därigenom finna en misstänkt person, dels en plats där en redan misstänkt person kan antas komma att uppehålla sig.

När det gäller internetrelaterad brottslighet eller annan brottslighet som kan genomföras med användande av telefon eller dator kan man tänka sig att den geografiska platsen för brottets utförande är sekundär i förhållande till medlet för brottets genomförande – datorn eller telefonen – eller annorlunda uttryckt: Datorn eller telefonen utgör den arena (plats) på vilken brottet utförs. Till följd av detta resonemang kan man därför argumentera för att datorn och telefonen, som båda ofta är flyttbara, utgör den plats där man förväntar sig finna en känd eller okänd gärningsman och där man vill kunna installera hemlig rumsavlyssning eller kameraövervakning.

Det är den tekniska utvecklingen av bl.a. datorer och mobiltelefoner som nu gör det möjligt att avlyssna eller ta fotografier från den telefon eller dator som en misstänkt person bär med sig. Behovet av

(eller tanken på möjligheten) att använda denna teknik kunde knappast ha formulerats innan själva tekniken uppfunnits som gör det möjligt.

d.i) Som en metod för att identifiera användaren

I en brottsutredning behöver man identifiera vilken person som använder eller har använt en viss telefon eller dator. En metod för att identifiera en användare av en telefon eller ett telefonnummer är att kartlägga dess kontakter med andra, tiderna och platserna för detta samt dess plats för ”nattvila”. Behovet av att kunna identifiera användaren gäller också under tid, eftersom kriminella ibland byter telefoner med varandra. Man kan alltså inte alltid utgå från att en telefon hela tiden används av en och samma person. Och i de fall utredarna är säkra på användarens identitet ifrågasätter inte sällan försvaret att det är den misstänkte som hanterat datorn eller telefonen vid de kritiska tillfällena eller över huvud taget – bl.a. med argumentet att telefonen har använts av flera personer. Det kan i sådana fall bli aktuellt med tidsödande analyser av telefonlistor, röstanalys eller andra utredningsåtgärder för att motbevisa invändningen om att det inte är den misstänkte som använt datorn eller telefonen vid ett eller flera tillfällen.

En möjlighet att med kameraaktivering ta bilder från en telefon eller dator innebär att man kan klargöra detta mera definitivt och spara stora utredningsresurser. Det skulle också bidra till att lättare identifiera en misstänkt gärningsman och var han befinner sig vid vissa tillfällen. Genom aktivering av denna funktion skulle bevisningen om vem som hanterat viss telefon eller dator bli säkrare. Därigenom skulle utrymmet för missriktade misstankar och felaktigt beslutsunderlag minimeras, vilket skulle främja rättssäkerheten. Det är redan idag möjligt att genom fysisk spaning konstatera hur en person använder en telefon. Det betyder att integritetsförlusten i förhållande till vad som gäller idag är relativt liten medan effektivitetsvinsten blir betydande. Metoden skulle i detta avseende kunna begränsas till att ta ögonblicksbilder eller kortare ljudinspelningar just i syfte att identifiera användarens identitet vid en viss tidpunkt.

För det fall HDA begränsas till att vara en verkställighetsåtgärd avseende HKÖ kommer det att innebära att möjligheterna att ta en ögonblicksbild i syfte att identifiera en misstänkt kommer att vara

ytterst begränsade med hänvisning till de avgränsningar som HKÖ av integritetsskäl uppställer avseende exempelvis geografisk plats. Det finns därför skäl att införa en särreglering som ger möjlighet att aktivera kameran i den tekniska utrustningen, t.ex. en dator eller telefon, i syfte att endast dokumentera vem som vid en viss tidpunkt brukar den tekniska utrustningen oavsett geografisk plats.

d.ii) Ett effektivare sätt att använda och verkställa HRA och HKÖ

HRA och HKÖ är som metoder mycket resurskrävande, eftersom platsen för verkställighet ofta måste undersökas i förväg och säkras under själva monteringsfasen. Det är inte alltid som man uppnår en fullgod ljud- eller bildkvalitet. Platsen för HRA är i regel sådan som den misstänkte kan räkna med att kunna bli föremål för avlyssning på och som han därmed kan undvika att föra förtroliga samtal på. Naturligtvis kan en misstänksam kriminell person tänkas vara försiktig med att prata i närheten av sin mobiltelefon eller dator, men samtidigt har moderna människor mycket svårt för att vara utan dessa föremål, och den disciplin som skulle krävas för ett sådant agerande kan förväntas vara låg.

En metod för HRA eller HKÖ genom funktionsaktivering av mikrofonen eller kameran i en dator eller en telefon skulle innebära ett minskat behov av de nu gängse metoderna. Det integritetsintrång som är förenat med installation av hemlig avlyssningsutrustning i bostäder samt installation av avlyssningsutrustning och kameror på andra platser skulle härigenom i vissa fall kunna besparas de misstänkta och deras umgängeskrets.

