Utökade möjligheter att använda hemliga tvångsmedel

Delbetänkande av Utredningen om utökade möjligheter att använda hemliga tvångsmedel

Stockholm 2022

STATENS OFFENTLIGA UTREDNINGAR

SOU 2022:19

SOU och Ds finns på regeringen.se under Rättsliga dokument.

Svara på remiss – hur och varför
Statsrådsberedningen, SB PM 2003:2 (reviderad 2009-05-02).
Information för dem som ska svara på remiss finns tillgänglig på regeringen.se/remisser.

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck och remisshantering: Elanders Sverige AB, Stockholm 2021

ISBN 978-91-525-0364-5 (tryck)
ISBN 978-91-525-0365-2 (pdf)
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 14 oktober 2020 att tillkalla en särskild utredare med uppdraget att se över delar av regleringen om hemliga tvångsmedel (dir. 2020:104). Till särskild utredare förordnades samma dag f.d. generaldirektören Barbro Thorblad. Den 17 mars 2022 beslutade regeringen om tilläggsdirektiv (dir. 2022:13). Enligt tilläggsdirektiven ska den särskilda utredaren se över ytterligare några frågor rörande hemliga tvångsmedel. Den del av uppdraget som omfattas av de ursprungliga direktiven ska, med undantag för frågan om det bör vara möjligt att använda hemlig övervakning av elektronisk kommunikation i syfte att lokalisera en skäligen misstänkt, redovisas i ett delbetänkande. Uppdraget enligt tilläggsdirektiven ska slutredovisas senast den 14 oktober 2022.

Rättssakkunniga Karolina Helling förordnades som sakkunnig att biträda utredningen från och med den 4 november 2020. Som experter förordnades från och med samma dag advokaten Anna Björklund (Advokatsamfundet), seniora kammaråklagaren Anna Broman Olasdotter (Ekobrottsmyndigheten), numera hovrättsrådet Nathalie Dahlén (Hovrätten över Skåne och Blekinge), kriminalkommissarien Roger Engström (Polismyndigheten), verksjuristen Daniel Gottberg (Tullverket), seniora kammaråklagaren Hans Harding (Malmö åklagarkammare), verksjuristen Carl Rundström (Säkerhetspolisen) och seniora föredraganden Johanna Rådberg (Säkerhets- och integritetsskyddsnämnden). Hovrättsassessorn Johanna Kallifatides har varit utredningens sekreterare.

Roger Engström entledigades den 13 januari 2022 och ersattes av verksamhetsutvecklaren Pär Runemar (Polismyndigheten). Johanna Rådberg entledigades den 4 februari 2022 och ersattes av enhetschefen Cecilia Agnehall (Säkerhets- och integritetsskyddsnämnden).

Vi överlämnar härmed delbetänkandet *Utökade möjligheter att använda hemliga tvångsmedel* (SOU 2022:19). Arbetet har bedrivits i nära samarbete med den sakkunniga och experterna. Betänkandet är därför skrivet i vi-form. Detta hindrar inte att det kan finnas skilda uppfattningar i enskilda frågor.

Arbetet fortsätter i enlighet med tilläggsdirektiven.

Stockholm i april 2022

Barbro Thorblad

/Johanna Kallifatides

Innehåll

Förkortningar

a.a.	anfört arbete
BrB	Brottsbalken (1962:799)
Brå	Brottsförebyggande rådet
f.	följande sida
ff.	följande sidor
inhämtningslagen	lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet
LEK	Lagen (2003:389) om elektronisk kommunikation
LIRB	lagen (2000:562) om internationell rättslig hjälp i brottmål
LSU	lagen (1991:572) om särskild utlänningskontroll
preventivlagen	lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott
RB	Rättegångsbalken (1942:740)
SIN	Säkerhets- och integritetsskyddsnämnden

Sammanfattning

Vårt uppdrag

Utredningens uppdrag har varit att se över delar av regleringen om hemliga tvångsmedel. Syftet med översynen har varit att ta ställning till hur hemliga tvångsmedel ska kunna användas i en större utsträckning för att bekämpa allvarlig brottslighet. Det har ingått i uppdraget att noga väga behovet av en effektiv brottsbekämpning mot den enskildes rätt till skydd för sin personliga integritet. Det har ålegat oss att göra en sådan avvägning för varje förslag för sig och även när det gäller förslagen sammantaget. Vidare framgår av direktiven ett krav på att förslagen uppfyller högt ställda krav på rättssäkerhet.

I uppdraget har ingått att

- ta ställning till om det bör införas en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning vid misstanke om flera brott vars samlade straffvärde kan antas överstiga ett visst straff,
- ta ställning till i vilka situationer och vid vilka straffvärden en sådan möjlighet bör kunna tillämpas,
- ta ställning till om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation bör få användas vid fler brott,
- ta ställning till om det bör vara tillåtet med hemlig övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet och i så fall i vilka situationer,
- ta ställning till om tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning bör kunna knytas till en person,

- ta ställning till om åklagare bör få möjlighet att fatta interimistiska beslut om hemlig rumsavlyssning inklusive tillträde för att installera utrustningen,
- ta ställning till om den verkställande myndigheten bör kunna få tillstånd att i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång för att verkställa ett beslut om enbart hemlig kameraövervakning,
- ta ställning till om åklagare bör få möjlighet att interimistiskt besluta om sådant tillträde,
- ta ställning till om en straffvärdeventil bör införas i inhämtningslagen,
- ta ställning till om skyddet för den personliga integriteten bör stärkas, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Det har ålegat oss att säkerställa att en välfungerande systematik i regelverket om hemliga tvångsmedel upprätthålls och att överväga behovet av och lämna förslag till behövliga följdändringar.

Den 1 april 2020 trädde lagen om hemlig dataavläsning i kraft. Därigenom infördes hemlig dataavläsning som ett nytt hemligt tvångsmedel. Tvångsmedlet kan användas för att genom avlyssning eller avläsning av ett avläsningsbart informationssystem få tillgång till motsvarande slags uppgifter som man kan få tillgång till genom de övriga hemliga tvångsmedlen. Hemlig dataavläsning omfattar även två nya uppgiftstyper, som inte motsvaras av de tidigare hemliga tvångsmedlen. Hemlig dataavläsning bör som utgångspunkt kunna användas i motsvarande fall som de befintliga hemliga tvångsmedlen, eftersom det annars finns en risk för att vissa allvarliga brott inte kan utredas när det visar sig vara omöjligt att använda befintliga hemliga tvångsmedel (jfr prop. 2019/20:64 s. 124). Med hänsyn till detta och av systematiska skäl omfattar våra överväganden genomgående även hemlig dataavläsning.

Straffvärdeventiler för viss flerfaldig brottslighet

Bestämmelserna om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning innehåller en s.k. straffvärdeventil. Enligt ventilen får respektive tvångsmedel användas under en förundersökning avseende misstanke om ett konkret brott vars straffvärde kan antas överstiga fängelse i två år. För hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter krävs att straffvärdet kan antas överstiga fyra års fängelse och att det dessutom är fråga om ett brott som räknas upp i en särskild brottskatalog. Det är inte möjligt att använda tvångsmedlen vid misstanke om flera brott där det sammanlagda straffvärdet kan antas vara högt, men där de ingående enskilda brotten inte har ett straffvärde på den nivå som krävs.

Vi föreslår att det införs straffvärdeventiler som gör det möjligt att i vissa situationer beakta en flerfaldig brottslighets samlade straffvärde vid bedömning av om det hemliga tvångsmedlet ska få användas. Möjligheten föreslås kunna tillämpas i förundersökningar om flerfaldig brottslighet som kan antas ha utövats i organiserad form eller systematiskt. Varje brott som inräknas ska kunna antas vara ett led i den organiserade eller systematiska brottsligheten. Vi föreslår att det samlade straffvärdet ska kunna antas överstiga fängelse i två år och att endast häktningsgrundande brott och försök, förberedelse eller stämpling till häktningsgrundande brott ska få inräknas. För hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter föreslår vi emellertid att det samlade straffvärdet ska kunna antas överstiga fängelse i fyra år och att endast brott med lägst sex månaders minimistraff och försök, förberedelse eller stämpling till sådana brott ska få inräknas. Det ska inte krävas att brotten ingår i någon brottskatalog för att straffvärdeventilerna ska kunna tillämpas. Vi föreslår vidare att brottskatalogen i den nuvarande straffvärdeventilen för hemlig rumsavlyssning avskaffas.

Förslaget avseende hemlig avlyssning av elektronisk kommunikation innebär att även möjligheten att använda hemlig övervakning av elektronisk kommunikation utvidgas.

En tydligare koppling mellan hemlig avlyssning och hemlig övervakning av elektronisk kommunikation

Vi föreslår en bestämmelse som innebär att alla brott och all brottslighet som kan leda till hemlig avlyssning av elektronisk kommunikation även ska kunna leda till hemlig övervakning av sådan kommunikation. Härigenom klargörs det att ett beslut om hemlig övervakning alltid kan fattas i fråga om sådana brott och sådan brottslighet oberoende av om det samtidigt fattas ett beslut om hemlig avlyssning.

Brottskatalogerna utvidgas

Vissa brottstyper som i dagsläget sällan eller aldrig kan leda till hemliga tvångsmedel är särskilt svårutredda. Ett skäl kan vara att det är vanligt att målsägande och vittnen inte vill eller vågar lämna upplysningar till de brottsbekämpande myndigheterna. Detta kan ha ett samband med s.k. tystnadskulturer. Exempel på sådana brott, som samtidigt kan vara systemhotande, är mened och övergrepp i rättssak. I andra fall kan de kriminellas användning av modern teknik göra det mycket svårt för de brottsbekämpande myndigheterna att ens identifiera en skäligen misstänkt för brott som kan vara systemhotande eller i övrigt särskilt angelägna att bekämpa. Exempel på detta är komplex cyberbrottslighet såsom ransomwareattacker och internetrelaterad sexualbrottslighet mot barn och barnpornografi. Det finns ett påtagligt behov av utökade möjligheter att använda hemliga tvångsmedel vid brottslighet av det angivna slaget.

Vi föreslår att det införs en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning, förutom sådan dataavläsning som gäller rumsavlyssningsuppgifter, vid förundersökningar om grovt dataintrång, sexualbrott mot barn och barnpornografibrott, utpressning och grov utpressning, mened, övergrepp i rättssak, grovt jaktbrott och grovt insiderbrott.

En möjlighet att inhämta uppgifter om meddelanden i realtid

När hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning används i syfte att utreda vem som skäligen kan misstänkas för brottet, får uppgifter om meddelanden endast avse förfluten tid. Det har framkommit att det numera finns ett påtagligt behov av en möjlighet att i dessa fall kunna inhämta uppgifter om meddelanden även i realtid, t.ex. i utredningar om komplex cyberbrottslighet. Vi föreslår att det ska vara tillåtet att hämta in uppgifter om meddelanden i realtid vid hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet. Motsvarande ändring föreslås i lagen om hemlig dataavläsning.

Hemlig övervakning av elektronisk kommunikation avseende målsäganden

Hemlig övervakning av elektronisk kommunikation får användas i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Lagtexten innehåller inga begränsningar i fråga om vem tvångsmedlet får riktas mot och det förekommer att hemlig övervakning av elektronisk kommunikation riktas mot en målsägande. Säkerhets- och integritetsskyddsnämnden har ifrågasatt om det är rimligt att brottsbekämpande myndigheters intresse av övervakningsuppgifter tillåts urholka målsägandens integritetsskydd på detta sätt utan uttryckligt lagstöd (dnr 132-2018). Samma slags uppgifter kan hämtas in genom hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet.

Vi har gjort bedömningen att det även i fortsättningen bör vara möjligt att rikta hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsövervaknings- och platsuppgifter mot målsäganden och att det inte krävs några författningsändringar.

Nya möjligheter att utreda vem som skäligen kan misstänkas

Det finns inte någon möjlighet att använda hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet. Det finns dock ett antal situationer där det finns ett behov av en sådan möjlighet för att man ska kunna komma framåt i utredningen om ett allvarligt brott. Det handlar bl.a. om fall där utredningen ger vid handen att någon person som döljer sig bakom ett visst telefonnummer eller en viss elektronisk adress eller kommunikationsutrustning gör sig skyldig till allvarlig brottslighet, men att det är okänt vem personen är. Ett annat exempel kan vara mordfall där det finns anledning att anta att målsäganden och gärningspersonen varit i kontakt med varandra före mordet och det är av stor vikt att man kan ta del av denna kommunikation.

Vi bedömer att behovet av en möjlighet att använda de aktuella tvångsmedlen är så stort att det överväger nackdelarna från integritetssynpunkt, inkluderat den ökade risken för att personer som sedan visar sig vara ovidkommande för utredningen drabbas av tvångsmedlet. Vi föreslår därför införande av en sådan möjlighet. Bedömningen förutsätter dock att användningsområdet görs betydligt snävare än vad som i övrigt gäller för respektive tvångsmedel. Vi föreslår därför att huvudregeln ska vara att brottet eller den samlade brottsligheten är sådan att hemlig rumsavlyssning kan förekomma. För att tillämpningsområdet inte ska bli alltför snävt föreslår vi dock att tvångsmedlen även ska kunna användas i det nya syftet vid utredning om vissa andra brott eller flerfaldig brottslighet där det föreligger ett särskilt påtagligt behov av en sådan möjlighet. Dessa andra brott ska räknas upp i en särskild brottskatalog.

Hemlig rumsavlyssning och hemlig kameraövervakning kan knytas till en person

Tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning måste enligt dagens regler alltid knytas till en viss plats. Åklagarmyndigheten har väckt frågan om tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning ska få knytas till en person. Bakgrunden

är bl.a. att kriminella är riskmedvetna och i hög grad undviker att ha viktiga samtal i bostaden och andra miljöer där de vet att det finns en risk för hemlig rumsavlyssning. Vidare vet man många gånger inte i förväg var ett för brottsutredningen viktigt möte kommer att äga rum. Det är också vanligt att personen är i rörelse utomhus och att det därför inte kan anges en specifik plats. Det förekommer även att man behöver kunna avlyssna eller kameraövervaka den misstänkte på en plats där spanare inte kan röra sig utan stor risk för upptäckt, såsom ödsliga platser och vissa områden som kriminella grupperingar bevakar. Det är vanligt att åklagare avstår från att ansöka om tillstånd eftersom man har inte har möjlighet att ange en viss plats. Det förekommer dock även att domstolar ger tillstånd till hemlig rumsavlyssning eller hemlig kameraövervakning som avser mycket brett angivna platser.

Vi bedömer att det finns ett behov av en möjlighet att i vissa fall knyta tillståndet till en hemlig rumsavlyssning eller hemlig kameraövervakning till den skäligen misstänkte i stället för till en viss plats. Vi anser vidare att en sådan möjlighet är godtagbar under förutsättning att den endast får användas om det finns särskilda skäl och att det ställs krav på att tillståndet alltid förenas med villkor som syftar till att minimera onödiga integritetsintrång för enskilda. Vi föreslår därför att en sådan möjlighet införs. Det bör ankomma på åklagaren att i samband med ansökan lämna förslag till villkor. Vi föreslår vidare ett antal begränsningar gällande verkställigheten, bl.a. i fråga om var den tekniska utrustningen som används får vara placerad.

I huvudsak motsvarande förslag lämnas angående hemlig dataavläsning som gäller rumsavlyssnings- och kameraövervakningsuppgifter.

En möjlighet till interimistiska åklagarbeslut om hemlig rumsavlyssning

Åklagare har möjlighet att i brådskande fall fatta beslut om hemliga tvångsmedel i avvaktan på rättens prövning. Någon sådan möjlighet finns emellertid inte när det gäller hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter. Detta ställer till problem i ärenden där det krävs snabba beslut, inte minst när behovet uppstår utanför domstolarnas öppettider, men även i vissa andra brådskande fall. Åklagare föreslås därför få fatta interimistiskt beslut

om hemlig rumsavlyssning och tillträdestillstånd för installation av utrustning för hemlig rumsavlyssning, om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd. Åklagare föreslås även få möjlighet att, på motsvarande villkor, fatta interimistiskt beslut om hemlig dataavläsning som gäller rumsavlyssningsuppgifter och tillträdestillstånd för installation av tekniska hjälpmedel i syfte att inhämta sådana uppgifter.

Tillträdestillstånd för enbart hemlig kameraövervakning

Ett tillträdestillstånd i syfte att installera kamerautrustning på en plats som annars skyddas mot intrång kan endast ges om det samtidigt ska verkställas ett beslut om hemlig rumsavlyssning. Det är dock vanligt att hemlig kameraövervakning behövs och är tillåten i ett ärende där det inte finns behov av eller förutsättningar för hemlig rumsavlyssning. I praktiken löser de brottsbekämpande myndigheterna ofta detta genom att man inhämtar samtycke från den som förfogar över platsen. Det finns dock fall där detta inte är möjligt eller lämpligt, t.ex. för att den som kan lämna samtycke är misstänkt för inblandning i brottsligheten.

Vi föreslår införande av en möjlighet att besluta om tillträdestillstånd för installation av kamerautrustning utan något krav på att även hemlig rumsavlyssning ska ske, och att åklagare ska kunna fatta sådana beslut interimistiskt om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd.

Det bör inte införas en straffvärdeventil i inhämtningslagen

Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) reglerar de brottsbekämpande myndigheternas möjligheter att i underrättelseverksamhet hämta in uppgifter om elektronisk kommunikation. Tillstånd till sådan inhämtning kan ges antingen för brott för vilket det inte är föreskrivet lindrigare straff än fängelse två år eller för vissa särskilt angivna samhällsfarliga brott. Lagen innehåller inte någon straffvärdeventil. Regleringen innebär att Ekobrottsmyndigheten inte har någon möjlighet att i sin under-

rättelseverksamhet inhämta uppgifter med stöd av inhämtningslagen, eftersom myndigheten inte handlägger något brott med lägst två års minimistraff. Ekobrottsmyndigheten har angett att det finns ett behov av en sådan möjlighet. Även Polismyndigheten och Tullverket har angett att det finns ett behov av en sådan möjlighet i fråga om vissa brott som i dag inte omfattas av lagen.

Vi har gjort bedömningen att någon straffvärdeventil inte bör införas med hänsyn till de svårigheter som föreligger att redan på underrättelsestadiet kunna göra ens en någorlunda rimlig bedömning av straffvärdet.