I jämförelse med de nu gängse metoderna – som man är begränsad till att verkställa på platser där man kan anta att den misstänkte kommer att befinna sig – skulle metoden genom aktivering av funktioner i den misstänktes telefon möjliggöra avlyssningen/bildupptagningen utan dessa rumsliga begränsningar. Detta skulle naturligtvis innebära en enorm effektivitetsvinst, då metoden skulle kunna användas dygnet runt och oavsett var den misstänkte befinner sig.

Såväl HKÖ som HRA är begränsade med hänsyn till vissa skyddade platser och yrkeskategorier hos samtalspartner (se 27 kap 20 e § tredje stycket, 25 a § andra stycket, 22 § andra stycket med hänvisning till 36 kap 5 § andra till sjätte styckena rättegångsbalken).

Detta kan ha fortsatt giltighet även med en ny metod för detta. Det går att säkerställa att inte dessa bestämmelser överträds genom fysisk spaning och gps-positionering samt med en föreskrift om radering av inspelat material för det fall det vid granskningen av upptagningar kommer fram att dessa bestämmelser överträtts.

d.iii) Som en metod för gps-positionering

De lokaliseringsuppgifter som med tillämpning av ett beslut om HÖK normalt kan fås ut idag är sällan särskilt exakta eller tillförlitliga, bl.a. med hänsyn till att flera master kan täcka delvis samma område och att det kan vara närmast slumpmässigt vilken mast inom ett visst geografiskt område som kopplas upp vid telefonaktivitet. Graden av precision i lokaliseringen kan slå på flera kilometer. Det har dessutom förekommit att teleoperatörer haft olika syn på vilka uppgifter i detta hänseende som de varit förpliktade att lagra och lämna ut till brottsbekämpande myndigheter. Någon operatör har exempelvis vägrat lämna ut en basstations öppningsvinkel och riktning, vilket gett ytterligare en dimension åt graden av osäkerhet i precisionen. Från vissa operatörer kan efter EU-domstolens dom den 21 december 2016 (Tele2-domen) inte längre inhämtas uppgifter om telefonens position vid samtalets slut eller uppgifter om missade (ej besvarade) samtal. En positionering enligt den nu beskrivna ordningen kräver också att telefonen är aktiv, vilket sällan är fallet i direkt samband med utförande av brott. Lokaliseringsuppgifter genom mastpositionering är alltså ett ytterst trubbigt instrument som kräver omfattande analyser och ofta kompletterande utredning för att vara användbara som bevisning i domstol.

Tele2-domen och dess effekter på kort och lång sikt har angetts som ett argument för att införa gps-positionering som komplement till lokaliseringsuppgifter enligt lagen om elektronisk kommunikation. Det finns flera andra mycket starka skäl för att införa denna möjlighet till lokalisering.

Gps-positionering i mobiltelefon har aktualiserats först under de senaste åren i kölvattnet av den allmänna spridningen av mobiltelefoner med denna funktion. Denna möjlighet till lokalisering av misstänkta synes inte ha övervägts i tidigare lagstiftningsarbeten.

Gps-positionering skulle kunna användas för att lokalisera en dator eller mobiltelefon i realtid och detta med en exakthet som är

klart överlägsen de lokaliseringsuppgifter som teleoperatörer fram till EU-domen var skyldiga att lagra för brottsbekämpande ändamål enligt lagen om elektronisk kommunikation.

En lokalisering kan vara ett sätt att identifiera en gärningsman och/eller en brottsplats. Detta kan vara aktuellt i utredningar av alla typer av brott som involverar användandet av t.ex. en telefon eller dator.

Inom den grova organiserade brottsligheten omger sig de inblandade ofta av egna spanare för att i tid uppmärksamma polisnärvaro (motspaning). Därtill rör de sig ofta i homogena miljöer som är svåra att spana i. Gps-positionering skulle vara ett mycket bra verktyg vid spaning i annars svårspanade miljöer, både i landsbygds- och stadsmiljö, när det gäller att veta var den misstänkte befinner sig och för att vara beredd på oväntade förflyttningar, t.ex. inför stundande brottslighet. En gps-positionering har just den exakthet som man skulle önska av lokaliseringsuppgifter. Den skulle i många fall kunna leda till bevisning om möten och mötesplatser, brottsplatser och gömmor för bl.a. vapen och narkotika, visa flyktvägar samt leda till snabba ingripanden och kortare och mer effektiva utredningstider. Den hade kunnat vederlägga påståenden om alibi likaväl som avfärda misstankar. Att kvantifiera behovet av gps-positionering som en form av förbättrad metod för lokalisering kan göras ganska enkelt genom att utgå från antagandet att de allra flesta fall av begärda HÖK-uppgifter omfattar lokaliseringsuppgifter (på grund av ett behov) och att väsentligt förbättrade lokaliseringsuppgifter naturligtvis är önskvärda. Beslut om HAK omfattar samma uppgifter som avser HÖK, däribland lokaliseringsuppgifter. Det är en enorm skillnad att påstå att en person befunnit sig på brottsplatsen X vid tidpunkten Y med hjälp av en positioneringsuppgift som täcker ett område av flera kvarter en kvart före brottstidpunkten än att påstå detsamma med en exakt gps-positionering vid den exakta brottstidpunkten. Med den senare bevisningen skulle man förmodligen i flera fall kunna undvara vittnesförhör med personer som riskerar att drabbas av repressalier eller påtryckningar från de misstänktas sida. Vittnen tenderar i utredningar om grovt organiserad brottslighet i högre utsträckning sakna viljan att medverka till utredningen. I denna typ av ärenden förekommer att vittnen utsätts för otillåten påverkan för att ändra sina vittnesmål.

Några tänkbara exempel:
Mord sker. Offret hade strax före mordet telefonkontakt med ett okänt kontantkortsnummer. Gps-positionering av den telefonen skulle snabbt kunna leda fram till den person som disponerar den telefonen. Det alternativ som idag gäller är att inhämta beslut om HÖK och med hjälp av samtalslistor och lokaliseringsuppgifter försöka analysera fram vem som kan tänkas disponera telefonen.

Äldre människor utsätts i en stad eller område för stölder som föregås av telefonsamtal från någon som utger sig vara utsänd från hemtjänsten och som annonserar ett förestående hembesök. En person släpps därför snart in hos den äldre personen och uppehåller denna medan någon annan tar sig in i bostaden och stjäler värdesaker. Brottsligheten är omfattande och har ett högt straffvärde. Med en gps-positionering på telefonen kan ett snabbt ingripande ske och även identifiering av gärningsman/med-hjälpare med telefonen.

Hemlig telefonavlyssning pågår mot ett kriminellt gäng pga misstankar om förberedelse till mord. Fysisk spaning mot dessa är inte möjlig i alla skeden på grund av risken att röja spaningen. En skjutning rapporteras in och – på grund av pågående gps-positionering – kan man genast konstatera att en eller flera från gänget varit på platsen. Man kan snabbt följa flyktvägen från brottsplatsen och längs denna påträffa vapnet samt den eller de misstänkta.

Förundersökning pågår mot ett kriminellt nätverk som misstänks syssla med omfattande narkotikahantering. De misstänkta är ytterst försiktiga i sina rörelsemönster och använder visuell motspaning för att värja sig mot polisinsatser. Genom gps-positionering kan man följa deras rörelsemönster, upptäcka deras mötesplatser och narkotikagömmor och därmed förbereda tillslag.

e) En skyldighet för operatörer att medverka

När HDA ska verkställas kan det, för att i det enskilda fallet få en fungerande teknik på plats, bli nödvändigt med assistans i viss utsträckning av den aktuella mobiltelefon- eller internetoperatören. En sådan skyldighet att medverka bör därför övervägas för alla operatörer.

Ekobrottsmyndigheten
Swedish Economic Crime Authority

Ekobrottsmyndighetens behovsbeskrivning avseende hemlig dataavläsning

Hemlig dataavläsning behövs då nuvarande hemliga tvångsmedel inte längre är lika effektiva som förr. Orsaken till den minskade effektiviteten är främst den kryptering som både sker vid samtal och överföring av meddelanden i övrigt. Den snabba tekniska utvecklingen med ständigt utvidgade möjligheter till kommunikation och kryptering medför att möjligheterna till hemlig avlyssning av elektronisk kommunikation (HAK) minskat och kan antas komma att ytterligare minska. Exempelvis så är kommunikation via IT-baserade appar som är krypterade vanliga. Samtal och meddelanden kan inte avlyssnas när dessa appar används. Kriminella personer är medvetna om att de kan komma att avlyssnas och går därför i allt större utsträckning över till att kommunicera på sätt som medför att avlyssning inte är möjlig.

Behovet av hemlig dataavläsning ska också ses mot bakgrund av problemen att säkra bevisning efter beslag av exempelvis datorer där krypteringen eller lösenordsskydd försvårar eller omöjliggör att i efterhand ta fram information från datorn. Det bör även i detta sammanhang pekas på de svårigheter som uppkommer då det vid undersökning av datorer och mobiltelefoner framkommer att viss information finns lagrad externt i en s.k. molntjänst/lagringstjänst. Dessa tjänster kan användas både för att lagra information och för att dela den med andra. För ekonomisk brottslighet kan särskilt pekas på de molntjänster som nu finns för bokföring och förvaring av räkenskapsinformation. Den vanliga tolkningen av rättsläget är att det inte är tillåtet att med hjälp av den undersökta datorn eller mobiltelefonen få ta del av information som finns lagrad i dessa tjänster. Det är svårt att få tillgång till denna externt lagrade information. Det gäller särskilt då molntjänster/lagringstjänster erbjuds av utländska företag och informationen som kan lagras på olika platser är svår att erhålla med internationell rättslig hjälp. I vart fall är det en mycket

tidsödande process som kan medföra att bevisvärdet minskar av den information som kan säkras.