Våra förslag och den personliga integriteten

Våra förslag innebär vissa ökade integritetsrisker. Samtidigt bedöms förslagen leda till förbättrade möjligheter att utreda allvarlig brottslighet mot enskilda och att avbryta pågående sådan brottslighet. I detta avseende innebär förslagen ett förstärkt skydd för enskildas personliga integritet.

Våra sammantagna förslag bedöms ge uttryck för en rimlig avvägning av behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet. Det finns enligt vår mening inte något behov av ytterligare rättssäkerhetsgarantier. Vi vill dock framhålla vikten av en effektiv tillsyn.

Följdändringar

Våra förslag föranleder vissa följdändringar i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m., lagen (2000:562) om internationell rättslig hjälp i brottmål och lagen (2017:1000) om en europeisk utredningsorder.

Ikraftträdande

Lagändringarna föreslås träda i kraft den 1 januari 2024. Det finns inte behov av några övergångsbestämmelser.

Konsekvenser

Det är synnerligen svårt att beräkna vilket resursbehov som våra förslag kan antas medföra. Det framstår emellertid som uppenbart att ökade resursbehov som inte ryms inom befintlig anslagsram kommer att uppstå hos Polismyndigheten, Åklagarmyndigheten, Ekobrottsmyndigheten, Tullverket och Säkerhets- och integritetsskyddsnämnden. Ett genomförande av våra förslag kräver att det tillskjuts medel till rättsväsendet från andra utgiftsområden.

De ökade resursbehov som kan förväntas uppkomma inom Säkerhetspolisen respektive Sveriges domstolar torde rymmas inom ram.

Förslagen kommer att bidra till att fler brott kommer att kunna utredas och till effektivare utredningar. Därigenom kommer fler personer att kunna lagföras för brott. Detta förväntas bidra till att färre brott begås. Förslagen bedöms vidare ge bättre förutsättningar för internationellt rättsligt samarbete, inte minst när det gäller cyberbrott.

Tilläggsdirektiv

Den 17 mars 2022 beslutade regeringen om tilläggsdirektiv (dir. 2022:13). Arbetet fortsätter i enlighet med tilläggsdirektiven. Dessa innebär bl.a. att en av de frågor som omfattas av de ursprungliga direktiven, nämligen frågan om det bör vara möjligt att använda hemlig övervakning av elektronisk kommunikation i syfte att lokalisera en skäligen misstänkt, i stället ska behandlas i slutbetänkandet. Uppdraget ska slutredovisas senast den 14 oktober 2022.

1 Författningsförslag

1.1 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs i fråga om rättegångsbalken

dels att 27 kap. 18–20 b, 20 d–21 a och 25 a §§ ska ha följande lydelse,

dels att det i balken ska införas tre nya paragrafer, 27 kap. 18 a, 19 a och 20 f §§, av följande lydelse.

Lydelse enligt prop. 2021/22:133	*Föreslagen lydelse*
27 kap.	
18 §	
Hemlig avlyssning av elektronisk kommunikation innebär att meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet.	
Hemlig avlyssning av elektronisk kommunikation får användas vid en förundersökning om	Hemlig avlyssning av elektronisk kommunikation får, *om inte något annat anges i 18 a §*, användas vid en förundersökning om
1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,	
	2. grovt dataintrång enligt 4 kap. 9 c § brottsbalken,
	3. sexuellt utnyttjande av barn, sexuellt övergrepp mot barn, grovt sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering, grovt utnyttjande av barn för sexuell posering, utnyttjande av barn ge-

	nom köp av sexuell handling, sexuellt ofredande eller kontakt för att träffa ett barn i sexuellt syfte enligt 6 kap. 5, 6, 8, 9, 10 § första stycket eller 10 a § brottsbalken,
	4. utpressning som inte är att anse som ringa eller grov utpressning enligt 9 kap. 4 § brottsbalken,
2. sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken,	*5.* 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,	*6.* 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,
	7. mened enligt 15 kap. 1 § brottsbalken som inte är att anse som ringa,
	8. barnpornografibrott som inte är ringa eller grovt barnpornografibrott enligt 16 kap. 10 a § brottsbalken,
	9. övergrepp i rättssak enligt 17 kap. 10 § brottsbalken som inte är att anse som ringa,
4. uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,	*10.* uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken,
5. högförräderi, krigsanstiftan, spioneri, grovt spioneri, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet mot Sverige,	*11.* högförräderi, krigsanstiftan, spioneri, grovt spioneri, 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,	mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6, 7, 8, 10, 10 a eller 10 b § brottsbalken,
	12. grovt jaktbrott enligt 44 § jaktlagen (1987:259),
	13. grovt insiderbrott enligt 2 kap. 1 § tredje stycket lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden,
6. företagsspionieri enligt 26 § lagen (2018:558) om 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,	*14.* företagsspionieri enligt 26 § lagen (2018:558) om 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, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:000),	*15.* terroristbrott, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet eller resa för terrorism eller särskilt allvarlig brottslighet enligt 4, 5, 6, 7, 8, 9 eller 10 § terroristbrottslagen (2022:000),
8. försök, förberedelse eller stämpling till brott som avses i 1–*7*, om en sådan gärning är belagd med straff, *eller*	*16.* försök, förberedelse eller stämpling till brott som avses i 1–*15*, 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.	*17.* annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år, *eller* *18. annan brottslighet som kan antas ha utövats i organiserad form eller systematiskt om det med hänsyn till omständigheterna kan antas att den samlade brottslighetens straffvärde överstiger fängelse i två år. I sammanläggningen får det endast ingå brott som kan antas utgöra ett led i denna brottslighet och för vilka det är föreskrivet fängelse i ett år eller däröver eller försök, förberedelse eller stämpling till ett sådant brott, om en sådan gärning är belagd med straff.*

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

Nuvarande lydelse	*Föreslagen lydelse*
	18 a § *I fall som avses i 20 § tredje stycket får hemlig avlyssning av elektronisk kommunikation användas endast vid en förundersökning om* *1. brott eller brottslighet som kan leda till hemlig rumsavlyssning enligt 20 d § andra stycket,* *2. brott som avses i 18 § andra stycket 2–6, 8, 10, 11, 14 eller 15,* *3. våldtäkt eller våldtäkt mot barn enligt 6 kap. 1 § första stycket eller 4 § första eller andra stycket brottsbalken,*

4. allmänfarlig ödeläggelse enligt 13 kap. 3 § första stycket brottsbalken,

5. grovt narkotikabrott enligt 3 § första stycket narkotikastrafflagen (1968:64),

6. grovt vapenbrott enligt 9 kap. 1 a § första stycket vapenlagen (1996:67),

7. grov narkotikasmuggling, grov vapensmuggling eller grov smuggling av explosiv vara enligt 6 § tredje stycket, 6 a § tredje stycket eller 6 b § tredje stycket lagen (2000:1225) om straff för smuggling,

8. grovt brott enligt 29 a § första stycket lagen (2010:1011) om brandfarliga och explosiva varor, eller

9. försök, förberedelse eller stämpling till brott som avses i 2–8, om en sådan gärning är belagd med straff.

Om brottet eller brottsligheten är sådan som avses i 18 § andra stycket 17 eller 18 får hemlig avlyssning av elektronisk kommunikation enligt 20 § tredje stycket användas även vid en förundersökning om

1. grovt sexuellt övergrepp enligt 6 kap. 2 § andra stycket brottsbalken,

2. grovt bedrägeri enligt 9 kap. 3 § brottsbalken som begåtts med hjälp av elektronisk kommunikation,

3. grovt penningtvättsbrott eller näringspenningtvätt, grovt brott enligt 5 eller 7 § andra stycket lagen (2014:307) om straff för penningtvättsbrott, eller

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

Lydelse enligt prop. 2021/22:119	*Föreslagen lydelse*
19 §	
Hemlig övervakning av elektronisk kommunikation innebär att uppgifter i hemlighet hämtas in om	
1. meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress,	
2. vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller	
3. i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.	
Genom hemlig övervakning av elektronisk kommunikation får sådana meddelanden som avses i första stycket 1 även hindras från att nå fram.	
Hemlig övervakning av elektronisk kommunikation får användas vid en förundersökning om	Hemlig övervakning av elektronisk kommunikation får, *om inte något annat anges i 19 a §*, användas vid en förundersökning om
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), narkotikasmuggling enligt 6 § första stycket lagen (2000:1225) om straff för smuggling,	2. dataintrång enligt 4 kap. 9 c § brottsbalken, narkotikabrott enligt 1 § narkotikastrafflagen (1968:64), narkotikasmuggling enligt 6 § första stycket lagen (2000:1225) om straff för smuggling,
3. brott som avses i 18 § andra stycket 2–7, eller	3. brott *eller brottslighet* som avses i 18 § andra stycket 2–*18*, eller

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

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

Nuvarande lydelse	*Föreslagen lydelse*
	19 a § *I fall som avses i 20 § andra stycket får hemlig övervakning av elektronisk kommunikation användas endast vid en förundersökning som avser brott eller brottslighet som kan leda till hemlig avlyssning av elektronisk kommunikation enligt 18 § andra stycket.*
20 §[1]	
Hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation får, om inte annat följer av andra stycket, endast ske om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får endast avse	Hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation får, om inte annat följer av andra *eller tredje* stycket, endast ske om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Åtgärden får endast avse

[1] Senaste lydelse 2012:281.

1. ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte, eller

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

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

Hemlig övervakning av elektronisk kommunikation får, utöver vad som anges i första stycket, ske i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen.

Hemlig avlyssning av elektronisk kommunikation får, utöver vad som anges i första stycket, ske i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Åtgärden får då endast avse

1. ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som under den tid som tillståndet avser kan antas innehas eller ha innehafts av någon som kan misstänkas ha begått eller annars medverkat till brottet eller annars kan antas ha använts eller kan komma att användas av en sådan person, eller

2. ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att

någon som kan misstänkas ha begått eller annars medverkat till brottet har kontaktat eller kommer att kontakta under den tid som tillståndet avser.

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

Lydelse enligt prop. 2021/22:119 *Föreslagen lydelse*

20 a §

Hemlig kameraövervakning innebär att fjärrstyrda tv-kameror, andra optisk-elektroniska instrument eller därmed jämförbara utrustningar används för optisk personövervakning vid förundersökning i brottmål, utan att upplysning om övervakningen lämnas.

Hemlig kameraövervakning får användas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,

2. brott som avses i 18 § andra stycket 2–*7*,

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

4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år.

2. brott som avses i 18 § andra stycket 2–*15*,

3. försök, förberedelse eller stämpling till brott som avses i 1 eller 2, 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, *eller*

5. annan brottslighet som kan antas ha utövats i organiserad form eller systematiskt om det med hänsyn till omständigheterna kan antas att den samlade brottslighetens straffvärde överstiger fängelse i två år. I sammanläggningen får det en-

dast ingå brott som kan antas utgöra ett led i denna brottslighet och för vilka det är föreskrivet fängelse i ett år eller däröver, eller försök, förberedelse eller stämpling till ett sådant brott, om en sådan gärning är belagd med straff.

Nuvarande lydelse	*Föreslagen lydelse*
20 b §[2]	
Hemlig kameraövervakning får, utom i fall som avses i 20 c §, användas endast om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen.	
Åtgärden får, utom i fall som avses i 20 c §, avse endast en sådan plats där den misstänkte kan antas komma att uppehålla sig.	Åtgärden får, utom i fall som avses i *tredje stycket eller* 20 c §, avse endast en sådan plats där den misstänkte kan antas komma att uppehålla sig.
	Om det finns särskilda skäl får ett beslut om hemlig kameraövervakning avse den skäligen misstänkte i stället för en viss plats. Beslutet får då verkställas endast på så sätt att övervakningen riktas mot en plats där det kan antas att den misstänkte kommer att uppehålla sig. De tekniska hjälpmedel som används får inte placeras på en plats som skyddas mot intrång.

[2] Senaste lydelse 2008:855.

20 d §[3]

Med hemlig rumsavlyssning avses avlyssning eller upptagning som

1. görs i hemlighet och med ett tekniskt hjälpmedel som är avsett att återge ljud, och

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

Hemlig rumsavlyssning får användas vid en förundersökning om

1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i fyra år,

2. spionerі enligt 19 kap. 5 § brottsbalken,

3. brott som avses i 26 § lagen (2018:558) om 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) grov människoexploatering enligt 4 kap. 1 b § tredje stycket brottsbalken,

c) våldtäkt enligt 6 kap. 1 § första stycket brottsbalken,

d) grovt sexuellt övergrepp enligt 6 kap. 2 § andra stycket brottsbalken,

e) våldtäkt mot barn enligt 6 kap. 4 § första eller andra stycket brottsbalken,

f) grovt sexuellt övergrepp mot barn enligt 6 kap. 6 § andra stycket brottsbalken,

4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i fyra år,

[3] Senaste lydelse 2020:174.

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

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

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

j) grovt barnpornografibrott enligt 16 kap. 10 a § sjätte stycket brottsbalken,

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

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

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

5. annan brottslighet som kan antas ha utövats i organiserad form eller systematiskt om det med hänsyn till omständigheterna kan antas att den samlade brottslighetens straffvärde överstiger fängelse i fyra år. I sammanläggningen får det endast ingå brott som kan antas utgöra ett led i denna brottslighet och för vilka det inte är föreskrivet lindrigare straff än fängelse i sex månader, eller försök, förberedelse eller stämpling till ett sådant brott, om en sådan gärning är belagd med straff, eller

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 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.

20 e §[4]

Hemlig rumsavlyssning får användas endast om någon är skäligen misstänkt för ett brott som avses i 20 d § och åtgärden är av synnerlig vikt för utredningen.

Åtgärden får avse endast 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.

Utom i fall som avses i 20 f §, får åtgärden avse endast 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.

Hemlig rumsavlyssning 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.

[4] Senaste lydelse 2014:1419.

20 f §

Om det finns särskilda skäl får ett beslut om hemlig rumsavlyssning avse den skäligen misstänkte i stället för en viss plats. Beslutet får då verkställas endast på så sätt att avlyssningen riktas mot en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Avlyssningen får riktas mot någon annan stadigvarande bostad än den misstänktes endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. De tekniska hjälpmedel som används får inte placeras på en plats som skyddas mot intrång eller på sådana platser som avses i 20 e § tredje stycket. Åtgärden får inte heller riktas mot sådana platser som avses i 20 e § tredje stycket.

21 §[5]

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

Frågor om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning prövas av rätten på ansökan av åklagaren. *Om ansökan med stöd av 20 b § tredje stycket eller 20 f § avser den skäligen misstänkte ska åklagaren i samband med ansökan föreslå sådana villkor som avses i sjätte stycket.*

[5] Senaste lydelse 2014:1419.

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

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

I ett tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning ska det anges vilken plats tillståndet gäller. Om tillståndet är förenat med ett särskilt tillstånd enligt 25 a § att få tillträde till en plats för att installera tekniska hjälpmedel, ska det anges särskilt i beslutet.

I ett tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning ska det, *utom i fall som avses i 20 b § tredje stycket eller 20 f §,* anges vilken plats tillståndet gäller. *Om beslutet med stöd av 20 b § tredje stycket eller 20 f § avser den skäligen misstänkte ska det anges i beslutet.* Om tillståndet är förenat med ett särskilt tillstånd enligt 25 a § att få tillträde till en plats för att installera tekniska hjälpmedel, ska det anges särskilt i beslutet.

I ett beslut att tillåta hemlig rumsavlyssning ska det också anges vem som är skäligen misstänkt för brottet.

I ett beslut att tillåta åtgärder enligt första stycket ska det, när det finns skäl till detta, också i övrigt anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan.

I ett beslut att tillåta åtgärder enligt första stycket ska det, när det finns skäl till detta, också i övrigt anges villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. *I ett beslut om tillstånd till hemlig kameraövervakning som avses i 20 b § tredje stycket eller hemlig rumsavlyssning som avses i 20 f § ska sådana villkor alltid anges*.

21 a §[6]

Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation *eller* hemlig kameraövervakning, 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 avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, *hemlig rumsavlyssning eller tillträde som avses i 25 a §*, 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.

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 avlyssningen eller övervakningen, eller för någon annan som uppgifterna avser.

25 a §[7]

Vid hemlig rumsavlyssning får den verkställande myndigheten, efter särskilt tillstånd, i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Ett sådant tillstånd får avse endast den plats som ska avlyssnas eller, om det finns särskilda skäl, en plats som direkt angränsar till den platsen. Ett tillstånd att skaffa sig tillträde till en sådan angränsande plats får dock inte avse någon annan stadigvarande bostad än den misstänktes.

[6] Senaste lydelse 2014:1419.
[7] Senaste lydelse 2014:1419.

Om en plats ska bli föremål för *både hemlig rumsavlyssning och* hemlig kameraövervakning, får ett särskilt tillstånd enligt första stycket meddelas *även* för kameraövervakningen. *Detta* får dock inte avse tillträde för installation av tekniska hjälpmedel i någons stadigvarande bostad.

Om en plats ska bli föremål för hemlig kameraövervakning, får ett särskilt tillstånd enligt första stycket meddelas för kameraövervakningen. *Tillståndet* får dock inte avse tillträde för installation av tekniska hjälpmedel i någons stadigvarande bostad.

Om ett tillstånd enligt första eller andra stycket avser ett fordon, får den verkställande myndigheten, om det behövs, tillfälligt flytta fordonet i samband med tillträdet.

Om ett tekniskt hjälpmedel har installerats med stöd av ett tillstånd enligt första eller andra stycket, ska hjälpmedlet tas bort eller göras obrukbart så snart som möjligt efter det att tiden för tillståndet har gått ut eller tillståndet har upphävts.

När ett beslut om hemlig rumsavlyssning eller hemlig kameraövervakning verkställs får olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt.

Denna lag träder i kraft den 1 januari 2024.

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 att 28 §[1] lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. ska upphöra att gälla.

Denna lag träder i kraft den 1 januari 2024.

[1] Senaste lydelse 2020:63.

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 att 4 kap. 27 och 28 a §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 kap.	
27 §[1]	
En ansökan om hemlig kameraövervakning av någon som befinner sig i Sverige handläggs av åklagare. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd eller, när det får ske enligt 27 kap. 21 a § rättegångsbalken, själv besluta om åtgärden.	En ansökan om hemlig kameraövervakning av någon som befinner sig i Sverige handläggs av åklagare. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd eller, när det får ske enligt 27 kap. 21 a § rättegångsbalken, själv besluta om åtgärden *och i förekommande fall om tillträdestillstånd*.

Upptagningar behöver inte granskas enligt 27 kap. 24 § rättegångsbalken.