Hemlig dataavläsning skulle i dessa fall ge en möjlighet att få den information som inte på grund av kryptering kan erhållas vare sig vid avlyssningen eller från beslagtagna datorer eller mobiltelefoner.

Behovet av hemlig dataavläsning finns vid de flesta utredningar av allvarlig brottslighet där hemliga tvångsmedel används. Här kommer att tas upp några särskilda problem vid utredningar om grov ekonomisk brottslighet. I många av utredningarna finns ofta bakomliggande huvudmän som styr den brottsliga verksamheten. De döljer sig bakom målvakter[4] och den brottsliga verksamheten utförs ofta med utnyttjande av företag, främst aktiebolag, som brottsverktyg. I förundersökningarna är det förenat med avsevärda svårigheter att lagföra dessa bakomliggande huvudmän. En väg att kunna binda bakomliggande huvudmän till aktuell brottslighet är att visa att de som faktiska företrädare har ett bestämmande inflytande över det aktiebolag där den brottsliga verksamheten bedrivs och framförallt är de som styr tillgångarna i bolaget. Det blir därför viktigt att kunna ”följa pengarna” för att visa vem som har möjlighet att faktiskt överföra medel både på bolagets konton och andra konton med anknytning till brottsligheten. Detta är också en viktig del i arbetat med att angripa brottsvinster. Det går inte att med sedvanliga utredningsåtgärder, exempelvis spaning, att identifiera och binda dessa bakomliggande huvudmän till den aktuella brottsligheten. Andra medverkande såsom målvakter m.fl. avslöjar inte vem som är den bakomliggande huvudmannen. I dessa fall kan hemliga tvångsmedel, främst HAK, vara lösningen men eftersom kommunikationen numera ofta är krypterad så kommer förundersökningarna i många fall att få begränsas till målvakter och andra medverkande som inte egentligen styrt brottsligheten eller gjort någon större brottsvinst. De som har resurser och kunskaper om hur man undgår avlyssning och inte lämnar ”sökbara spår” som kan utnyttjas i utredningarna undkommer lagföring som istället drabbar målvakter och andra utan erfaren-

[4] Med målvakt avses inom ekobrottsbekämpningen en person som aldrig har för avsikt att seriöst delta i ett aktiebolags verksamhet utan enbart lånar ut sitt namn för att lagens formella krav ska uppfyllas. De saknar som regel kännedom om den verksamhet som de företräder men är beredda att mot ersättning bära det formella och straffrättsliga ansvaret för bolagets handlande. Bolaget kan också redan ha plundrats på sina tillgångar och stå utan både ledning och verksamhet men målvakten sätts in i slutskedet med den beräkningen att efterräkningarna ska drabba denne och inte dem som legat bakom plundringen.

het och/eller kunskaper inom området. I andra utredningar om ekonomisk brottslighet, såsom punktskatteärenden, MTIC-ärenden och penningtvättbrott, är problematiken likartad.

Det finns därför ett behov av att med hemlig dataavläsning av den misstänktes dator eller mobiltelefon löpande och i realtid kunna ta del av både kommunikation och lagrad information innan den krypteras samt även identiteten på den utrustning som den misstänkte kommunicerar med. De fördelar som detta skulle kunna ge i utredningar om ekonomisk brottslighet är främst följande.

- Det går att visa vem som är bakomliggande huvudman genom att den brottsliga verksamheten handläggs (administreras) från den misstänktes dator eller mobiltelefon. Administrationen kan bestå i ”svart bokföring”, kontoöverföringar från det aktiebolag som används som brottsverktyg eller framställning av falska/oriktiga fakturor. Det kan också vara fråga om insiderinformationen vid ett insiderbrott.
- Genom att löpande kunna följa kommunikation och kontoöverföringar över internet kan bevisning succesivt säkras under den pågående förundersökningen. Det kan ske genom spaning, bankförfrågningar m.m.
- Det går att säkra bevisning som annars skulle vara ”dold” i molntjänster/lagringstjänster.
- Det går att säkra information i datorer och mobiltelefoner innan informationen raderas.
- Det går att säkra lösenord så att vid tillslag tillgång kan fås till krypterad information.
- Det går att löpande följa kontoöverföringar via internet så att vid tillslag tillgångar kan säkras.

För att den hemliga dataavläsningen skulle bli fullt ut effektiv krävs att olika funktionaliteter aktiveras i datorer och mobiltelefoner m.m. Det är först genom den tekniska utvecklingen som denna möjlighet uppkommit men måste också ses som en följd av att brottsligheten sker med hjälp av bärbara datorer och mobiltelefoner som inte är bundna till viss plats vilket innebär helt andra möjligheter för kriminella att både utföra och dölja den pågående brottsligheten. Genom

att aktivera datormediets kamera eller GPS-positionering skulle förbättra förutsättningar för att säkra bevisning och klargöra vem som är användare av datormediet då det används vid brottslig verksamhet.

Den exakthet som en GPS-positionering ger ska jämföras med de lokaliseringsuppgifter som nu erhålls efter ett tillstånd till hemlig övervakning av elektronisk kommunikation (HÖK). Dessa är inte så exakta då de bygger på uppgifter från master där det kan vara närmas slumpmässigt vilken mast som kopplas upp mot aktuell mobiltelefon. Till det kommer också att teleoperatörerna har olika syn på vilka uppgifter i detta hänseende som de är förpliktigade att lagra och lämna ut efter EU-domstolens förhandsavgörande den 21 december 2016. Lokaliseringsuppgifter genom mastpositionering är därför inte så exakt och kräver ofta kompletterande utredning. GPS-positioneringen skulle kunna användas för att lokalisera en dator eller mobiltelefon löpande i realtid med en exakthet som är klart överlägsen de lokaliseringsuppgifter som erhålls efter beslut om HÖK. Behovet av GPS-positionering kan ta sin utgångspunkt i den omfattning som lokaliseringsuppgifter omfattas av ansökningar om HÖK och HAK. De fördelar som detta skulle kunna ge i utredningar om ekonomisk brottslighet är främst följande.

– Det skulle gå att lokalisera brottsplatser som kan vid ekonomisk brottslighet vara ”kontoret” varifrån exempelvis den svarta verksamheten handläggs, varifrån de ”svarta kontanta utbetalningarna” sker etc. Genom spaningsinsatser kan från platserna bevisning säkras om den brottsliga verksamheten.
– Det skulle gå att med exakthet lokalisera de datorer eller mobiltelefoner varifrån t.ex. kontoöverföringar sker och därigenom med spaning kunna få bevisning om användaren, se nedan om att identifiera användaren (misstänkt).
– Det skulle vid en s.k. bolagstömning (oredlighet mot borgenär) ge möjlighet att lokalisera bolagets tillgångar.
– Vid ett tillslag skulle genom lokalisering av datorer och mobiltelefoner bevisning kunna säkras och misstänkta kunna anträffas.

Även om det kan visas att det är den misstänktes dator eller mobiltelefon som använts vid den brottsliga verksamhet så är en vanlig invändning att det inte är han eller hon som vid tillfället innehaft och

använt datorn eller mobiltelefonen. Några uppgifter om vem denne person är lämnas inte. Invändningar av detta slag är ofta svåra att motbevisa även om omfattande utredning sker exempelvis genom analys av telefonlistor. Detta gäller särskilt när förundersökningarna rör organiserad brottslighet. Genom att aktivera kameran i datorn eller mobiltelefonen skulle användaren i dessa fall kunna identifieras. Vid en hemlig dataavläsning som sker i realtid skulle metoden kunna begränsas till de tider då den brottsliga gärningen utförs.

Alternativa lösningar

Vid de förundersökningar som bedrivs vid Ekobrottsmyndigheten används hemliga tvångsmedel främst i ärenden avseende grov ekonomisk brottslighet. I dessa ärenden har innan hemliga tvångsmedel blir aktuella konstaterats att ordinarie utredningsmetoder såsom spaning inte är möjliga i ärendet eller i vart fall inte kan ge tillräcklig bevisning för att driva förundersökningen framåt. Hemliga tvångsmedel blir då aktuella och vanligen då HAK som ofta inleds med en HÖK. De alternativa lösningar som kan tänkas utgör då andra hemliga tvångsmedel, främst hemlig kameraövervakning (HKÖ). Det kan här tilläggas att vid Ekobrottsmyndigheten handläggs enbart brott som inte ger möjlighet att ansöka om hemlig rumsavlyssning (HRA). Hemlig kameraövervakning är begränsad till viss plats vilket begränsar användningsområdet. För att HKÖ ska kunna vara ett effektivt krävs kännedom om t.ex. var den brottsliga verksamheten handläggs. Det är ovanligt med sådan kännedom och även om så är fallet ger det sällan bevisning om sådant som bakomliggande huvudmäns medverkan i brottsligheten. HKÖ utgör därför inte ett alternativ till HAK.

Tidigare kunde ofta från beslag, då främst datorer, erhållas avgörande bevisning om den ekonomiska brottsligheten. Denna möjlighet har dock begränsats på grund av att datorer m.m. i ökad utsträckning är krypterade och/eller lösenordskyddade eller att ett raderingsprogram använts. Det är förenat med stora svårigheter att vid ett tillslag få tillgång till en dator innan den stängs av och mycket ovanligt att uppgifter om lösenord hittas vid husrannsakan eller lämnas ut av misstänkt.