Om åklagaren har fattat beslut enligt första stycket, ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om hemlig kameraövervakning. Upptagningar får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning har skett enligt 2 kap. 1 § endast om detta är tillåtet enligt 27 kap. 24 § rättegångsbalken.

I fråga om underrättelse till en enskild enligt 27 kap. 31–33 §§ rättegångsbalken ska bestämmelserna i 4 kap. 25 § tredje stycket denna lag tillämpas.

[1] Senaste lydelse 2014:1424.

28 a §[2]

En ansökan om hemlig rumsavlyssning av någon som befinner sig i Sverige handläggs av åklagare. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd.	En ansökan om hemlig rumsavlyssning av någon som befinner sig i Sverige handläggs av åklagare. Åklagaren ska genast pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd, *eller, när det får ske enligt 27 kap. 21 a § rättegångsbalken, själv besluta om åtgärden och i förekommande fall om tillträdestillstånd*.

Upptagningar och uppteckningar behöver inte granskas enligt 27 kap. 24 § rättegångsbalken.

Upptagningar och uppteckningar får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning skett enligt 2 kap. 17 § endast om detta är tillåtet enligt 27 kap. 24 § rättegångsbalken.	*Om åklagaren har fattat beslut enligt första stycket, ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om hemlig rumsavlyssning.* Upptagningar och uppteckningar får bevaras efter det att ärendet om rättslig hjälp har avslutats och återredovisning skett enligt 2 kap. 17 § endast om detta är tillåtet enligt 27 kap. 24 § rättegångsbalken.

I fråga om underrättelse till en enskild enligt 27 kap. 31–33 §§ rättegångsbalken ska bestämmelserna i 4 kap. 25 § tredje stycket denna lag tillämpas.

Denna lag träder i kraft den 1 januari 2024.

[2] Senaste lydelse 2014:1424

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

Härigenom föreskrivs i fråga om lagen (2017:1000) om en europeisk utredningsorder att 2 kap. 5 och 3 kap. 10 §§ ska ha följande lydelse.

Lydelse enligt prop. 2021/22:119	*Föreslagen lydelse*
2 kap.	
5 §	
Innan åklagaren utfärdar en utredningsorder ska åklagaren ansöka om domstolens tillstånd till att utfärda utredningsordern, om utredningsåtgärden avser	
1. kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken,	
2. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning, eller	
3. rättsmedicinsk undersökning enligt 16 § lagen (1995:832) om obduktion m.m.	
I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken eller 17 § lagen (2020:62) om hemlig dataavläsning utfärda en utredningsorder för *kvarhållande av försändelse, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning eller hemlig dataavläsning.* Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.	I avvaktan på domstolens beslut får åklagaren under de förutsättningar som anges i 27 kap. 9 a och 21 a §§ rättegångsbalken eller 17 § lagen (2020:62) om hemlig dataavläsning utfärda en utredningsorder för *en åtgärd som avses i första stycket första eller andra punkten och i förekommande fall tillträdestillstånd.* Åklagaren ska utan dröjsmål anmäla till domstolen att en utredningsorder har utfärdats.
Innan en utredningsorder för husrannsakan, genomsökning på distans, kroppsvisitation eller kroppsbesiktning utfärdas, får åklagaren enligt 28 kap. 4 § första stycket, 10 d § andra 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.

Nuvarande lydelse	*Föreslagen lydelse*
3 kap.	
10 §[1]	
I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a *och* 21 a §§ rättegångsbalken eller 17 § lagen (2020:62) om hemlig dataavläsning, besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning eller hemlig dataavläsning.	I avvaktan på domstolens beslut enligt 9 § första stycket får åklagaren, enligt de förutsättningar som anges i 27 kap. 9 a, 21 a *och 25 a* §§ rättegångsbalken eller 17 § lagen (2020:62) om hemlig dataavläsning, besluta att erkänna och verkställa en utredningsorder för kvarhållande av försändelse enligt 27 kap. 9 § rättegångsbalken eller för hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, *hemlig rumsavlyssning* eller hemlig dataavläsning *och i förekommande fall tillträdestillstånd.*

Denna lag träder i kraft den 1 januari 2024.

[1] Senaste lydelse 2020:67.

1.5 Förslag till lag om ändring i lagen (2020:62) om hemlig dataavläsning

Härigenom föreskrivs i fråga om lagen (2020:62) om hemlig dataavläsning

dels att 4–6, 14, 15, 17 och 18 §§ ska ha följande lydelse,

dels att det i lagen ska införas två nya paragrafer, 4 a och 5 a §§, av följande lydelse.

Lydelse enligt prop. 2021/22:119	*Föreslagen lydelse*
4 §	
Ett tillstånd till hemlig dataavläsning får, om åtgärden är av synnerlig vikt för utredningen och inte annat anges i 6 § första stycket, beviljas vid en förundersökning om	Ett tillstånd till hemlig dataavläsning får, om åtgärden är av synnerlig vikt för utredningen och inte annat anges i *5 a § eller* 6 § första stycket, beviljas vid en förundersökning om
1. brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år,	
2. brott som avses i 27 kap. 18 § andra stycket 2–*7* rättegångsbalken,	2. brott som avses i 27 kap. 18 § andra stycket 2–*15* rättegångsbalken,
3. försök, förberedelse eller stämpling till brott som avses i 1 eller 2, om en sådan gärning är belagd med straff, *eller*	3. försök, förberedelse eller stämpling till brott som avses i 1 eller 2, 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.	4. annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år, *eller*
	5. annan brottslighet som kan antas ha utövats i organiserad form eller systematiskt om det med hänsyn till omständigheterna kan antas att den samlade brottslighetens straffvärde överstiger fängelse i två år. I sammanläggningen får det endast ingå brott som kan antas ut-

göra ett led i denna brottslighet och för vilka det är föreskrivet fängelse i ett år eller däröver, eller försök, förberedelse eller stämpling till ett sådant brott, om en sådan gärning är belagd med straff.

Ett tillstånd enligt första stycket får, om inte annat anges i 5 §, endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för brottet.

Ett tillstånd enligt första stycket som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får, om inte annat anges i 5 §, även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Ett tillstånd enligt första stycket som gäller kameraövervakningsuppgifter får endast avse en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Ett tillstånd enligt första stycket får, om inte annat anges i 5 § *eller 5 a §*, endast avse ett avläsningsbart informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för brottet.

Ett tillstånd enligt första stycket som gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får, om inte annat anges i 5 § *eller 5 a §*, även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta.

Ett tillstånd enligt första stycket som gäller kameraövervakningsuppgifter får, *utom i fall som avses i 4 a §*, endast avse en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.

Nuvarande lydelse	*Föreslagen lydelse*
	4 a § *Om det finns särskilda skäl får ett tillstånd enligt 4 § första stycket som gäller kameraövervakningsuppgifter, i stället för en viss plats avse den skäligen misstänkte. Åtgärden får då endast användas på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad.*
5 §	
Ett tillstånd till hemlig dataavläsning enligt 4 § som gäller kommunikationsövervaknings- eller platsuppgifter får även beviljas för att utreda vem som skäligen kan misstänkas för ett brott som avses i 4 §. *Avläsning eller upptagning av kommunikationsövervakningsuppgifter får då endast avse förfluten tid.*	Ett tillstånd till hemlig dataavläsning enligt 4 § som gäller kommunikationsövervaknings- eller platsuppgifter får även beviljas för att utreda vem som skäligen kan misstänkas för ett brott *eller brottslighet* som avses i 4 §.

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

	5 a § *Ett tillstånd till hemlig dataavläsning enligt 4 § som gäller kommunikationsavlyssningsuppgifter får även beviljas för att utreda vem som skäligen kan misstänkas för ett brott eller brottslighet som avses i 27 kap. 18 a § rättegångsbalken.*

Hemlig dataavläsning enligt första stycket får endast avse ett avläsningsbart informationssystem

1. som under den tid som tillståndet avser kan antas ha använts eller kan komma att användas av någon som kan misstänkas ha begått eller annars medverkat till brottet, eller

2. som det finns synnerlig anledning att anta att någon som kan misstänkas ha begått eller annars medverkat till brottet har kontaktat eller kommer att kontakta under den tid som tillståndet avser.

6 §

Ett tillstånd till hemlig dataavläsning enligt 4 § som gäller rumsavlyssningsuppgifter får endast beviljas vid en förundersökning om brott som avses i 27 kap. 20 d § andra stycket rättegångsbalken.

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

Ett tillstånd till hemlig dataavläsning enligt 4 § som gäller rumsavlyssningsuppgifter får endast beviljas vid en förundersökning om brott *eller brottslighet* som avses i 27 kap. 20 d § andra stycket rättegångsbalken.

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

Om det finns särskilda skäl får ett tillstånd enligt första stycket i stället för en viss plats avse den

	skäligen misstänkte. Åtgärden får då endast användas där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Om platsen är någon annan stadigvarande bostad än den misstänktes, får hemlig dataavläsning ske endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där.

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

14 §

Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagare. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen eller Polismyndigheten.	Frågor om hemlig dataavläsning prövas av rätten på ansökan av åklagare. En ansökan om hemlig dataavläsning enligt 9 § ska dock göras av Säkerhetspolisen eller Polismyndigheten. *Om beslutet med stöd av 4 a § eller 6 § tredje stycket avser den skäligen misstänkte ska åklagaren i samband med ansökan föreslå sådana villkor som avses i 18 § första stycket 4.*

Lydelse enligt prop. 2021/22:119 *Föreslagen lydelse*

15 §

Frågor om hemlig dataavläsning under en förundersökning prövas av den domstol som anges i 19 kap. rättegångsbalken. Om förundersökningen avser brott som anges i 27 kap. 18 § andra stycket *2–7* rättegångsbalken eller försök, förberedelse eller stämpling till ett sådant brott, om en	Frågor om hemlig dataavläsning under en förundersökning prövas av den domstol som anges i 19 kap. rättegångsbalken. Om förundersökningen avser brott som anges i 27 kap. 18 § andra stycket *5*, *6*, *10*, *11*, *14 eller 15* rättegångsbalken eller försök, förberedelse eller stämpling till ett

sådan gärning är belagd med straff, får frågan även prövas av Stockholms tingsrätt.	sådant brott, om en sådan gärning är belagd med straff, får frågan även prövas av Stockholms tingsrätt.

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

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

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

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

18 §

I ett tillstånd till hemlig dataavläsning ska följande anges:

1. vilken tid tillståndet avser,

2. vilket avläsningsbart informationssystem tillståndet avser,

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

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

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

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

Om beslutet med stöd av 4 a § eller 6 § tredje stycket avser den skäligen misstänkte ska det anges i beslutet.

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

Denna lag träder i kraft den 1 januari 2024.

2 Uppdraget och vårt arbete

2.1 Uppdraget enligt dir. 2020:104

Utredningens direktiv, bilaga 1, beslutades vid ett regeringssammanträde den 14 oktober 2020. I direktiven anförs bl.a. följande. De brottsbekämpande myndigheterna måste ha tillgång till ändamålsenliga och verkningsfulla verktyg för att kunna lagföra dem som begår brott. Förändringar i brottsligheten och av misstänkta personers beteenden samt den tekniska utvecklingen har inneburit att det finns ett ökat behov av att kunna använda hemliga tvångsmedel. Detta behov är påtagligt när det gäller den grova våldsbrottslighet och förmögenhetsbrottslighet som begås i kriminella miljöer. Många kriminella nätverk i Sverige är i dag löst sammansatta. Samtidigt ökar samverkan mellan kriminella aktörer med kompetens inom ekonomi och kriminella aktörer med våldskapital. För att uppnå ekonomisk vinning söker kriminella aktörer efter olika konstellationer och samverkansformer. Formerna för dessa kan variera beroende på typ av brottsupplägg, men generellt sett följs graden av organisering och komplexiteten i ett brottsupplägg åt. De kriminella aktörerna blir också mer tekniskt sofistikerade (Nationellt underrättelsecentrums rapport Myndighetsgemensam lägesbild om organiserad brottslighet 2018–2019 s. 4). Brott som begås inom ramen för kriminella nätverk är ofta särskilt svåra att utreda eftersom brottsoffer och vittnen av olika anledningar kan vara obenägna att lämna information till polisen. Det finns därför skäl att se över om de brottsbekämpande myndigheterna ska ges utökade möjligheter att använda hemliga tvångsmedel.

Utredningens uppdrag har varit att se över delar av regleringen om hemliga tvångsmedel. Syftet med översynen har varit att ta ställning till hur hemliga tvångsmedel ska kunna användas i en större utsträckning för att bekämpa allvarlig brottslighet. Det har ingått i uppdraget att noga väga behovet av en effektiv brottsbekämpning mot

den enskildes rätt till skydd för sin personliga integritet. Det har ålegat oss att göra en sådan avvägning för varje förslag för sig och även när det gäller förslagen sammantaget. Vidare framgår av direktiven ett krav på att förslagen uppfyller högt ställda krav på rättssäkerhet.

I uppdraget har ingått att

- ta ställning till om det bör införas en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning vid misstanke om flera brott vars samlade straffvärde kan antas överstiga ett visst straff,
- ta ställning till i vilka situationer och vid vilka straffvärden en sådan möjlighet bör kunna tillämpas,
- ta ställning till om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation bör få användas vid fler brott,
- ta ställning till om det bör vara tillåtet med hemlig övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet och i så fall i vilka situationer,
- ta ställning till om tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning bör kunna knytas till en person,
- ta ställning till om åklagare bör få möjlighet att fatta interimistiska beslut om hemlig rumsavlyssning inklusive tillträde för att installera utrustningen,
- ta ställning till om den verkställande myndigheten bör kunna få tillstånd att i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång för att verkställa ett beslut om enbart hemlig kameraövervakning,
- ta ställning till om åklagare bör få möjlighet att interimistiskt besluta om sådant tillträde,
- ta ställning till om en straffvärdeventil bör införas i inhämtningslagen,
- ta ställning till om skyddet för den personliga integriteten bör stärkas, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Det ingår i uppdraget att säkerställa att en välfungerande systematik i regelverket om hemliga tvångsmedel upprätthålls. Det innebär att vi även ska bedöma behovet av följdändringar i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen (1991:572) om särskild utlänningskontroll samt lagen (2020:62) om hemlig dataavläsning. Utredaren ska även bedöma behovet av följdändringar i lagen (2000:562) om internationell rättslig hjälp i brottmål och lagen (2017:1000) om en europeisk utredningsorder. När det finns behov av det ska förslag på författningsändringar lämnas.

Utredningen har möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska utredas under förutsättning att uppdraget ändå kan redovisas i tid.

2.2 Uppdraget enligt dir. 2022:13

Den 17 mars 2022 beslutade regeringen om tilläggsdirektiv (dir. 2022:13). Vi fick därigenom, utöver vad som framgår av de ursprungliga direktiven, även i uppdrag att särskilt bedöma om det finns ett behov av att ändra reglerna om underrättelse till enskild om användning av hemliga tvångsmedel, ta ställning till om och i så fall i vilka situationer hemlig övervakning av elektronisk kommunikation bör få användas för att lokalisera personer som är häktade i sin frånvaro efter att en förundersökning har avslutats eller som har uteblivit eller avvikit från verkställighet av påföljder, och lämna förslag till författningsändringar som bedöms nödvändiga. Utredningstiden ligger fast för större delen av det ursprungliga uppdraget som redovisas i detta delbetänkande. Utredningstiden har dock förlängts för frågan i de ursprungliga direktiven om i vilka situationer hemlig övervakning av elektronisk kommunikation bör få användas för att lokalisera skäligen misstänkta. Den frågan ska, tillsammans med den del av uppdraget som omfattas av tilläggsdirektiven, slutredovisas senast den 14 oktober 2022.

2.3 Vårt arbete

Utredningen började i praktiken sitt arbete i november 2020 och höll sitt första utredningssammanträde i december samma år. Vi har hållit sammanlagt 10 utredningssammanträden inför avgivande av delbetänkandet. På grund av pandemin har flertalet sammanträden hållits digitalt. Vi har haft underhandskontakter med företrädare för Post- och telestyrelsen och TechSverige.

Vi har inte kunnat beakta propositioner och annat material som tillkommit efter den 28 februari 2022.

3 Regler till skydd för den personliga integriteten

3.1 Regeringsformen

Den offentliga makten ska enligt 1 kap. 2 § regeringsformen utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet. Av paragrafen följer även att det allmänna ska värna den enskildes privatliv och familjeliv. Bestämmelsen ger uttryck för en grundläggande målsättning med det allmännas verksamhet. Enligt 2 kap. 6 § första stycket regeringsformen gäller vidare att var och en gentemot det allmänna är skyddad mot bl.a. husrannsakan och liknande intrång, undersökning av brev eller annan förtrolig försändelse samt hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Det finns också i paragrafens andra stycke en bestämmelse som tillförsäkrar enskilda ett generellt skydd gentemot det allmänna, mot betydande intrång i den personliga integriteten om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet enligt 2 kap. 6 § regeringsformen kan begränsas endast genom lag. Begränsningen får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar (2 kap. 20 och 21 §§ regeringsformen). För utländska medborgare som är bofasta i riket gäller att särskilda begränsningar i dessa rättigheter får göras genom lag (2 kap. 25 § regeringsformen).

3.2 Europakonventionen

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

Rätten till privatliv, familjeliv, hem och korrespondens

Enligt artikel 8.1 Europakonventionen har var och en rätt till respekt för sitt privatliv och familjeliv, sitt hem och sin korrespondens. Rättigheterna får enligt artikel 8.2 Europakonventionen inskränkas endast 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.

Skyddet enligt artikel 8 är omfattande. Europadomstolen har flera gånger framhållit att det inte är möjligt att definiera begreppet genom en uttömmande beskrivning av olika aspekter som rör den enskildes privata förhållanden. Begreppet täcker olika aspekter av en enskild individs såväl fysiska som psykiska integritet. Här kan särskilt nämnas kommunikation genom telefon och e-post, rörelsemönster, personuppgifter samt en persons ära och hem. Det följer också av bestämmelsen att det ska finnas rättsmedel för att effektivt bekämpa brott som utgör ett ingrepp i brottsoffrets rätt till privatliv. Även uppgifter som är hänförliga till en persons yrkesliv kan omfattas av rätten till privatliv.