Problemens omfattning

Det är svårt att närmare ange hur vanlig kryptering är. Det finns fall då avlyssning avbryts då det på grund av kryptering inte är meningsfullt att fortsätta avlyssningen och eventuellt kan också finnas fall där det på grund av kännedom om att kryptering används det inte anses möjligt att använda HAK. Det förs inte vid Ekobrottsmyndigheten någon närmare statistik över omfattningen av krypterade och/eller lösenordskyddade datorer m.m. Det kan dock konstateras att kryptering är vanlig vilket bl.a. framkommit vid de forensiska undersökningarna av beslagtagna datorer, mobiltelefoner etc. Det kan också konstateras att kryptering sker i ökad omfattning. När det gäller raderingsprogram så förekommer det i de undersökta datorerna, mobiltelefonerna m.m. Enligt uppgift från IT-forensiker sker det i sig i ökad utsträckning men inte så ofta med hjälp av särskild programvara för löpande radering. Vid tillslag inträffar dock att innan dator och beslag hunnit tas i beslag raderingsprogram används vilket medför att den raderade informationen inte kan återskapas.

Typfall

Här beskrivs kort några typfall av grov ekonomisk brottslighet där hemlig dataavläsning antagligen skulle kunnat ge värdefull information i förundersökningarna. De beskrivna typfallen anger exempel då krypteringen försvårat avlyssningen eller medfört att någon avlyssning inte kunnat genomföras eller det efter tillslag det inte gått att få information från de beslagtagna datorerna m.m. på grund av kryptering och/eller lösenordsskydd. Något typfall tar även upp den ytterligare information som skulle ha kunnat erhållas om vid en hemlig dataavläsning positionering varit möjlig eller att via datorns kamera visa vem som utfört vissa åtgärder.

A. I en förundersökning avseende grovt bokföringsbrott och grovt skattebrott (svart arbetskrafthärva) var en av de huvudmisstänkta medlem i ett s.k. MC-gäng. Vid avlyssningen konstaterades att viss kommunikation som antogs att de misstänkta ville hålla hemlig gick över Viber. Trafiken kunde på grund av kryptering inte avlyssnas men vid något/några tillfällen kunde bilder

ur datatrafiken lyftas ur avlyssningssystemet och analysers med annan mjukvara. Den möjligheten försvann dock när Viber gjorde om sin kryptering. Då även all e-post krypterades (SSL) kunde inte viktig information fås om den huvudmisstänkte vilket medförde att bl.a. en bostad inte gick att spåra där det antogs att viktig utredningsinformation fanns.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes mobiltelefon som skulle kunna ge information bl.a. om innehållet i kommunikationen innan den krypterades och om lagrad information. GPS-positionering av den misstänktes mobiltelefon skulle kunnat göra det möjligt att hitta den misstänktes bostad.

B. Sedan en förundersökning avseende grovt insiderbrott och grovt svindleri inletts erhölls tillstånd för HAK. Vid verkställighet av HAK pratar de misstänkta med varandra om alldagliga saker men också att de ibland säger att ”vi tar Skype”. Det kan starkt misstänkas att man då pratar om de misstänkta brotten. Eftersom Skype, liksom t.ex. Twitter, Viber och Facebook, är en krypterad tjänst, går det inte att få del av innehållet i kommunikationen.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes mobiltelefon som skulle kunnat ge information bl.a. om innehållet i kommunikationen innan den krypterades och om lagrad information.

C. I en förundersökning om grovt penningtvättbrott där misstänkt lånade ut sitt konto till ett svenskregistrerat bolag som handlade med guld med baltiska företrädare som inte betalade skatter och avgifter. Under två veckor överfördes 1,2 miljoner kr från bolaget via den misstänkte penningtvättaren och vidare till ett inaktivt bolag i Lettland. Försök gjordes att IP-spåra transaktionerna i syfte att bringa klarhet i om den misstänkte utförde transaktionerna eller om han bara hade lämnat över konto och inloggningsuppgifter till företrädaren för det svenska bolaget. Transaktionerna gjordes från en dator krypterad med VPN eller TOR, vilket medförde att IP-adresserna studsade mellan servrar i olika länder. Det gick inte heller att få fram vilken operatör som tillhandahållit IP-adressen från början.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som skulle kunnat ge information bl.a. om innehållet i kommunikationen innan den krypterades och om lagrad information samt om identiteten på den utrustning den misstänkte kommunicerar med (exempelvis användar-ID i en viss app, e-postadress m.m.).

D. I samband med en förundersökning avseende grovt bokföringsbrott och grovt skattebrott erhölls tillstånd till HAK. Vid verkställighet av HAK framkommer att en stor del av de misstänktas kommunikation, både med varandra och med andra, gick via krypterade sociala medietjänster. Efter tillslag så kontrollerades en beslagtagen dator. I datorn anträffades viss information som rörde försäljning av olja där den misstänkte verkade agera mellanhand i försäljningen. Digitala dokument anträffades som visade en anknytning till mellanöstern. Det kunde antas att dokumenten avsåg affärshändelser som inte bokförts eller deklarerats. På grund av den kryptering som fanns i datorn kunde inte ytterligare information tas fram från datorn.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som skulle kunnat ge information bl.a. om innehållet i kommunikationen innan den krypterades och om lagrad information.

E. Vid en förundersökning avseende grovt skattebrott och grovt bokföringsbrott köptes mobiltelefoner från annat land inom EU utan att någon mervärdesskatt deklarerades. Mobiltelefonerna såldes sedan till kunder i Sverige. Under förundersökningen användes HAK men enbart begränsade delar av kommunikationen kunde avlyssnas på grund av kryptering. Det framkom dock att ett möte skulle hållas på samma plats som tidigare i en stad i Sverige. Vid mötet skulle säljaren (okänd person) vara närvarande och det skulle diskuteras kommande affärer. Den del av den avlyssnade kommunikationen som kunde avlyssnas gav inte någon uppgift om när mötet skulle hållas.

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes mobiltelefon som skulle kunnat ge information bl.a. om innehållet i kommunikationen innan den krypterades och om lagrad information. GPS-positionering av den

misstänktes mobiltelefon skulle kunna gjort det möjligt att hitta mötesplatsen och genom att använda mobiltelefonens kamera skulle ha framkommit vilka som deltog i mötet och säljaren kunnat identifieras.

F. I ett punkskatteärende där HAK användes kunde på grund av kryptering inte kommunikationen avlyssnas. Vid tillslag beslagtogs hos den misstänkte datorer och lösa hårddiskar som innehöll vissa filer som var krypterade. Filerna kunde inte dekrypteras av IT-forensiker vid Ekobrottsmyndigheten. Efter att hjälp fåtts från experter så lyckades till slut vissa av de aktuella filerna dekrypteras. Det innehåll som dekrypterade bedömdes utgöra god bevisning i ärenden. Innehållet i de återstående filerna som inte kunde dekrypteras är oklart och det går inte att säga om de skulle ha påverkat bevisläget

Hemlig dataavläsning skulle ge möjlighet att installera ett tekniskt hjälpmedel i den misstänktes utrustning, som skulle ha kunnat i realtid löpande ge information bl.a. om innehållet i kommunikationen innan den krypterades.

Statens offentliga utredningar 2017

Kronologisk förteckning

1. För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. N.
2. Kraftsamling för framtidens energi. M.
3. Karens för statsråd och statssekreterare. Fi.
4. För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. S.
5. Svensk social trygghet i en globaliserad värld. Del 1 och 2. S.
6. Se barnet! Ju.
7. Straffprocessens ramar och domstolens beslutsunderlag i brottmål – en bättre hantering av stora mål. Ju.
8. Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. M.
9. Det handlar om oss. – unga som varken arbetar eller studerar. U.
10. Ny ordning för att främja god sed och hantera oredlighet i forskning. U.
11. Vägskatt. Volym 1 och 2. Fi.
12. Att ta emot människor på flykt. Sverige hösten 2015. Ju.
13. Finansiering av infrastruktur med privat kapital? Fi.
14. Migrationsärenden vid utlandsmyndigheterna. Ju.
15. Kvalitet och säkerhet på apoteksmarknaden. S.
16. Sverige i Afghanistan 2002–2014. UD.
17. Om oskuldspresumtionen och rätten att närvara vid rättegången. Genomförande av EU:s oskuldspresumtionsdirektiv. Ju.
18. En nationell strategi för validering. U.
19. Uppdrag: Samverkan. Steg på vägen mot fördjupad lokal samverkan för unga arbetslösa. A.
20. Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. U.
21. Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. S.
22. Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. M.
23. digitalforvaltning.nu. Fi.
24. Ett arbetsliv i förändring – hur påverkas ansvaret för arbetsmiljön? A.
25. Samlad kunskap – stärkt handläggning. S.
26. Delningsekonomi. På användarnas villkor. Fi.
27. Vissa frågor inom fastighets- och stämpelskatteområdet. Fi.
28. Ett nationellt centrum för kunskap om och utvärdering av arbetsmiljö. A.
29. Brottsdatalag. Ju.
30. En omreglerad spelmarknad. Del 1 och 2. Fi.
31. Stärkt konsumentskydd på bostadsrättsmarknaden. Ju.
32. Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. M.
33. Stärkt ställning för hyresgäster. Ju.
34. Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. M.
35. Samling för skolan. Nationell strategi för kunskap och likvärdighet. U.
36. Informationssäkerhet för samhällsviktiga och digitala tjänster. Ju.
37. Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra. Ju.