Om staten lagrar information hänförligt till folks privatliv, kan både det och tillgången till informationen utgöra ett intrång i rätten till privatliv. Det gäller även om informationen består av enbart offentliga och okänsliga uppgifter samt sker utan hjälp av något hemligt tvångsmedel. Se Gillberg mot Sverige punkt 66, Rotaru mot Rumänien punkt 43, Leander mot Sverige punkt 48, Segerstedt-Wiberg m.fl. mot Sverige punkt 72, S. och Marper mot Förenade kungariket punkt 66, Uzun mot Tyskland punkt 46 och Amann mot Schweiz punkterna 65–67.

När det gäller hemliga tvångsmedel kan särskilt noteras att det inte bara är privatlivet för personen som tvångsmedlet riktas mot som är skyddat, utan även privatlivet hos den som t.ex. ringer till en avlyssnad telefon. Avlyssningen i sig innebär ett ingrepp, det spelar ingen roll om inspelningarna aldrig ens nått åklagaren utan förstörts och aldrig använts. Se Amann mot Schweiz punkt 45 och Kopp mot Schweiz punkterna 51–53.

Rätten till respekt för privatlivet innefattar både ett förbud för staten att göra otillåtna ingrepp i privatlivet och en skyldighet för staten att genom bl.a. lagstiftning och andra åtgärder skydda den enskildes privatliv, familjeliv och korrespondens mot ingrepp från andra, se X och Y mot Nederländerna punkt 23, von Hannover mot Tyskland § 57 och K.U. mot Finland punkterna 47–49. Ett sådant skydd tillförsäkras bl.a. genom kriminalisering av olika åtgärder som innefattar allvarliga intrång i den personliga integriteten, såsom sexuella övergrepp. I målet Söderman mot Sverige (punkterna 86–117) fann Europadomstolen att det skett en kränkning av artikel 8 då det saknades straffbestämmelser för att ett barn i hemlighet hade filmats eller fotograferats naken, och då de civilrättsliga rättsmedlen ansågs ineffektiva.

En förutsättning för att staten ska kunna leva upp till kraven på att upprätthålla rättstryggheten för enskilda är att staten har en väl fungerande och effektiv brottsbekämpning. Detta krav innebär t.ex. att myndigheterna ska ha tillgång till effektiva utredningsverktyg – även i den elektroniska miljön – för att utreda brott som innefattar allvarliga kränkningar. När så inte har varit fallet har staten ansetts kränka de rättigheter som följer av artikel 8. Ett exempel på detta var målet K.U. mot Finland. I målet hade en okänd person hade lagt upp en kränkande kontaktannons avseende ett 12-årigt barn på en dejtingsajt. Europadomstolen fann att avsaknaden av en möjlighet enligt finsk rätt att inhämta uppgift om vem som använt en ip-adress från operatören, vilket ledde till att personen inte kunde identifieras, utgjorde en kränkning av artikel 8. Europadomstolen uttalade i domen att konfidentialitet för kommunikation och yttrandefrihet ibland måste få vika för brottsbekämpande ändamål. Målet Khadija Ismayilova mot Azerbajdzjan gällde en hemlig filmning av en journalist i hennes hem och publiceringen av bildmaterialet. I det fallet fanns det tillämpliga straffbestämmelser och en brottsutredning hade inletts. Emellertid fann Europadomstolen att myndigheterna genom att inte genom-

föra en effektiv brottsutredning av det mycket allvarliga intrånget i hennes privatliv hade underlåtit att tillförsäkra klaganden ett tillräckligt skydd för hennes privatliv (punkterna 119–131).

Inskränkningar i skyddet

Det skydd som följer av artikel 8 är inte absolut utan får inskränkas. För att en inskränkning ska vara tillåten måste den ha stöd i inhemsk lag som i sin tur måste uppfylla rimliga anspråk på rättssäkerhet, såsom att skydda mot godtycke, vara tillgänglig för allmänheten och vara förutsebar. Att inskränkningen måste vara nödvändig i ett demokratiskt samhälle för något av de i artikeln skyddade intressena innebär i huvudsak att det ska finnas ett angeläget samhälleligt behov av åtgärden och att den måste stå i rimlig proportion till det syfte som ska tillgodoses (Hans Danelius, Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna, 5 uppl., s. 369 och 370). Konventionsstaterna har ett visst handlingsutrymme att själva avgöra om begränsningarna är nödvändiga för ett givet syfte (eng. margin of appreciation). Europadomstolen förbehåller sig dock rätten att överpröva denna bedömning inom ramen för prövningen av någons enskilda klagomål hos domstolen.

Hemliga tvångsmedel

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

Europadomstolen har genom praxis utvecklat en minimistandard för de krav som bör ställas på lagstiftningen om dolda spaningsåtgärder eller hemliga tvångsmedel till undvikande av missbruk (se målet

Roman Zakharov mot Ryssland punkt 231 och där angivna rättsfall). Enligt denna bör i den nationella lagstiftningen anges

– 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, och
– de omständigheter under vilka inspelningar kan eller måste raderas.

Den grad av förutsebarhet som krävs varierar beroende på vilken typ av hemlig tvångsåtgärd som lagstiftningen avser och hur ingripande åtgärden är. I ett mål om dold gps-övervakning av förflyttningar på offentliga platser, uttalade Europadomstolen att de relativt strikta krav som minimistandarden ställer har utarbetats i mål om telefonavlyssning. Domstolen fann att dessa krav inte var fullt ut tillämpliga i målet eftersom en sådan övervakning utgjorde ett mindre intrång i privatlivet, se Europadomstolens dom den 2 september 2010 i målet Uzun mot Tyskland punkt 65 och 66, jämför även dom den 25 september 2001 i P.G. och J.H. mot Förenade kungariket punkt 42.

Europadomstolen har vidare slagit fast att nationell lagstiftning om dolda spaningsåtgärder och hemliga tvångsmedel måste innehålla kontrollmekanismer för att skydda mot missbruk. Vad som krävs i det avseendet beror på åtgärdernas karaktär, räckvidd och varaktighet, vilka motiv som krävs för att besluta, utföra och övervaka dem samt vilken typ av rättsmedel som finns i den nationella lagstiftningen (se t.ex. målet P.G. och J.H. mot Storbritannien punkt 76–81 och målet Uzun mot Tyskland). Enligt artikel 13 Europakonventionen ska var och en som fått sina fri- och rättigheter enligt konventionen kränkta ha tillgång till ett effektivt rättsmedel inför en nationell myndighet, även om kränkningen förövats av någon under utövning av offentlig myndighet. Enligt propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation (prop. 2011/12:55 s. 55) kräver inte artikeln ett rättsmedel inför

domstol, utan även administrativa rättsmedel kan vara tillräckliga för att uppfylla konventionskraven. För att rättsmedlet ska anses vara effektivt får dock den rättsliga prövningen inte vara alltför begränsad. Den ska i princip sträcka sig lika långt som Europadomstolens egen prövning av om konventionen blivit överträdd. I många fall är möjligheten att föra skadeståndstalan tillräcklig för att motsvara kraven på effektiva rättsmedel i artikel 13 (Hans Danelius, Mänskliga rättigheter i europeisk praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna, 5 uppl., s. 546). Europadomstolen har framhållit att det vid hemlig telefonavlyssning är svårt att använda normala rättsmedel. Enligt domstolen kan det inte krävas att den som berörs ska underrättas om avlyssningen i förväg, utan kravet måste i detta sammanhang förstås så att det ska finnas ett så effektivt rättsmedel som möjligt med hänsyn till de särskilda omständigheterna. Domstolen har lagt vikt vid bl.a. om det funnits regler om underrättelse om tvångsmedlet i efterhand, när detta kunnat ske utan risk eller skada (Danelius, a.a., s. 547).

3.3 FN:s konvention om medborgerliga och politiska rättigheter

FN:s generalförsamling antog år 1948 en allmän förklaring om de mänskliga rättigheterna. I artikel 12 i förklaringen slås fast att ingen får utsättas för godtyckliga ingripanden i fråga om bl.a. privatliv, familj, hem eller korrespondens. Förklaringen är inte rättsligt bindande för staterna. Grundsatsen har emellertid även arbetats in i 1966 års FN-konvention om medborgerliga och politiska rättigheter (artikel 17) som trädde i kraft den 23 mars 1976 och som är rättsligt bindande för konventionsstaterna. Sverige ratificerade konventionen den 26 november 1971 (SÖ 1971:42).

3.4 EU:s rättighetsstadga

En bestämmelse om rätt till respekt för bl.a. privatlivet och korrespondensen finns också i artikel 7 Europeiska unionens stadga om de grundläggande rättigheterna av den 7 december 2000, anpassad den 12 december 2007 i Strasbourg (rättighetsstadgan). I artikel 8 i rättighetsstadgan slås därutöver fast en rätt till skydd för person-

uppgifter som rör någon enskild. Denna rättighet har ingen direkt motsvarighet i Europakonventionen, men det framgår av Europadomstolens praxis att en rätt till skydd för personuppgifter omfattas av främst artikel 8 i Europakonventionen (Satakunnan Markkinapörssi Oy och Satamedia Oy mot Finland, § 137 och Z. mot Finland, punkt 95). Av artikel 52.3 följer att i den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen ska de ha samma innebörd och räckvidd som enligt konventionen. Det hindrar dock samtidigt inte unionsrätten från att tillförsäkra ett mer långtgående skydd (jfr artikel 52.3 och artikel 53).

Rättighetsstadgan riktar sig till medlemsstaterna endast när de tillämpar unionsrätten. Det innebär att rättigheterna i stadgan måste iakttas bara vid tillämpningen av nationell lagstiftning som genomför EU-rätt och nationell lagstiftning som omfattas av unionens tillämpningsområde (se t.ex. EU-domstolens dom den 26 februari 2013 i målet Åkerberg Fransson, C617/10, punkt 21). Av artikel 52.1 framgår att varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan ska vara föreskriven i lag och förenlig med det väsentliga innehållet i dessa rättigheter och friheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter.

EU-domstolen har i ett antal avgöranden gjort vissa uttalanden utifrån ett rättighetsperspektiv om myndigheters tillgång till lagrade uppgifter för brottsbekämpande ändamål, se vidare i avsnitt 4.2.2.

4 Gällande rätt

4.1 De brottsbekämpande myndigheternas uppdrag

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

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

Säkerhetspolisens uppdrag kan i huvudsak delas in i fem områden: kontraspionage, kontraterrorism, författningsskydd, säkerhetsskydd och personskydd. Säkerhetspolisen arbetar dessutom med att förhindra spridning, anskaffning och produktion av massförstörelsevapen samt ansvarar vidare för utredningar som rör brott mot Sveriges säkerhet och terroristbrott. Tyngdpunkten i Säkerhetspolisens verksamhet är dock underrättelseverksamhet, dvs. att förebygga, förhindra och upptäcka brottslig verksamhet. Säkerhetspolisen kan därför som regel inte bedriva sin verksamhet utifrån brottsanmälningar. Myndigheten måste i stället själv ha förmåga att identifiera företeelser som kan utvecklas till brott, och aktörer som har för avsikt att begå

brott samt att leta upp brott som hittills är okända men som pågår i det fördolda. Underrättelseverksamheten bedrivs i ett skede innan det finns tillräckliga skäl för att inleda förundersökning.

Tullverkets verksamhet inom kontroll- och tullkriminalavdelningen har till syfte att stoppa eller allvarligt störa den organiserade brottsligheten och att förhindra den illegala införseln av narkotika- och dopingpreparat, alkohol, tobak, vapen och andra varor som hotar liv, hälsa och miljö, dvs. smuggling. Kontrollavdelningen ska tillse att kontrollen av att in och utförselreglerna följs. Vidare ska avdelningen förebygga, förhindra och upptäcka brott i samband med in- och utförsel av varor samt att se till att den som begått brott identifieras och lagförs. Myndighetens brottsbekämpande verksamhet består huvudsakligen av verksamheterna gränsskydd och tullkriminal och arbetet sträcker sig genom hela kedjan från underrättelse, analys och kontroll till färdig förundersökning.

4.2 Uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

4.2.1 Allmänt om elektronisk kommunikation

Elektronisk kommunikation innebär överföring av signaler i elektronisk form. Elektronisk kommunikation omfattar telefoni, datakommunikation och utsändningar till allmänheten via radio eller tv. Den tekniska utvecklingen har medfört att dessa delar gradvis växer samman. Flera av de hemliga tvångsmedlen tar sikte på elektronisk kommunikation. Det finns därför anledning att inledningsvis säga några ord om användningen av elektronisk kommunikation och vilken information som genereras av sådan information.

Elektronisk kommunikation är en allt större del av människors vardag, såväl privat som i arbetet. Vi ringer till varandra, skickar sms, e-post och andra meddelanden och kopplar upp oss mot internet för att använda appar eller besöka webbsidor. De flesta gör allt detta dagligen. För att all kommunikation ska hamna rätt och för att den ska kunna faktureras av tjänsteleverantörerna genereras en del information om varje samtal och meddelande. Denna information om meddelandet (men inte vad som sägs eller står skrivet) kallas för metadata. Exempel på sådan information är telefonnummer, utrustningsnummer (IMEI, MAC), abonnemangsnummer (IMSI), ip-adresser

(ett nummer som används som adress på internet), e-postadresser och användarnamn som meddelandet skickas mellan, tidpunkt som meddelandet sänds och vilken mobilmast som meddelandet skickas genom. Informationen följer sedan med själva samtalet eller meddelandet.

Varje samtal och meddelande innehåller bara uppgifter om det specifika meddelandet (samtal är också ett slags meddelande). Men om man får tillgång till flera uppgifter, t.ex. en lista över all kommunikation från ett visst nummer, en telefon eller en e-postadress, kan man dra flera slutsatser, bl.a. om vilka kontakter en person haft i anslutning till en viss händelse eller hur en kommunikationsutrustning förflyttats under samma tid.

Förutom metadata, som följer med meddelanden, skapas det löpande uppgifter om var en mobiltelefon befinner sig. Det behövs för att operatören ska kunna skicka fram meddelanden till telefonen eller leverera andra tjänster. Både den informationen och de lokaliseringsuppgifter som genereras med meddelanden gör att det går att se i vilket område en telefon har varit eller vilka telefoner som har varit i ett visst område, t.ex. vid en mordplats.

Om man inte tar del av informationen i realtid krävs det att informationen lagras för att man ska kunna ta del av den. En del information lagras hos telekombolagen för att informationen behövs t.ex. för fakturering. Annan information lagrar bolagen för att staten kräver det, t.ex. för att de brottsbekämpande myndigheterna ska kunna använda sig av informationen om det behövs. Denna lagring av information i brottsbekämpande syfte kallas vanligen för datalagring.

Uppgifter om elektronisk kommunikation har i svensk rätt delats in i tre olika grupper. Med *uppgift om abonnemang* (abonnemangsuppgifter) avses främst uppgifter om abonnentens nummer, namn, titel och adress. Vidare innefattas IMEI-nummer (se Post- och telestyrelsens beslut 2021-03-17, dnr 20-3147) och uppgift om vem som har använt en fast eller dynamisk ip-adress eller ett IMSI-nummer (International Mobile Subscriber Identity, ett nummer som är kopplat till abonnentens simkort och telefonnummer). Med *trafikuppgifter* avses i detta sammanhang uppgifter som behandlas i syfte att förmedla ett elektroniskt meddelande i ett elektroniskt kommunikationsnät eller för att fakturera ett sådant meddelande. Med *lokaliseringsuppgifter* avses här uppgifter som visar den geografiska positionen för

terminalutrustningen för en användare.[1] Det kan t.ex. vara fråga om vilken cell (antenn på basstation) som utrustningen kopplat upp sig mot. De olika uppgiftskategorierna är delvis överlappande.

4.2.2 EU-direktiv om elektronisk kommunikation

På området för elektronisk kommunikation finns ett flertal EU-rättsakter. För att säkerställa rätten till respekt för privatlivet och rätten till skydd för personuppgifter inom sektorn för elektronisk kommunikation har EU antagit Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), även kallat e-dataskyddsdirektivet. Direktivet definierar trafikuppgifter och lokaliseringsuppgifter, men inte uppgifter om abonnemang. Direktivet föreskriver bl.a. att medlemsstaterna ska säkerställa konfidentialitet vid elektronisk kommunikation och därmed förbundna trafikuppgifter. Uppgifter som inte längre behövs ska utplånas eller avidentifieras. Medlemsstaterna får dock göra undantag från dessa åligganden om det behövs för bl.a. brottsbekämpande verksamhet.

EU-domstolen har i praxis uttalat sig om vad möjligheten till undantag i brottsbekämpande syfte innebär, tolkad mot bakgrund av artiklarna 7 och 8 i rättighetsstadgan. Rättsfallen handlar främst om lagring av uppgifter, men innehåller även vissa uttalanden om tillgång till uppgifter i brottsbekämpande syfte. I EU-domstolens dom den 21 december 2016 i de förenade målen C-203-15 och C-698/15, den s.k. Tele2-domen, beslutade domstolen att artikel 15.1 i direktivet ska tolkas på så sätt att bestämmelsen utgör hinder för en nationell lagstiftning som i brottsbekämpande syfte föreskrifter en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel. Domen ledde till att de svenska bestämmelserna om lagring ändrades.

[1] I lagrådsremissen Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation definieras lokaliseringsuppgift som 1. en uppgift som behandlas i ett allmänt mobilt elektroniskt kommunikationsnät och som anger den geografiska positionen för en slutanvändares terminalutrustning, eller 2. en uppgift i ett allmänt fast elektroniskt kommunikationsnät om nätanslutningspunktens fysiska adress. Enligt förteckningen över propositioner som är avsedda att lämnas under 2022 planeras proposition den 1 mars 2022.

I Tele2-domen uttalade sig domstolen även om villkoren för att brottsbekämpande myndigheter ska kunna få tillgång till lagrade uppgifter. Domstolen uttalade att den berörda nationella lagstiftningen måste vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till uppgifter om abonnenter eller registrerade användare. Vidare angavs att tillgång i princip bara kan beviljas till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. Av EU-domstolens praxis följer vidare att endast bekämpning av allvarlig brottslighet kan motivera allvarliga ingrepp i de grundläggande rättigheter som anges i artiklarna 7 och 8 i EU:s rättighetsstadstadga. Endast ingrepp som inte är av allvarligt slag kan därför enligt domstolens praxis vara godtagbara i syfte att förebygga, undersöka, avslöja och väcka åtal för brott i allmänhet (se bl.a. dom av den 2 mars 2021 Prokuratuur, C-746/18, punkt 33 och ett liknande resonemang i dom av den 6 oktober 2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18 punkterna 140 och 146). Lagstiftningsåtgärder som avser behandling av uppgifter om användarna av elektroniska kommunikationsmedels fysiska identitet som sådana, bland annat lagring av och åtkomst till uppgifterna enbart i syfte att identifiera den berörda användaren, och utan att uppgifterna kan kopplas till information om de kommunikationer som har ägt rum, anses utgöra sådana mindre allvarliga ingrepp (se bl.a. Prokuratuur-domen, punkt 34).