38. Kvalitet i välfärden – bättre upphandling och uppföljning. Fi.
39. Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. Ju.
40. För dig och för alla. S.
41. Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd. Ju.
42. Vem har ansvaret? M.
43. På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. S.
44. Entreprenad, fjärrundervisning och distansundervisning. U.
45. Ny lag om företagshemligheter. Ju.
46. Stärkt ordning och säkerhet i domstol. Ju.
47. Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. S.
48. Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. S.
49. EU:s dataskyddsförordning och utbildningsområdet. U.
50. Personuppgiftsbehandling för forskningsändamål. U.
51. Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. U.
52. Så stärker vi den personliga integriteten. Ju.
53. God och nära vård. En gemensam färdplan och målbild. S.
54. Fler nyanlända elever ska uppnå behörighet till gymnasiet. U.
55. En ny kamerabevakningslag. Ju.
56. Jakten på den perfekta ersättningsmodellen. Vad händer med medarbetarnas handlingsutrymme? Fi.
57. Lag om flygpassageraruppgifter i brottsbekämpningen. Ju.
58. Amerikansk inresekontroll vid utresa från Sverige – så kan avtalen genomföras. Ju.
59. Reglering av alkoglass m.fl. produkter. S.
60. Nästa steg? Förslag för en stärkt minoritetspolitik. Ku.
61. Villkorlig frigivning – förstärkta åtgärder mot återfall i brott. Ju.
62. Kärnavfallsrådets yttrande över SKB:s Fud-program 2016. M.
63. Miljötillsyn och sanktioner – en tillsyn präglad av ansvar, respekt och enkelhet. M.
64. Detaljplanekravet. N.
65. Hyran vid nyproduktion – en utvärdering och utveckling av modellen med presumtionshyra. Ju.
66. Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning. S.
67. Våldsbejakande extremism. En forskarantologi. Ku.
68. Barnets rättigheter i ett straffrättsligt förfarande m.m. Genomförande av EU:s barnrättsdirektiv och två andra straffprocessuella frågor. Ju.
69. Marknadskontrollmyndigheter – befogenheter och sanktionsmöjligheter. UD.
70. Förstärkt skydd för uppgifter av betydelse för ett internationellt samarbete för fred och säkerhet som Sverige deltar i. Ju.
71. Bostäder på statens mark – en möjlighet? N.
72. Genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism. Ju.
73. En gemensam bild av bostadsbyggnadsbehovet. N.
74. Brottsdatalag – kompletterande lagstiftning. Ju.
75. Datalagring – brottsbekämpning och integritet. Ju.
76. Enhetliga priser på receptbelagda läkemedel. S.
77. En generell rätt till kommunal avtalssamverkan. Fi.
78. En sammanhållen budgetprocess. Fi.
79. Finansiering av public service – för ökad stabilitet, legitimitet och stärkt oberoende. Ku.

80. Stärkt integritet i Rättsmedicinalverkets verksamhet. Ju.
81. Rättslig översyn av skogsvårdslagstiftningen. N.
82. Vägledning för framtidens arbetsmarknad. A.
83. Brännheta skatter! Bör avfallsförbränning och utsläpp av kväveoxider från energiproduktion beskattas? Fi.
84. Uppehållstillstånd på grund av praktiska verkställighetshinder och preskription. Ju.
85. Rekrytering av framtidens domare. Ju.
86. Hyresmarknad utan svarthandel och otillåten andrahandsuthyrning. Ju.
87. Finansiering, subvention och prissättning av läkemedel – en balansakt. S.
88. Nästa steg? Del 2. Förslag för en stärkt minoritetspolitik. Ku
89. Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet. Ju.

Statens offentliga utredningar 2017

Systematisk förteckning

Förstärkt skydd för uppgifter av betydelse för ett internationellt samarbete för fred och säkerhet som Sverige deltar i. [70]

Genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism. [72]

Brottsdatalag – kompletterande lagstiftning. [74]

Datalagring – brottsbekämpning och integritet. [75]

Stärkt integritet i Rättsmedicinalverkets verksamhet. [80]

Uppehållstillstånd på grund av praktiska verkställighetshinder och preskription. [84]

Rekrytering av framtidens domare. [85]

Hyresmarknad utan svarthandel och otillåten andrahandsuthyrning. [86]

Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet. [89]

Kulturdepartementet

Nästa steg? Förslag för en stärkt minoritetspolitik. [60]

Våldsbejakande extremism. En forskarantologi. [67]

Finansiering av public service – för ökad stabilitet, legitimitet och stärkt oberoende. [79]

Nästa steg? Del 2. Förslag för en stärkt minoritetspolitik. [88]

Miljö- och energidepartementet

Kraftsamling för framtidens energi. [2]

Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. [8]

Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. [22]

Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. [32]

Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. [34]

Vem har ansvaret? [42]

Kärnavfallsrådets yttrande över SKB:s Fud-program 2016. [62]

Miljötillsyn och sanktioner – en tillsyn präglad av ansvar, respekt och enkelhet. [63]

Näringsdepartementet

För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. [1]

Detaljplanekravet. [64]

Bostäder på statens mark – en möjlighet? [71]

En gemensam bild av bostadsbyggnadsbehovet. [73]

Rättslig översyn av skogsvårdslagstiftningen. [81]

Socialdepartementet

För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. [4]

Svensk social trygghet i en globaliserad värld. Del 1 och 2. [5]

Kvalitet och säkerhet på apoteksmarknaden. [15]

Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. [21]

Samlad kunskap – stärkt handläggning. [25]

För dig och för alla. [40]

På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. [43]

Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. [47]

Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. [48]

God och nära vård. En gemensam färdplan och målbild. [53]

Utbildningsdepartementet

Utrikesdepartementet