Det ingrepp i de grundläggande rättigheter som stadfästs i artiklarna 7 och 8 i rättighetsstadgan som det innebär när en offentlig myndighet får tillgång till ett stort antal trafik- eller lokaliseringsuppgifter som kan ge information om kommunikation som en användare har utfört medelst elektronisk kommunikationsutrustning, eller om lokaliseringen av terminalutrustning som vederbörande har använt, är enligt domstolen alltid av allvarlig art, för det fall att dessa samlade uppgifter gör det möjligt att dra specifika slutsatser om den berörda personens privatliv. Detta gäller oberoende av under hur lång tid som myndigheterna ges tillgång till uppgifterna och mängden eller arten av de uppgifter som är tillgängliga under denna period (se Prokuratuur-domen punkt 39). En nationell lagstiftning om som gör det möjligt för offentliga myndigheter att få tillgång till sådana uppgifter måste därför vara begränsad till bekämpning av grov brottslighet eller förebyggande av allvarliga hot mot allmän säkerhet

(Prokuratuur-domen punkt 45). Någon definition av grov brottslighet framgår inte av EU-domstolens praxis.

Europeiska kommissionen har lämnat ett förslag till en ny förordning om respekt för privatlivet och skydd för personuppgifter i samband med elektronisk kommunikation. Förordningen ska ersätta e-dataskyddsdirektivet och utgöra en specialreglering i förhållande till den allmänna dataskyddsförordningen. Förslaget bereds för närvarande inom EU.

4.2.3 Lagen om elektronisk kommunikation

E-dataskyddsdirektivet har genomförts i svensk rätt främst genom bestämmelser som tagits in i lagen (2003:389) om elektronisk kommunikation (LEK). LEK syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster. Den 11 december 2018 antogs Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation. Direktivet trädde i kraft den 21 december 2018. I lagrådsremissen Genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation lämnas förslag till hur EU-direktivet ska genomföras. Bland annat föreslås att LEK ska ersättas av en ny lag om elektronisk kommunikation.

Tystnadsplikten

Tillhandahållare av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst omfattas enligt 6 kap. 20 § LEK av tystnadsplikt (9 kap. 31 § nya lagen enligt lagrådsremissen). Tystnadsplikten omfattar uppgifter om abonnemang, innehållet i ett elektroniskt meddelande och andra uppgifter som angår ett särskilt elektronisk meddelande. Tystnadsplikten gäller inte mot sändaren och mottagaren av ett elektroniskt meddelande. När det gäller abonnemangsuppgifter och andra uppgifter som angår ett särskilt elektroniskt meddelande gäller tystnadsplikten inte heller i förhållande till abonnenten. Tillhandahållaren har dock i förhållande till abonnenten tystnadsplikt om innehållet i ett meddelande.

Trafikuppgifter

Uppgifter om elektronisk kommunikation är mycket viktiga för brottsbekämpningen. Det finns därför regler i LEK och i förordningen (2003:396) om elektronisk kommunikation som har till syfte att säkerställa att dessa uppgifter lagras av dem som tillhandahåller elektroniska kommunikationstjänster och att de brottsbekämpande myndigheterna under vissa förutsättningar kan få tillgång till dem. Operatörerna är även skyldiga att bedriva sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs. Bestämmelserna om lagringsskyldighet ändrades den 1 oktober 2019 i syfte att göra dem förenliga med Tele2-domen. Ändringarna innebar bl.a. att lagringsskyldigheten inskränktes i förhållande till det som tidigare gällt och att lagringstiderna differentierades beroende på vilken typ av uppgift det är fråga om (prop. 2018/19:86 Datalagring vid brottsbekämpning – anpassningar till EU-rätten).

Samtidigt som det alltså finns en viss lagringsskyldighet är huvudregeln att trafikuppgifter ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande. Ett viktigt undantag från regeln om utplånande och avidentifierande är att kraven inte gäller för elektroniska meddelanden som omfattas av beslut om hemlig avlyssning eller övervakning av elektronisk kommunikation, tekniskt bistånd med sådan avlyssning eller övervakning eller inhämtning av uppgifter enligt inhämtningslagen.

Lokaliseringsuppgifter som inte är trafikuppgifter får som utgångspunkt behandlas endast sedan de har avidentifierats eller användaren eller abonnenten gett sitt samtycke till behandlingen. Även beträffande dessa uppgifter finns ett undantag som innebär att de får behandlas utan nyss nämnda begränsning om de omfattas av beslut om inhämtning av uppgifter enligt 27 kap. RB eller inhämtningslagen.

Brottsbekämpande myndigheter kan i princip endast begära ut trafikuppgifter och lokaliseringsuppgifter med stöd av ett beslut om hemlig övervakning eller hemlig avlyssning av elektronisk kommunikation. Beslut om hemliga tvångsmedel bryter igenom tystnadsplikten.

2021 års datalagringsutredning (Ju 2021:09) har i uppdrag att se över den lagstiftning som medför en skyldighet för tillhandahållare av elektroniska kommunikationstjänster att lagra uppgifter om elek-

tronisk kommunikation för brottsbekämpande syften. Uppdraget ska redovisas senast den 6 februari 2023.

Abonnemangsuppgifter

Uppgifter om abonnemang anses typiskt sett vara mindre integritetskänsliga än t.ex. trafik- och lokaliseringsuppgifter. Tillgången till abonnemangsuppgifter har inte heller bedömts utgöra ett hemligt tvångsmedel och regleras därför direkt i LEK.

Trots tystnadsplikten har en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet (Tullverket, Kustbevakningen eller Skatteverket) rätt att få tillgång till abonnemangsuppgifter, om uppgiften gäller misstanke om brott som myndigheten ska ingripa mot. Regleringen innebär att de brottsbekämpande myndigheterna i princip har rätt att hämta in abonnemangsuppgifter för att beivra alla typer av brott utom sådana som åtalas enbart av målsäganden.

4.3 Hemliga tvångsmedel

Tre allmänna principer gäller för all tvångsmedelsanvändning, nämligen ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Dessa principer gäller alltid vid beslut om, och tillämpning av, de hemliga tvångsmedlen. Enligt ändamålsprincipen får ett tvångsmedel användas endast för det ändamål som framgår av lagstiftningen. Behovsprincipen innebär att ett tvångsmedel får användas endast om det finns ett påtagligt behov och en mindre ingripande åtgärd är otillräcklig. Proportionalitetsprincipen innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden.

Rättegångsbalken (RB) innehåller inte någon definition av straffprocessuella tvångsmedel. Det rör sig dock om åtgärder som har en funktion inom straffprocessen men som inte är straff eller andra sanktioner. Åtgärderna utgör myndighetsutövning och är ett intrång i någons rättssfär. Vanligtvis innefattar användningen tvång mot person eller egendom (se t.ex. Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas?).

I förundersökning används straffprocessuella tvångsmedel i brottsutredande syfte eller för att en rättegång ska kunna genomföras. Exempel på sådana tvångsmedel är husrannsakan, kroppsvisitation, kroppsbesiktning, beslag, gripande, anhållande och häktning. En grundläggande förutsättning för att använda straffprocessuella tvångsmedel är normalt att en förundersökning har inletts. I vart fall inleds en förundersökning i samband med att en åtgärd vidtas, t.ex. ett gripande (se dock t.ex. 23 kap. 22 § RB). Under vissa förutsättningar får emellertid några av de brottsbekämpande myndigheterna använda hemliga tvångsmedel redan i underrättelseverksamhet. Detta görs då i syfte att förhindra särskilt allvarlig brottslighet. Med undantag för redogörelsen i avsnitt 4.3.3 om den inhämtning som kan ske enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) omfattar denna framställning endast användning av hemliga tvångsmedel under en förundersökning.

Bland de straffprocessuella tvångsmedlen intar de hemliga tvångsmedlen en särställning eftersom den berörde inte är medveten om att de används mot honom eller henne, men det antas att de äger rum mot hans eller hennes vilja.

Hemliga tvångsmedel under en förundersökning får endast användas om åtgärden är av synnerlig vikt för utredningen. De får däremot inte under en förundersökning användas i exempelvis enbart preventivt syfte. Förutsatt att åtgärden är av synnerlig vikt för utredningen och övriga förutsättningar är uppfyllda, har det dock ansetts förenligt med regeringsformens legalitetskrav att använda tvångsmedlet när detta även kan leda till andra positiva effekter, såsom att man kan förhindra att ett brott fullbordas (prop. 2013/14:237 Hemliga tvångsmedel mot allvarliga brott, s. 95 och 96).

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

direktivet). Dessa registerförfattningar innehåller regler till skydd för den personliga integriteten när personuppgifter behandlas i den brottsbekämpande verksamheten och när de överförs till annan verksamhet.

De hemliga tvångsmedlen är:

- hemlig avlyssning av elektronisk kommunikation
- hemlig övervakning av elektronisk kommunikation
- hemlig kameraövervakning
- hemlig rumsavlyssning, och
- hemlig dataavläsning.

Även kvarhållande (och kontroll) av försändelse enligt 27 kap. 9 § RB anses vara ett hemligt tvångsmedel eftersom den mot vilken åtgärden riktas inte känner till att så sker och det kan antas att den äger rum mot dennes vilja. Av samma skäl har också regeringen tidigare ansett att inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) utgör ett hemligt tvångsmedel (se prop. 2011/12:55 s. 111).

4.3.1 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. Tvångsmedlet kan tillämpas på alla former av kommunikation genom elektroniska kommunikationsnät och är tillämpligt på muntlig och skriftlig kommunikation, liksom även på datakommunikation.

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

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

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

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

4.3.2 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. Till skillnad från hemlig avlyssning av elektronisk kommunikation ger inte tvångsmedlet tillgång till uppgifter om innehållet i meddelanden. Det som kan hämtas in är i stället trafikuppgifter och uppgifter om lokalisering.

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

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

4.3.3 Inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet

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

4.3.4 Hemlig kameraövervakning

Hemlig kameraövervakning innebär att fjärrstyrda tv-kameror, andra optisk-elektroniska instrument eller därmed jämförbar utrustning används för optisk personövervakning vid förundersökning i brottmål utan att upplysning om övervakningen lämnas. I förarbetena till lagstiftningen om hemlig kameraövervakning förtydligas att tvångsmedlet inte omfattar ljudupptagning, se propositionen Hemlig kameraövervakning (prop. 1995/96:85 s. 37).

Tillstånd till hemlig kameraövervakning kan lämnas vid förundersökning som rör de brott som kan aktualisera tillstånd till hemlig avlyssning av elektronisk kommunikation (27 kap. 20 a § andra stycket RB). Övervakningen får som huvudregel användas endast om någon är skäligen misstänkt för brottet. Åtgärden får endast avse sådan plats där den skäligen misstänkte kan antas komma att uppehålla sig (27 kap. 20 b § RB). Om det inte finns någon skäligen misstänkt för brottet får hemlig kameraövervakning dock användas för att övervaka den plats där brottet har begåtts eller en nära omgivning till denna plats, dock endast om syftet är att fastställa vem som skäligen kan misstänkas för brottet (27 kap. 20 c §). Om en plats ska bli föremål för både hemlig rumsavlyssning och hemlig kameraövervakning får det meddelas ett tillstånd för polisen att bereda sig tillträde till en plats som annars är skyddad mot intrång för att installera tekniska hjälpmedel. Ett sådant tillstånd får inte avse installation av tekniska hjälpmedel i någons stadigvarande bostad.

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

4.3.5 Hemlig rumsavlyssning

Hemlig rumsavlyssning innebär avlyssning eller upptagning som görs i hemlighet, och med ett tekniskt hjälpmedel som är avsett att återge ljud, och avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte

har tillträde till. Rumsavlyssning får endast användas vid förundersökning avseende brott för vilket det inte är föreskrivet lindrigare straff än fängelse fyra år, spionerі, brott mot lagen (2018:558) om företagshemligheter som kan antas ha begåtts eller understötts av främmande makt samt för vissa andra särskilt uppräknade brott (t.ex. människohandel, våldtäkt mot barn, grovt övergrepp i rättssak) om det i det enskilda fallet kan antas att brottets straffvärde överstiger fängelse i fyra år (27 kap. 20 d § RB).

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

4.3.6 Hemlig dataavläsning

Den 1 april 2020 trädde lagen (2020:62) om hemlig dataavläsning i kraft. Lagen är tidsbegränsad till utgången av mars 2025. Hemlig dataavläsning är ett nytt hemligt tvångsmedel som kan användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll. Hemlig dataavläsning innebär att uppgifter som är avsedda för automatiserad behandling, i hemlighet och med ett tekniskt hjälpmedel läses av eller tas upp i ett avläsningsbart informationssystem. Tillstånd till hemlig dataavläsning kan enligt 2 § första stycket 1–5 lagen om hemlig dataavläsning omfatta en eller flera olika uppgiftstyper, nämligen kommunikationsavlyssnings-, kommunikationsövervaknings-, plats-, kameraövervaknings- och rumsavlyssningsuppgifter. Det handlar alltså om samma slags uppgifter som kan hämtas in med hjälp av de andra hemliga tvångsmedlen. Skillnaden är att hemlig dataavläsning tar sikte på uppgifter som finns eller kan avläsas i ett visst informationssystem. Medan hemlig avlyssning av elektronisk kommunikation sker genom att meddelanden fångas upp under överföring i kommunikationsnätet riktar sig hemlig dataavläsning av samma slags uppgifter mot ett visst informationssystem, såsom ett elektroniskt kommunikationsmedel eller ett virtuellt an-

vändarkonto. En hemlig kameraövervakning genomförs genom att kameror monteras på den plats som ska övervakas, medan motsvarande uppgifter kan hämtas in med hemlig dataavläsning genom att den brottsutredande myndigheten exempelvis aktiverar en mobiltelefons kamera.

Enligt punkterna 6 och 7 i den nyss nämnda paragrafen kan hemlig dataavläsning även avse lagrade uppgifter och uppgifter om hur ett avläsningsbart informationssystem används, förutsatt att uppgifterna inte är sådana som avses i punkterna 1–5.

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

Liksom när det gäller andra hemliga tvångsmedel är viss verksamhet fredad från hemlig avläsning (11 §). Det gäller framför allt viss yrkesmässig tystnadsplikt, såsom tystnadsplikten för advokater, läkare och präster. Tillstånd till hemlig dataavläsning får inte avse ett avläsningsbart informationssystem som stadigvarande används eller är avsett att användas i sådan verksamhet.

Den verkställande myndigheten får efter särskilt tillstånd och under närmare angivna förutsättningar i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång (12 §). Tillträdestillståndet får inte avse en plats där hemlig dataavläsning inte får förekomma enligt 11 § (13 §).

Hemlig dataavläsning under en förundersökning får endast användas vid en förundersökning om brott av det slag som kan föranleda hemlig avlyssning av elektronisk kommunikation under en förundersökning (4 § första stycket). Åtgärden måste, i likhet med vad som gäller i fråga om andra hemliga tvångsmedel, vara av synnerlig vikt för utredningen.

Som huvudregel får ett tillstånd till hemlig dataavläsning under en förundersökning endast avse ett informationssystem som används, eller som det finns särskild anledning att anta har använts eller kommer att användas, av någon som är skäligen misstänkt för brottet. Om åtgärden gäller kommunikationsavlyssnings-, kommunikationsövervaknings- eller platsuppgifter får åtgärden även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har kontaktat eller kommer att kontakta. Ett tillstånd som gäller kamera-

övervakningsuppgifter får endast avse en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats får dock inte vara någons stadigvarande bostad. (4 § andra–fjärde stycket).

I vissa fall får hemlig dataavläsning under en förundersökning även användas för att utreda vem som skäligen kan misstänkas för ett brott (5 §). Denna möjlighet finns i fråga om avläsning som gäller kommunikationsövervaknings- eller platsuppgifter. I ett sådant fall får dock avläsning eller upptagning av kommunikationsövervakningsuppgifter endast avse förfluten tid. Detta motsvarar vad som gäller i fråga om hemlig övervakning av elektronisk kommunikation i samma syfte.

Om en begäran om tillstånd till hemlig dataavläsning avser rumsavlyssningsuppgifter får begäran beviljas endast vid en förundersökning om sådana brott som kan omfattas av ett tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § RB. Sådan hemlig dataavläsning får användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Om platsen är någon annan stadigvarande bostad än den misstänktes, får tillstånd till hemlig dataavläsning beviljas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. Hemlig dataavläsning som avser rumsavlyssningsuppgifter får aldrig användas på en plats dit tillträdestillstånd inte får beviljas.

I 10 § regleras att tillstånd till hemlig dataavläsning i vissa fall får beviljas för avläsning eller upptagning av uppgifter i underrättelseverksamhet (inhämtningsfallen). I dessa fall får hemlig dataavläsning endast avse kommunikationsövervakningsuppgifter och platsuppgifter.

Hemlig dataavläsning kan även i vissa andra fall användas utanför en förundersökning. Vi går inte närmare in på dessa bestämmelser.

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

4.4.1 Domstolsprövning

I förundersökningsfallen gäller som utgångspunkt att en domstol ska pröva frågor om hemliga tvångsmedel. Ansökan görs av åklagaren när det gäller hemlig avlyssning av elektronisk kommunikation,

hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning (27 kap. 21 § RB och 14 § lagen om hemlig dataavläsning).

I förundersökningsfallen finns möjlighet för åklagare att i vissa fall besluta om tillstånd till hemliga tvångsmedel interimistiskt, i avvaktan på rättens beslut. Om åklagaren har gett ett sådant tillstånd ska denne utan dröjsmål skriftligt anmäla beslutet till rätten och ange skälen för åtgärden. Rätten ska skyndsamt pröva ärendet och om den finner att det inte finns skäl för åtgärden ska beslutet upphävas. Om åklagarens beslut har verkställts innan rätten hunnit göra en sådan prövning och det senare visar sig att det saknats skäl för åtgärden får de inhämtade uppgifterna inte användas i en brottsutredning till nackdel för den som har omfattats av avlyssningen eller övervakningen, eller för någon annan som uppgifterna avser (27 kap. 21 a § RB och 17 § lagen om hemlig dataavläsning).

Det är inte möjligt att utan domstolsprövning tillåta hemlig rumsavlyssning. I konsekvens med detta är det inte heller tillåtet för åklagaren att fatta interimistiskt beslut om hemlig dataavläsning som gäller rumsavlyssningsuppgifter (17 § första stycket lagen om hemlig dataavläsning). Undantag avseende hemlig rumsavlyssning gäller dock i vissa situationer om Sverige befinner sig i krig eller krigsfara. Enligt 28 § lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. gäller nämligen att om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig rumsavlyssning enligt 27 kap. 20 d § RB, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.

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

För att hemliga tvångsmedel ska få tillåtas ställs det också upp vissa kvalificerande krav som tar sikte på behovet av åtgärden i det enskilda fallet. I förundersökningsfallen krävs det att åtgärden är av synnerlig vikt för utredningen.

4.4.2 Beslutets innehåll

Vad ett beslut om hemliga tvångsmedel ska innehålla under en förundersökning regleras i 27 kap. 21 § RB respektive 18 § lagen om hemlig dataavläsning. I underrättelseverksamhet finns motsvarande regler i 8 § preventivlagen och 21 § LSU (vilken hänvisar till 27 kap. RB). I beslutet ska det anges vilken tid beslutet gäller. Tiden får inte bestämmas längre än nödvändigt och får inte överstiga en månad från dagen för beslutet. Om tiden löper ut krävs ett nytt beslut.

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

I ett tillstånd till hemlig dataavläsning ska det anges vilket avläsningsbart informationssystem tillståndet avser och vilken typ av uppgift som får läsas av eller tas upp (18 § första stycket 2 och 3 lagen om hemlig dataavläsning). Om tillståndet avser en plats ska även platsen anges och även ett eventuellt tillträdestillstånd ska anges i beslutet (andra stycket samma paragraf). Vid en åtgärd som gäller rumsavlyssningsåtgärder ska det även anges vem som är skäligen misstänkt för brottet (första stycket 5 samma paragraf).

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

I samtliga fall gäller att rätten också, när det finns skäl till det, i övrigt ska ange villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Vid hemlig dataavläsning är dock skyldigheten obligatorisk.

Vid beslut om inhämtning av uppgifter enligt inhämtningslagen ska det anges vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet avser.

4.4.3 Skydd för vissa yrkesgrupper

Vissa personkategorier är till följd av sitt yrke undantagna från vittnesplikten under vissa förutsättningar (36 kap. 5 § andra–sjätte styckena RB). Detta gäller bl.a. advokater, präster och läkare. Dessa personer har även en priviligierad ställning vid hemlig avlyssning av elektronisk kommunikation och hemlig rumsavlyssning. Det finns nämligen särskilda bestämmelser om användningen av dessa hemliga tvångsmedel när den som tvångsmedlet riktas mot kommunicerar med någon i den nyss nämnda personkretsen (27 kap. 22 § RB). Hemlig avlyssning av elektronisk kommunikation får inte avse telefonsamtal eller andra meddelanden där någon som yttrar sig inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram. På motsvarande sätt får hemlig rumsavlyssning inte avse samtal eller annat tal där en sådan person talar. Om det under avlyssningen kommer fram att det är fråga om ett sådant samtal eller meddelande, ska avlyssningen omedelbart avbrytas och upptagningar och uppteckningar, dvs. det material där uppgifter från tvångsmedelsanvändningen finns sparat, omedelbart förstöras i de delar som de omfattas av förbud. Motsvarande bestämmelse beträffande hemlig avlyssning av elektronisk kommunikation finns i preventivlagen (11 §). I praktiken är begränsningen mindre omfattande än den kan förefalla, eftersom avlyssning i de flesta fall är tillåten vid allvarliga brott. Ett absolut skydd gäller bara i fråga om försvarare, präster och andra personer med motsvarande ställning i ett trossamfund (se vidare i avsnitt 6.13).

Hemlig dataavläsning får inte avse uppgifter som omfattas av beslagsförbudet enligt 27 kap. 2 § RB. Hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter får inte avse uppgifter i telefonsamtal, samtal eller andra meddelanden eller tal där någon som yttrar sig, på grund av bestämmelserna om undantag från vittnesplikten, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram. Om det under verkställigheten kommer fram uppgifter av angivet slag ska verkställigheten omedelbart avbrytas och upptagningar och uppteckningar omedelbart förstöras i de delar de omfattas av förbudet.

4.4.4 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 i fall enligt inhämtningslagen, där i stället den brottsbekämpande myndigheten själv ska häva beslutet (27 kap. 23 § RB, 10 § preventivlagen och 4 § inhämtningslagen). Tillstånd till hemlig dataavläsning upphävs av rätten eller den som ansökt om åtgärden (20 § andra stycket lagen om hemlig dataavläsning).

4.4.5 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. Detsamma gäller hemlig dataavläsning, förutom om den gäller rumsavlyssningsuppgifter (28 § första stycket lagen om hemlig dataavläsning). En förundersökning eller motsvarande utredning om brottet får dock inledas på grund av sådana uppgifter endast om det är föreskrivet fängelse i ett år eller därutöver för brottet och det kan antas att brottet inte endast leder till böter, eller om det finns särskilda skäl.

Överskottsinformation från hemlig rumsavlyssning eller hemlig dataavläsning som gäller rumsavlyssningsuppgifter får användas för att utreda brott endast om uppgifterna rör ett brott som hade kunnat leda till tillstånd till hemlig rumsavlyssning eller som har minst tre års fängelse i straffskalan. I annat fall får uppgifterna inte användas för brottsutredande ändamål, vare sig för att inleda en förundersökning eller som tillägg till en redan pågående förundersökning (27 kap. 23 a § RB och 28 § första stycket lagen om hemlig dataavläsning).

Frågan om hur överskottsinformation ska få användas är föremål för överväganden inom Regeringskansliet (SOU 2018:61 Rättssäkerhetsgarantier och hemliga tvångsmedel).

4.4.6 Granskning, bevarande och förstörande av insamlat material

När hemliga tvångsmedel använts ska den upptagning eller uppteckning som gjorts granskas snarast möjligt. När det är fråga om hemliga tvångsmedel under förundersökning får rätten, förundersökningsledaren eller åklagaren, alternativt sakkunnig eller annan som någon av dessa bestämt, genomföra granskningen. De delar som är av betydelse för att utreda brott ska bevaras till dess förundersökningen har lagts ned eller avslutats eller, om åtal väckts, målet slutligt har avgjorts. I de delar som upptagningarna och uppteckningarna är av betydelse för att förhindra förestående brott ska de bevaras så länge det behövs för att förhindra brott. De ska därefter förstöras (27 kap. 24 § RB och 28 § första stycket lagen om hemlig dataavläsning).

4.4.7 Offentliga ombud

Offentliga ombud bevakar enskildas integritetsintressen i ärenden hos domstol om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning. Samma regler om offentliga ombud gäller för förundersökningsfallen som för underrättelsefallen (27 kap. 26–30 §§ RB, 6 § preventivlagen, 21 § LSU och 16 § lagen om hemlig dataavläsning). Däremot finns det inte några regler om offentligt ombud vid hemlig övervakning av elektronisk kommunikation. Inte heller finns det krav på offentligt ombud vid tillämpning av inhämtningslagen.

Ett offentligt ombud har rätt att ta del av vad som förekommer i ärendet, yttra sig i ärendet och överklaga rättens beslut (27 kap. 26 § RB). När en ansökan eller anmälan om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning har kommit in till rätten ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla sammanträde. Vid sammanträdet ska åklagaren och det offentliga ombudet närvara (27 kap. 28 § RB). Vid ett sammanträde om hemlig dataavläsning ska den som gjort ansökan eller anmälan och det offentliga ombudet närvara (16 § första stycket lagen om hemlig dataavläsning).

4.4.8 Underrättelse till enskilda

Det finns en skyldighet att i efterhand underrätta den enskilde om att hemliga tvångsmedel har använts. I förundersökningsfallen gäller som huvudregel att den som är eller har varit misstänkt för brott ska underrättas om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning eller hemlig rumsavlyssning som han eller hon har utsatts för (27 kap. 31 § RB).

Om hemlig avlyssning eller övervakning av elektronisk kommunikation har avsett ett telefonnummer, en adress eller kommunikationsutrustning som innehas av någon annan än den misstänkte ska enligt huvudregeln även denna person underrättas. Om hemlig kameraövervakning eller hemlig rumsavlyssning har avsett en plats som innehas av någon annan än den misstänkte och som allmänheten inte har tillträde till, ska även innehavaren av platsen underrättas. En underrättelse ska lämnas så snart det kan ske utan men för utredningen, dock senast en månad efter det att förundersökningen avslutades (27 kap. 31 § RB).

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

Bestämmelserna om underrättelse till en enskild vid hemlig dataavläsning under förundersökning går ut på att rättegångsbalkens bestämmelser för motsvarande slags uppgifter ska tillämpas (28 § andra stycket lagen om hemlig dataavläsning). Med andra ord ska rättegångsbalkens bestämmelser om hemlig kameraövervakning tillämpas för hemlig dataavläsning som avser kameraövervakningsuppgifter, osv. Dock ska Säkerhets- och integritetsskyddsnämnden alltid underrättas när rätten har beslutat i frågor om hemlig dataavläsning (21 § samma lag).

4.4.9 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 och förordningen (2007:1141) med instruktion för Säkerhets- och integritetsskyddsnämnden.

Nämnden ska bl.a. utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och därmed sammanhängande verksamhet. Tillsynen ska särskilt syfta till att säkerställa att verksamheten bedrivs i enlighet med lag eller annan författning och ska utövas genom inspektioner och andra undersökningar. Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan författning avhjälps. Nämnden är också skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel samt om användningen av tvångsmedlen och därmed sammanhängande verksamhet har skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde om att kontrollen har utförts.

Som framgår i föregående avsnitt ska Säkerhets- och integritetsskyddsnämnden få underrättelse från åklagaren i de fall underrättelse till enskild har underlåtits på grund av sekretess. Säkerhets- och integritetsskyddsnämnden ska också underrättas om beslut om inhämtning enligt inhämtningslagen (5 §) och beslut i frågor om hemlig dataavläsning (21 § lagen om hemlig dataavläsning).

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

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

I 1 kap. 2 § räknas upp alla de åtgärder som omfattas av lagen, t.ex. förhör under förundersökning, beslag och olika hemliga tvångs-

medel. En uttalad målsättning med lagen är att svenska åklagare och domstolar ska kunna lämna rättslig hjälp till utländska myndigheter med alla de åtgärder som kan vidtas vid en svensk förundersökning eller rättegång, se propositionen Internationell rättslig hjälp i brottmål (prop. 1999/2000:61 s. 79 och 80). När ett nytt tvångsmedel införts i nationell rätt har det också införts motsvarande bestämmelser i lagen om internationell rättslig hjälp i brottmål, se propositionen Hemlig rumsavlyssning (prop. 2005/06:178 s. 89).

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

I 4 kap. 25–28 b §§ LIRB finns detaljerade bestämmelser om handläggningen av dessa ärenden och verkställigheten av ett hemligt tvångsmedel, t.ex. om granskning och underrättelse till enskild vid verkställighet i Sverige och om att åklagaren i vissa fall måste inhämta rättens tillstånd till åtgärden. Mot bakgrund av Europeiska unionens konvention om ömsesidig rättslig hjälp i brottmål mellan Europeiska unionens medlemsstater från 2000 (SÖ 2005:42) finns vissa bestämmelser i lagen som rör hemliga tvångsmedel, som avviker från det traditionella sättet att samarbeta när en stat ansöker om hjälp i en annan stat som efter en prövning verkställer åtgärden där. Dessa bestämmelser gäller endast gentemot en medlemsstat i Europeiska unionen, Island eller Norge.

En sådan särreglering är tekniskt bistånd med hemlig avlyssning eller övervakning av elektronisk kommunikation eller med hemlig dataavläsning. Tekniskt bistånd innebär att avlyssningen, övervakningen eller avläsningen görs gentemot någon som finns i en annan stat än den som bistår med avlyssningen eller övervakningen och då meddelandena eller uppgifterna om meddelandena, under betryggande former, omedelbart kan överföras till den ansökande staten. Det kan t.ex. röra sig om svenska myndigheter som bistår tyska myndigheter med att avlyssna någon som finns i Danmark. För ett sådant bistånd gäller särskilda förutsättningar (4 kap. 25 b § andra stycket 3 och

fjärde stycket och 28 e §). Omedelbar överföring av meddelanden eller uppgifter om meddelanden kan också äga rum när den som avlyssnas eller övervakas finns i Sverige (4 kap. 25 a §).

En annan särreglering i lagen gäller tillstånd till gränsöverskridande hemlig avlyssning eller övervakning av elektronisk kommunikation eller gränsöverskridande hemlig dataavläsning (4 kap. 26 a–c och 28 f §§). Det är i egentlig mening inte fråga om att något bistånd lämnas, utan att en tillåtelse lämnas till att en stat avlyssnar eller övervakar en person som finns i den stat som lämnar tillståndet. Det kan t.ex. röra sig om att svenska myndigheter tillåter att danska myndigheter avlyssnar någon som finns i Sverige. I dessa fall gäller samma förutsättningar som för motsvarande åtgärd i rättegångsbalken (4 kap. 26 a § tredje stycket). Om ansökan avser tillstånd till gränsöverskridande hemlig dataavläsning enligt 2 § första stycket 1 och 2 lagen om hemlig dataavläsning tillämpas det som gäller för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation enligt 26 a § första och andra styckena och 26 b §. De förutsättningar som gäller enligt 1–6, 11, 14 och 18 §§ lagen om hemlig dataavläsning tillämpas vid tillståndsprövningen. Rätten ska även tillämpa motsvarande förfarande som anges i 16 § den lagen.

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

4.6 Lagen (2017:1000) om en europeisk utredningsorder

Europaparlamentets och rådets direktiv 2014/41/EU av den 3 april 2014 om en europeisk utredningsorder på det straffrättsliga området ersätter samarbetet mellan EU:s medlemsstater som tidigare skedde enligt bestämmelserna om internationell rättslig hjälp i brottmål (se föregående avsnitt). Direktivet genomfördes i huvudsak genom lagen

(2017:1000) om en europeisk utredningsorder. Lagen gäller i förhållande till alla EU-medlemsstater utom Danmark och Irland (1 kap. 2 §). Gentemot dessa två stater tillämpas lagen om internationell rättslig hjälp i brottmål. En europeisk utredningsorder innebär – något förenklat – att en åklagare eller domstol i den stat där brottsutredningen eller rättegången pågår beslutar om att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning.

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

En europeisk utredningsorder avseende hemliga tvångsmedel får utfärdas i Sverige av åklagare om de förutsättningar som gäller för att vidta utredningsåtgärden under en svensk förundersökning är uppfyllda och åtgärden är proportionerlig (2 kap. 1 och 3 §§). Dessutom krävs att domstol har lämnat tillstånd att utfärda ordern. Åklagaren har dock viss möjlighet att fatta interimistiska beslut. När det gäller hemlig avlyssning eller övervakning av elektronisk kommunikation kan en utredningsorder utfärdas för avlyssning eller övervakning i Sverige eller i en annan medlemsstat, såväl i den medlemsstat till vilken ordern översänds som i en tredje medlemsstat (2 kap. 17 §).

Liksom i lagen om internationell rättslig hjälp i brottmål kan det bli aktuellt med omedelbart överförande av meddelanden eller uppgifter om meddelanden (även om begreppet tekniskt bistånd inte används). I de fall ett sådant överförande är möjligt och upptagningen eller upptecknin gen sker i Sverige tillämpas 27 kap. 31–33 §§ rättegångsbalken om underrättelse till enskild. Vid samtliga hemliga tvångsmedel, även hemlig kameraövervakning och hemlig rumsavlyssning, tillämpas 27 kap. 22–24 §§ samma balk om t.ex. granskning.

När en europeisk utredningsorder avseende hemliga tvångsmedel har utfärdats i en annan medlemsstat och sänts över till Sverige är utgångspunkten att den ska erkännas och verkställas här (3 kap. 1 §). Det krävs dock att den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag och att övriga förutsättningar som

gäller för en motsvarande åtgärd i en svensk förundersökning är uppfyllda. En utredningsorder ska inte respektive behöver inte heller erkännas och verkställas om en vägransgrund i 3 kap. 5–7 §§ är tillämplig. En utredningsorder avseende hemliga tvångsmedel handläggs av åklagare, men domstol prövar om utredningsordern ska erkännas och verkställas (3 kap. 8 och 9 §§). Åklagaren har viss möjlighet att fatta interimistiska beslut om erkännande och verkställighet (3 kap. 10 §). Om utredningsordern kan erkännas och verkställas i Sverige, ska beslut meddelas om att verkställighet ska äga rum, en s.k. verkställbarhetsförklaring (3 kap. 19 §). För verkställigheten av utredningsordern finns särskilda bestämmelser om hemliga tvångsmedel i 3 kap. 34–37 §§.

Liksom i lagen om internationell rättslig hjälp i brottmål finns, beträffande hemlig avlyssning och övervakning av elektronisk kommunikation och hemlig dataavläsning, möjlighet till omedelbar överföring till den andra staten (3 kap. 38 och 37 a §). 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 §§).

Det finns också särskilda regler om underrättelse till annan medlemsstat och om underrättelse från annan medlemsstat till Sverige när hemlig avlyssning eller övervakning av elektronisk kommunikation kan ske på den andra statens territorium utan bistånd från denna (4 kap. 12–15 §§). Det som anges om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation tillämpas även för hemlig dataavläsning som avser kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter (4 kap. 16 §).

4.7 Sekretessfrågor

Enligt 2 kap. 1 § tryckfrihetsförordningen har, till främjande av ett fritt meningsutbyte och en fri och allsidig upplysning och ett fritt konstnärligt skapande, var och en rätt att ta del av allmänna handlingar. Rätten får dock begränsas bl.a. om det krävs med hänsyn till intresset att förebygga eller beivra brott och skyddet för enskildas personliga eller ekonomiska förhållanden (2 kap. 2 § första stycket tryckfrihetsförordningen). Regler om sådana begränsningar finns i offentlighets- och sekretesslagen (2009:400), förkortad OSL. Lagen

innehåller bestämmelser som är av särskild betydelse när reglerna om hemliga tvångsmedel ska beskrivas.

Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs (18 kap. 1 § OSL).

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

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

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

avlyssning av elektronisk kommunikation eller med hemlig övervakning av elektronisk kommunikation enligt 4 kap. 25 b § LIRB.

4.8 Användningen av hemliga tvångsmedel

Varje år redovisar regeringen användningen av hemliga tvångsmedel i en skrivelse till riksdagen. Skrivelsen baseras på Åklagarmyndighetens årliga redovisning, vilken myndigheten sammanställer tillsammans med Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen och Tullverket. Redovisningen innehåller bl.a. uppgifter om antalet meddelade tillstånd om hemliga tvångsmedel, hur många personer som varit föremål för åtgärder och om uppgifterna som kommit fram gjort nytta. Det framgår av redovisningarna att hemliga tvångsmedel används i en mycket liten del av alla förundersökningar. Användningen under 2020 har redovisats i skr. 2021/22:79.

5 Relevanta straffskärpningar

5.1 Genomförda straffskärpningar

Under de senaste åren har det genomförts ett antal straffskärpningar som lett till att hemliga tvångsmedel kan användas i fler fall än tidigare.

Den 1 juli 2016 genomfördes omfattande skärpningar i den straffrättsliga lagstiftningen i syfte att mer effektivt motverka organiserad brottslighet (prop. 2015/16:113 Bättre straffrättsliga verktyg mot organiserad brottslighet). Lagändringarna innebar bl.a. att försök, förberedelse och stämpling till allvarliga brott kriminaliserades i större utsträckning än tidigare. Det gäller bl.a. grovt olaga hot, grov utpressning, övergrepp i rättssak, grovt övergrepp i rättssak samt grovt och synnerligen grovt vapenbrott. Vidare infördes regler om ytterligare omständigheter som särskilt ska beaktas vid bedömningen av om ett brott är grovt. Bland annat ska det vid vissa brott med hotinslag särskilt beaktas om gärningen har innefattat hot som påtagligt har förstärkts med hjälp av vapen, sprängämne eller vapenattrapp eller genom anspelning på ett våldskapital eller om gärningen annars har varit av allvarligt slag. Bestämmelsen om straff för förberedelse och stämpling ändrades på så sätt att högre straff än fängelse i två år ska kunna dömas ut i fler fall. Skärpningarna innebär att hemliga tvångsmedel kan användas i fler fall, i synnerhet vid misstanke om förberedelse eller stämpling.

Den 1 juli 2016 infördes också brotten synnerligen grovt narkotikabrott och synnerligen grov narkotikasmuggling med ett minimistraff om sex års fängelse. Lagändringarna innebar att straffen skärptes bl.a. för gärningar som avser hantering av synnerligen stora mängder narkotika (prop. 2015/16:111 Synnerligen grova narkotikabrott). Straffskalan för de synnerligen grova brotten vidgade förutsättningarna för att tillgripa hemlig rumsavlyssning.

Genom lagändringar som trädde i kraft den 1 juli 2017 skärptes vidare straffskalorna för grov misshandel, synnerligen grov misshandel, grovt olaga tvång, grovt olaga hot, grovt rån och grov utpressning (prop. 2016/17:108 Straffskalorna för vissa allvarliga våldsbrott). De höjda minimistraffen för grov misshandel och grov utpressning antogs vid införandet innebära att fler gärningar än tidigare kommer att anses ha ett straffvärde överstigande två års fängelse och därmed möjliggöra användning av hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning med stöd av straffvärdeventilen i respektive bestämmelse (anförd prop. s. 48).

År 2017 genomfördes flera lagändringar som tar sikte på regleringen av förmögenhetsbrott i allmänhet. Bland annat gavs förekomsten av integritetskränkande inslag större vikt vid bedömningen av om brotten skadegörelse och stöld ska anses vara grova och efter en översyn av straffskalorna för förmögenhetsbrott skärptes straffen för skadegörelse och grov skadegörelse för att bättre överensstämma med vad som gäller för andra brott. För skadegörelse skärptes straffskalan från böter eller fängelse i högst ett år till enbart fängelse i högst två år. För grov skadegörelse skärptes straffskalan från fängelse i högst fyra år till fängelse i lägst sex månader och högst sex år. Straffskärpningen avseende grov skadegörelse innebär att hemlig övervakning av elektronisk kommunikation kan förekomma och även, med stöd av respektive straffvärdeventil, hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning. För att komma till rätta med omfattande systematiska förfaranden avseende s.k. bluffakturor infördes samtidigt en straffbestämmelse om grovt fordringsbedrägeri i brottsbalken. Straffskalan är fängelse i lägst sex månader och högst sex år, vilket innebär att hemlig övervakning av elektronisk kommunikation kan användas och om straffvärdet överstiger två år även hemlig avlyssning av elektronisk kommunikation m.m. med stöd av respektive straffvärdeventil.

Den 1 januari 2018 trädde ett antal lagändringar i kraft som innebar att straffskalorna för vapenbrott och brott mot tillståndsplikten för explosiva varor skärptes i flera avseenden (prop. 2017/18:26 Skjutvapen och explosiva varor – skärpta straff för de grova brotten). Ändringarna gick ut på att straffskalorna för grovt vapenbrott och grovt brott mot tillståndsplikten för explosiva varor ändrades från fängelse i lägst ett och högst fyra år till fängelse i lägst två och högst fem år, att minimistraffen för de synnerligen grova brotten höjdes från fängelse

i tre år till fängelse i fyra år, och att straffmaximum för vapenbrott och brott mot tillståndsplikten för explosiva varor av normalgraden ändrades från fängelse i två år till fängelse i tre år. Ändringarna innebär att hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning kan användas i fler fall som avser grovt brott och att hemlig rumsavlyssning kan användas i fråga om de synnerligen grova brotten.

I januari 2020 infördes ett stärkt straffrättsligt skydd för blåljusverksamhet (prop. 2018/19:155 Ett stärkt straffrättsligt skydd för blåljusverksamhet och myndighetsutövning). I lagstiftningsärendet konstaterades att det på flera orter runt om i Sverige förekommer återkommande angrepp på polis, räddningstjänst och ambulanssjukvård. För att stärka det straffrättsliga skyddet infördes ett nytt brott i brottsbalken, sabotage mot blåljusverksamhet. Gärningarna var redan straffbelagda som exempelvis misshandel, olaga hot eller hot eller våld mot tjänsteman, men regeringen ville åstadkomma en påtaglig straffhöjning för det aktuella sortens gärningar. Straffet är fängelse i högst fyra år och för grovt sabotage mot blåljusverksamhet fängelse på viss tid, lägst två och högst 18 år, eller på livstid. För att stärka det straffrättsliga skyddet för myndighetsutövning skärptes samtidigt straffskalan för grovt våld eller hot mot tjänsteman till fängelse i lägst ett och högst sex år. Straffskärpningarna innebär att det i fler fall kan vara möjligt att använda hemliga tvångsmedel.

Den 1 december 2020 höjdes maximistraffet för synnerligen grovt vapenbrott och synnerligen grovt brott mot tillståndsplikten för explosiva varor från fängelse i sex år till fängelse i sju år. Samtidigt blev vapensmuggling och smuggling av explosiva varor egna brott med strängare straffskalor än för vanliga smugglingsbrott. Straffskalorna för de nya brotten motsvarar straffskalorna för vapenbrott och brott mot tillståndsplikten för explosiva varor (prop. 2019/20:200 En strängare syn på hantering av vapen och explosiva varor). Minimistraffet för grov smuggling av vapen respektive explosiva varor innebär att det numera är möjligt att bedriva hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning som inte avser rumsavlyssningsuppgifter med stöd av huvudregeln i respektive bestämmelse. Även lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet har blivit tillämplig. Minimistraffet för de synnerligen grova smugglingsbrotten innebär att det

för dessa brott också är möjligt att tillgripa hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

Under senare år har ett antal lagändringar skett för att bekämpa penningtvätt och finansiering av terrorism, både på det administrativa och på det straffrättsliga området. De straffrättsliga bestämmelser som i huvudsak är av relevans i nuvarande sammanhang återfinns i lagen (2014:307) om straff för penningtvättsbrott. I denna finns bl.a. bestämmelser som straffbelägger penningtvättsbrott och grovt penningtvättsbrott med fängelse i högst två år respektive fängelse i lägst sex månader och högst sex år. Det grova brottet kan föranleda hemlig övervakning av elektronisk kommunikation och, med stöd av straffvärdeventilerna, hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning som inte avser rumsavlyssningsuppgifter.

I januari 2020 utvidgades bidragsbrottslagens (2007:612) tillämpningsområde till att även avse stöd, bidrag och ersättningar som enligt lag eller förordning beslutas av Försäkringskassan, Arbetsförmedlingen eller en kommun och som avser en enskild person, men betalas ut till eller tillgodoräknas någon annan än den enskilde (ekonomiskt stöd). Dessutom skärptes maximistraffet för grovt bidragsbrott från fängelse i fyra år till sex år. Den övre delen av straffskalan angavs därvid i första hand vara avsedd att tillämpas vid kvalificerad och omfattande brottslighet riktad mot välfärdssystemen, t.ex. vid organiserad brottslighet som rör mycket stora belopp. I sammanhanget bör nämnas att regeringen i juni 2021 tillsatte en utredning (S 2021:03) för att göra en översyn av möjligheterna att stärka arbetet med att bekämpa bidragsbrott som riktas mot Försäkringskassan, Pensionsmyndigheten, Centrala studiestödsnämnden, Migrationsverket och Arbetsförmedlingen. Syftet är att säkerställa en ändamålsenlig och effektiv hantering för att därigenom minska antalet felaktiga utbetalningar och bidragsbrott i de ekonomiska förmåner och stöd som hanteras av myndigheterna. Uppdraget ska slutredovisas i augusti 2023.

I mars 2021 infördes bestämmelser som innebär att det vid bedömningen av om ett stöld- eller häleribrott är grovt särskilt ska beaktas om gärningen har ingått som ett led i en brottslighet som utövats systematiskt (prop. 2020/21:52 Tillträdesförbud till butik och förstärkt straffrättsligt skydd mot tillgreppsbrottslighet). I propositionen anfördes det bl.a. att lagändringen kan göra det mindre attraktivt för internationella brottsnätverk att verka i Sverige. Ändringen kan

innebära att fler brott rubriceras som grova, vilket i sin tur innebär att bl.a. hemlig avlyssning av elektronisk kommunikation med stöd av straffvärdeventilerna aktualiseras i fler fall. Samtidigt infördes en ny straffbestämmelse om inbrottsstöld. Brottet omfattar stöld som har skett efter intrång i bostad eller annat liknande boende och straffet är fängelse i lägst ett och högst sex år. Dessa lagändringar gäller sedan mars 2021.

Den 1 januari 2022 höjdes minimistraffet för grov fridskränkning och grov kvinnofridskränkning från fängelse i nio månader till fängelse i ett år. Straffskärpningen skulle kunna ha en viss påverkan på möjligheten att med stöd av respektive straffvärdeventil använda främst hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter.

Den 1 juli 2022 införs ett grovt djurplågeribrott i brottsbalken. Straffskalan fängelse i lägst sex månader och högst fyra år. Straffskalan innebär att hemlig övervakning av elektronisk kommunikation blir möjlig. Övriga tvångsmedel, förutom hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter, blir möjliga om respektive straffvärdeventil är tillämplig (prop. 2021/22:18, Brott mot djur – skärpta straff och ett mer effektivt sanktionssystem).

Den 24 februari 2022 beslutades prop. 2021/22:133 En samlad straffrättslig terrorismlagstiftning. I propositionen föreslås vissa straffskärpningar. Samtliga dessa brott omfattas av brottskatalogen i 27 kap. 2 § RB (27 kap. 18 § enligt prop. 2021/22:119 Modernare regler för användningen av tvångsmedel). Det straffbara området för brotten utvidgas, vilket påverkar möjligheten att tillgripa hemliga tvångsmedel.

5.2 Pågående lagstiftningsärenden

Utöver de lagändringar som redovisats i det föregående finns det anledning att kortfattat nämna vissa pågående lagstiftningsarbeten som kan leda till straffskärpningar som påverkar tillämpningsområdet för hemliga tvångsmedel. Förslag till sådana straffskärpningar lämnas i lagrådsremisserna Ett särskilt brott för hedersförtryck, En stärkt rättsprocess och en ökad lagföring, Skärpt straff för gravfridsbrott, Skärpta straff för knivbrott, Skärpt syn på våldtäkt och andra sexuella kränkningar och Ett modernare straffrättsligt skydd mot hemfridsbrott och olaga intrång samt betänkandena Skärpta straff för

brott i kriminella nätverk (SOU 2021:68) och En skärpt syn på brott mot journalister och utövare av vissa samhällsnyttiga funktioner (SOU 2022:2).

Vi har inte haft möjlighet att beakta material som publicerats efter den 28 februari 2022.

6 Straffvärdeventiler vid flerfaldig brottslighet

6.1 Uppdraget

Det krävs misstanke om ett konkret brott vars straffvärde kan antas överstiga två års fängelse för att hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning ska få användas under en förundersökning med stöd av den s.k. straffvärdeventilen i respektive bestämmelse (27 kap. 18 och 20 a §§ RB). Det är emellertid inte möjligt att använda tvångsmedlen vid misstanke om flera brott där det sammanlagda straffvärdet kan antas vara högt, men där samtliga ingående enskilda brott kan betraktas som mindre allvarliga.

Som en konsekvens av hur dagens regler är utformade kan i normalfallet misstankar om systematisk brottslighet bestående av t.ex. flera skattebrott, stölder eller bedrägerier falla utanför tillämpningsområdet för dessa hemliga tvångsmedel. I utredningsdirektiven framhålls att de ovan angivna brottstyperna utgör exempel på vad som kan vara viktiga inkomstkällor för kriminella, enligt Brottsförebyggande rådets (Brå) rapport Kriminella nätverk och grupperingar – Polisers bild av maktstrukturer och marknader (rapport 2016:12 s. 87, 99–102 och 114–119). När det gäller den ekonomiska brottsligheten anges det i direktiven att det är vanligt med brottsupplägg som omfattar flera olika brott. Det kan t.ex. handla om brott som begås i ett och samma bolag eller en individ som begår samma brott i flera olika bolag. Det framhålls att dessa typer av brott, som sedda för sig inte alltid är särskilt allvarliga, utgör en inkomstkälla för nätverk som ägnar sig åt betydligt allvarligare brottslighet än så.

Straffvärdeventilen i bestämmelsen om hemlig rumsavlyssning är utformad på så sätt att det krävs att brottets straffvärde kan antas överstiga fängelse i fyra år och att det dessutom är fråga om ett brott som räknas upp i en katalog i paragrafen (27 kap. 20 d § RB).

Mot denna bakgrund är vårt uppdrag att

- ta ställning till om det bör införas en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning vid misstanke om flera brott vars samlade straffvärde kan antas överstiga ett visst straff,
- ta ställning till i vilka situationer och vid vilka straffvärden en sådan möjlighet bör kunna tillämpas,
- ta ställning till om straffvärdeventilen i fråga om hemlig rumsavlyssning bör få tillämpas oavsett brott, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Hemlig dataavläsning omfattas av våra överväganden

Det ankommer på utredningen att säkerställa att en välfungerande systematik upprätthålls i regelverket om hemliga tvångsmedel och att bedöma behovet av följdändringar i annan relevant lagstiftning. Vi har även möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska utredas.

Vi konstaterar att det nyligen införda tvångsmedlet hemlig dataavläsning får användas vid förundersökning om samma slags brott som hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning, se 4 § första stycket lagen (2020:62) om hemlig dataavläsning. Om dataavläsning avser rumsavlyssningsuppgifter gäller i stället att det ska vara fråga om en förundersökning om sådana brott som kan föranleda hemlig rumsavlyssning (6 § samma lag). Hemlig dataavläsning kan vara ett sätt för de brottsbekämpande myndigheterna att få tillgång till samma slags uppgifter som avses med hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning. Ett syfte med införande av hemlig dataavläsning var att motverka konsekvenserna av att bl.a. den ökade användningen av kryptering gjort det svårare att få tillgång till innehållet i elektronisk kommunikation genom hemlig avlyssning (prop. 2019/20:64 Hemlig dataavläsning, s. 69–71). Det finns alltså ett starkt sakligt och systematiskt samband mellan de tvångsmedel som uttryckligen omfattas av vårt uppdrag och hemlig dataavläsning. Regeringen har uttalat att det är av väsentlig betydelse att hemlig dataavläsning kan användas i motsvarande fall som de befintliga hemliga tvångsmedlen, eftersom

det annars finns en risk för att vissa allvarliga brott inte kan utredas när det visar sig vara omöjligt att använda befintliga hemliga tvångsmedel (se prop. 2019/20:64 s. 124). Vi har därför valt att låta våra överväganden i detta kapitel omfatta även hemlig dataavläsning.

Hemlig övervakning av elektronisk kommunikation

Frågan om en ny straffvärdeventil för hemlig övervakning av elektronisk kommunikation nämns inte särskilt i våra direktiv. Bestämmelserna om hemlig övervakning har emellertid ett direkt samband med bestämmelserna om hemlig avlyssning av elektronisk kommunikation. Ett tillstånd till hemlig avlyssning ger nämligen också rätt att vidta de åtgärder som kan omfattas av ett tillstånd till hemlig övervakning (27 kap. 18 § tredje stycket). Vidare kan hemlig övervakning användas för att utreda vem som skäligen kan misstänkas för visst brott förutsatt att det är fråga om brott som kan leda till hemlig avlyssning av elektronisk kommunikation (27 kap. 20 § andra stycket och 19 § fjärde stycket). En ändring av reglerna rörande avlyssning leder därför till motsvarande ändring av möjligheten att övervaka, om inte ändringar görs också i övervakningsreglerna. I avsnitt 6.15 tar vi ställning till om sambandet mellan bestämmelserna ska vara oförändrat även om en ny straffvärdeventil införs.

6.2 Gällande rätt

6.2.1 Allmänt om straffvärdebedömning

Straff ska, med beaktande av intresset av en enhetlig rättstillämpning, bestämmas inom ramen för den tillämpliga straffskalan efter brottets eller den samlade brottslighetens straffvärde (29 kap. 1 § första stycket brottsbalken, förkortad BrB). Med straffvärde avses brottets svårhet – eller allvar – i förhållande till andra brott. Åtskillnad görs därvid mellan det abstrakta och det konkreta straffvärdet. Det *abstrakta straffvärdet* avser en hel brottstyps straffvärde, uttryckt genom angivande av brottets straffskala. Med det *konkreta straffvärdet* avses det exakta straffvärde som fastställs för en enskild gärning, med tillämpning av de föreskrifter av generell karaktär som kan finnas i lag.

Bestämmelsen i 29 kap. 1 § BrB ger uttryck för att straffvärdebedömningen vid flerfaldig brottslighet ska avse brottsligheten i dess helhet. Vid bedömningen av straffvärdet ska rätten beakta den skada, kränkning eller fara som gärningen inneburit, vad den tilltalade insett eller borde ha insett om detta samt de avsikter eller motiv som han eller hon haft. Det ska särskilt beaktas om gärningen inneburit ett allvarligt angrepp på någons liv eller hälsa eller trygghet till person (andra stycket i samma paragraf). Den enskilda domarens värdering av olika brotts svårhet ska inte ha någon betydelse för resultatet i det enskilda fallet, utan straffet ska bestämmas utifrån den tillämpliga straffskalan och med beaktande av reglerna i 29 kap. BrB och den rättspraxis som utvecklats.

I 29 kap. 2 § anges ett antal försvårande omständigheter som särskilt ska beaktas vid bedömningen av straffvärdet. Ett antal förmildrande omständigheter som särskilt ska beaktas vid bedömningen av straffvärdet, och som alltså inverkar på detta i sänkande riktning, räknas upp i 29 kap. 3 §. Uppräkningarna av förmildrande och försvårande omständigheter är exemplifierande men är avsedda att innehålla de vanligaste och mest betydelsefulla straffvärdehöjande respektive straffvärdesänkande faktorerna. Utrymmet för att beakta andra faktorer som förmildrande är dock avsett att vara större än motsvarande utrymme i fråga om försvårande omständigheter.

6.2.2 Straffvärdebedömning vid flerfaldig brottslighet

Vid flerfaldig brottslighet tillämpas en gemensam straffskala för den samlade brottsligheten. Utgångspunkten för den gemensamma straffskalan är det högsta maximistraff som kan följa på något av brotten. Med ett visst tillägg utgör det straffskalans maximum. Av regleringen i 26 kap. 2 § BrB följer, när det gäller fängelse som gemensamt straff, att tillägget är som minst ett år och som mest fyra år beroende på hur allvarlig brottsligheten är. Är det fråga om återfall kan straffskalan skärpas ytterligare enligt 26 kap. 3 § brottsbalken. Om påföljden bestäms till fängelse på viss tid får straffet aldrig överstiga vare sig de högsta straffen sammanlagda med varandra eller 18 år. Den gemensamma straffskalans minimum utgörs av det högsta minimistraff som kan följa på något av brotten.

Brottsbalken innehåller inte någon regel om hur man vid flerfaldig brottslighet ska bestämma den samlade brottslighetens straffvärde. I propositionen om ändring i brottsbalken m.m. (straffmätning och påföljdsval, m.m.) har frågan i hög grad överlämnats till rättstillämpningen (prop. 1987/88:120 om ändring i brottsbalken m.m. [straffmätning och påföljdsval m.m.], s. 79). I rättspraxis har det utbildats vissa allmänna principer för straffvärdebedömning vid flerfaldig brottslighet. Dessa kommer till uttryck i Högsta domstolens avgörande i rättsfallet NJA 2008 s. 359. Metoden går ut på att domstolen först bestämmer straffvärdet för vart och ett av brotten. När sedan den samlade brottslighetens straffvärde ska bestämmas utgår rätten från det allvarligaste av brotten. Till straffvärdet för detta brott läggs därefter en efter hand minskande del av straffvärdet för vart och ett av de övriga brotten i ordning efter brottens allvar (asperationsprincipen). En allmän kontroll görs också av att det straffvärde som domstolen kommer fram till på detta sätt inte framstår som oproportionerligt i förhållande till den typ av brottslighet som är aktuell.

Av HD:s praxis framgår att särskilda överväganden i fråga om asperationsprincipens tillämpning kan göra sig gällande vid seriebrottslighet där det föreligger ett tydligt samband mellan brotten. Särskilt systematik och planering kan, trots att det inte varit fråga om sådant systematiskt tillvägagångssätt som medför att brotten rubriceras som grova, ges betydelse på så sätt att den reduktion av den samlade brottslighetens straffvärde som följer av en tillämpning av asperationsprincipen blir något mindre än annars. Detta kan ske inom ramen för den efterkontroll som alltid ska göras. (Se NJA 2018 s. 378 p. 33.)

En särskild utredare har fått i uppdrag att överväga och föreslå förändringar av strafflagstiftningen som ger uttryck för en skärpt syn på flerfaldig brottslighet (dir. 2021:56). Inom ramen för uppdraget ska utredaren överväga olika modeller för hur en sådan förändring kan åstadkommas. Utredaren ska även överväga vilken inverkan ett samband mellan brotten bör ges vid straffvärdebedömningen. Uppdraget ska redovisas senast den 20 januari 2023.

6.2.3 Straffvärdet vid organiserad eller systematisk brottslighet

Betydelsen som en försvårande omständighet

Enligt 29 kap. 2 § 6 BrB ska det som en försvårande omständighet vid bedömningen av straffvärdet särskilt beaktas om brottet har utgjort ett led i en brottslighet som utövats i organiserad form eller systematiskt eller om brottet föregåtts av särskild planering. I propositionen Skärpta straff för allvarliga våldsbrott m.m. (prop. 2009/10:147) utvecklas vad som avses med brottslighet som utövas i organiserad form (s. 43). Där anges följande.

Med brottslighet som utövats i organiserad form avses brottslighet som har begåtts inom ramen för en struktur där flera personer samverkat under en inte helt obetydlig tidsperiod för att begå brott. Det är inte tillräckligt att det aktuella brottet har skett i samverkan. Personerna ska ha ingått i en sammanslutning eller ett nätverk av viss kontinuitet vars syfte att begå brott sträckt sig längre än till enbart det ifrågavarande brottet. Att brottet ska ha utgjort ett led i en brottslighet som utövats i organiserad form innebär att brottet ska ha haft ett naturligt samband med brottsligheten. Det är inte nödvändigt att brottet begåtts av den eller de som organiserat brottsligheten. Ett exempel på brottslighet som utövats i organiserad form kan vara fickstölder som begåtts av en grupp av personer. Ett annat exempel är illegal indrivningsverksamhet som en gruppering ägnat sig åt. Punkten är däremot inte tillämplig när ett brott begåtts inom en sammanslutning eller ett nätverk med legal verksamhet, som inte utgör en täckmantel för illegal verksamhet. I kommentaren till bestämmelsen (Agneta Bäcklund m.fl., Brottsbalken. En kommentar [2021-12-01 JUNO], kommentaren till 29 kap. 2 § 6 BrB) anges att problemet med gängbrottslighet torde kunna hänföras till kategorin organiserad brottslighet, men att det dock fordrar att åklagaren lyfter fram och styrker att brottsligheten skett inom ramen för en sådan struktur. Gängbrottsutredningen framhåller dock i betänkandet Skärpta straff för brott i kriminella nätverk (SOU 2021:68) att det i utsatta områden förekommer löst sammansatta kriminella nätverk som inte alltid har en sådan organiserad form som avses i bestämmelsen och att det under alla förhållanden i många fall kan vara svårt att bevisa att förutsättningarna i punkten är uppfyllda i förhållande till sådana, och andra, kriminella nätverk med en lägre grad av organisation.

I prop. 2009/10:147 (s. 43) utvecklas även vad som avses med brottslighet som utövats systematiskt. Där framgår att skrivningen avser brottslighet där ett visst tillvägagångssätt upprepats ett flertal gånger av antingen en ensam gärningsman eller av flera personer i samförstånd. Som ett exempel nämns att någon vid upprepade tillfällen förmått annan till utbetalning av en förmån som han eller hon inte har haft rätt till. Ett annat exempel som nämns är om flera personer rånat olika butiker eller banker och då gått till väga på ett likartat sätt vid varje tillfälle.

Den aktuella straffskärpningsgrunden har, såvitt avser brott som är ett led i organiserad brottslighet, nyligen varit föremål för översyn av Gängbrottsutredningen (s. 219–221). Utredningen har kommit fram till att den inte bör avskaffas eller ändras, även om den som ovan nämnts bedöms inte alltid vara tillämplig på löst sammansatta nätverk av det slag som är av särskilt intresse för utredningens arbete och som till stor del kan knytas till de senaste årens skjutningar och sprängningar. Utredningens bedömning är att det varken är lämpligt att utmönstra bestämmelsen eller ändra i den. Däremot föreslås nya straffskärpningsgrunder som tar sikte på våldsamma kriminella uppgörelser.

Betydelsen av ett systematiskt tillvägagångssätt vid gradindelade brott

Vid gradindelade brott är varje grad av brottet en egen brottstyp. Gradindelningen måste i princip ske före straffvärdebedömningen. Vid gradindelade brott är det vanligt att det anges vilka omständigheter, s.k. kvalifikationsgrunder, som särskilt ska beaktas vid bedömningen av till vilken grad en gärning ska hänföras. Det är emellertid inte nödvändigt att kvalificera brottet som grovt när någon av de angivna omständigheterna föreligger och heller inte uteslutet att bedöma brottet som grovt i fall där ingen av de angivna omständigheterna är för handen. En samlad bedömning ska alltid göras. För att ett brott ska bedömas som grovt krävs emellertid i princip att omständigheterna i det enskilda fallet framstår som försvårande i motsvarande grad som normalt gäller i de fall som anges i lagens exemplifiering (jfr t.ex. rättsfallen NJA 2018 s. 634, NJA 2018 s. 767 I och NJA 2019 s. 747). Att en brottslighet har utövats systematiskt anges i fråga om gradindelade brott inte sällan som ett kvalificerande rekvisit för en gradhöjning. Brottslighetens systematiska karaktär kan

också beaktas inom sådana kvalifikationsgrunder som går ut på att gärningen har varit av särskilt farlig art (se NJA 1985 s. 444). HD har i ett rättsfall som handlade om rubriceringen av ett antal skattebrott uttalat att systematisk brottslighet inte är något enhetligt begrepp, men att man som regel avser brott som upprepas på ett likartat sätt, och att det i allmänhet också krävs att brottsligheten har föregåtts av planering eller att gärningsmannen använder en särskild metod för att begå brotten (NJA 2018 s. 634).

När det gäller att bedöma gradindelade brott som grova med hänvisning till att de har skett systematiskt eller föregåtts av särskild planering utan att dessa omständigheter anges i straffbestämmelsen, framträder i praxis en tydlig återhållsamhet särskilt under senare år. För att sådana förhållanden ska föranleda en gradhöjning bör det i dessa fall normalt krävas att brotten har en frekvens och präglas av en förslagenhet som klart går utöver vad som gäller för annan, i och för sig upprepad och likartad brottslighet. (Se NJA 2016 s. 1143 p. 25 och NJA 2018 s. 378 p. 9.).

När en omständighet uttryckligen har angetts som en kvalifikationsgrund för grovt brott bör den enligt HD:s uttalanden i rättsfallet NJA 2018 s. 634, som handlade om upprepade skattebrott, tillmätas större betydelse för rubriceringsfrågan än när omständigheten aktualiseras enbart som en straffskärpningsgrund enligt 29 kap. 2 § 6 BrB. Detta eftersom det då inte sällan handlar om omständigheter som ofta är för handen vid den specifika brottstypen och som i sig medför att brottsligheten är av allvarligare beskaffenhet, t.ex. genom att den – om den är välplanerad – kan vara svårare att upptäcka. HD uttalade vidare följande.

> Det finns ändå skäl till viss restriktivitet vid bedömningen av vad som utgör ett systematiskt tillvägagångssätt även när den omständigheten utgör en särskild kvalifikationsgrund. En uppflyttning i svårhetsgrad innebär regelmässigt en repressionsökning och bör begränsas till de fall där omständigheterna är sådana att en ändrad rubricering framstår som motiverad. En inte önskad konsekvens av att upprepade och likartade brott bedöms som grova enbart på grund av det repetitiva tillvägagångssättet är att straffvärdet av varje enskilt brott av rimlighetsskäl ofta måste sättas lägre än vad som borde följa på ett grovt brott av den aktuella brottstypen. Det samlade straffvärdet av brottsligheten i dess helhet kan annars framstå som alldeles för högt.

> Enbart det förhållandet att ett förfarande upprepas på likartat sätt bör alltså inte medföra att brottsligheten bedöms vara systematisk på det sätt som krävs för att det ska vara fråga om grova skattebrott. Som regel bör det krävas någon form av brottsplan eller i allt fall att upprepningarna framstår som en påräknelig fortsättning på tidigare gärning eller gärningar. Att brotten har upprepats kan dock, även om brottsligheten inte är att anse som systematisk i gradindelningshänseende, sammantaget med andra omständigheter föranleda att brotten ska bedömas som grova.

6.2.4 Förutsättningarna för användning av hemliga tvångsmedel i en förundersökning

Hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning får enligt 27 kap. 18 § andra stycket respektive 27 kap. 20 a § andra stycket RB användas vid en förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, för vissa särskilt uppräknade brott och försök, förberedelse eller stämpling till de angivna brotten, om en sådan gärning är belagd med straff. Enligt de s.k. straffvärdeventilerna får tvångsmedlen även användas vid misstanke om ett annat brott om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år (27 kap. 18 § andra stycket 4 och 20 a § andra stycket 4 RB). Med straffvärde avses brottets konkreta straffvärde, med beaktande av eventuella försvårande och förmildrande omständigheter. Om det finns osäkerhetsfaktorer ska dessa vägas in till förmån för den misstänkte (prop. 2002/03:74 Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering, s. 34). Det har ingen betydelse om brottet är fullbordat eller har stannat vid försök, förberedelse eller stämpling så länge brottet har det angivna straffvärdet. Straffvärdeventilerna ska tillämpas restriktivt (prop. 2002/03:74 s. 35 och 48).

Enligt ordalydelsen beaktas inte faktorer som utöver straffvärdet ska beaktas vid straffmätningen, såsom återfall i brott (29 kap. 4 §), att den misstänkte är under 21 år (29 kap. 7 §) eller sådana omständigheter som räknas upp i 29 kap. 5 § BrB. Det bör dock nämnas att hemliga tvångsmedel inte kan inte användas mot någon misstänkt person som inte har fyllt 15 år (36 f § lagen [1964:167] med särskilda bestämmelser om unga lagöverträdare). Vidare innebär de allmänna principerna för tvångsmedelsanvändning och då särskilt proportionalitetsprincipen att beslutsfattaren i sin bedömning måste ta hänsyn till hur tvångsmedlet kan påverka den som utsätts för det. Det kan då

i vissa fall vara nödvändigt att ta särskilda hänsyn om den som drabbas är en ung person (Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas? fjärde upplagan, s. 785).

Hemlig rumsavlyssning anses som det hemliga tvångsmedel som är allra mest ingripande i förhållande till enskildas personliga integritet. Det ställs därför högre krav i fråga om de brott som kan utredas med hjälp av tvångsmedlet. Hemlig rumsavlyssning får endast användas vid en förundersökning om

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 26 § lagen (2018:558) om 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) grov människoexploatering enligt 4 kap. 1 b § tredje stycket brottsbalken,
   c) våldtäkt enligt 6 kap. 1 § första stycket brottsbalken,
   d) grovt sexuellt övergrepp enligt 6 kap. 2 § andra stycket brottsbalken,
   e) våldtäkt mot barn enligt 6 kap. 4 § första eller andra stycket brottsbalken,
   f) grovt sexuellt övergrepp mot barn enligt 6 kap. 6 § andra stycket brottsbalken,
   g) grovt utnyttjande av barn för sexuell posering enligt 6 kap. 8 § tredje stycket brottsbalken,
   h) grovt koppleri enligt 6 kap. 12 § tredje stycket brottsbalken,
   i) grov utpressning enligt 9 kap. 4 § andra stycket brottsbalken,

j) grovt barnpornografibrott enligt 16 kap. 10 a § sjätte stycket brottsbalken,

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

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

m) 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, eller

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.

Till skillnad från vad som gäller vid bl.a. hemlig avlyssning av elektronisk kommunikation räcker det alltså inte med att det konkreta straffvärdet motsvarar ett visst straff för att straffvärdeventilen ska tillämpas i fråga om rumsavlyssning, utan det krävs även att brottet ingår i den brottskatalog som finns i fjärde punkten.

Hemlig dataavläsning får användas vid samma slags brott som hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning (4 § lagen om hemlig dataavläsning). Om avläsningen avser rumsavlyssningsuppgifter gäller i stället att förundersökningen måste avse de slags brott som kan utredas med hjälp av hemlig rumsavlyssning (6 § samma lag).

Ett tillstånd till hemlig avlyssning ger också rätt att vidta de åtgärder som avses med en hemlig övervakning av elektronisk kommunikation (27 kap. 18 § tredje stycket). Dessa åtgärder går ut på att man i hemlighet hämtar in uppgifter 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 (s.k. basstationstömning), eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Åtgärden får även användas för att hindra meddelanden från att nå fram. Hemlig övervakning får användas vid en förundersökning om brott

för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader samt vissa andra brott som räknas upp i 27 kap. 19 § tredje stycket. Om tvångsmedlet används i syfte att utreda vem som skäligen kan misstänkas för brottet krävs dock att förundersökningen avser brott som kan leda till hemlig avlyssning av elektronisk kommunikation (27 kap. 19 § fjärde stycket).

6.3 Olika metoder för att bestämma tillämpningsområdet för tvångsmedel

Det finns flera metoder för att bestämma tillämpningsområdet för ett visst tvångsmedel. En metod är att möjligheten att använda tvångsmedlet knyts till straffskalans övre gräns, dvs. att det på brottet ska kunna följa fängelse i t.ex. ett år eller mer. För häktning krävs enligt 24 kap. 1 § RB att det för brottet är föreskrivet minst ett års fängelse. En nackdel med denna metod är att många brott har en mycket vid straffskala och att det finns en stor risk för att tvångsmedel kommer att användas vid brott som i det enskilda fallet är mindre grovt (jfr prop. 2002/03:74 s. 32). Metoden används inte i dagsläget i regleringen om hemliga tvångsmedel men förekommer i våra nordiska grannländer.

En annan metod är att använda en brottskatalog, dvs. att låta lagtexten innehålla en uttömmande uppräkning av de brott för vilka tvångsmedlet kan komma i fråga. Denna metod används bl.a. i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. En fördel med denna metod är att det blir klart avgränsat när tvångsmedlet kan komma till användning, vilket främjar förutsebarheten. En nackdel med användning av brottskataloger är dock att regleringen blir otymplig och måste ändras varje gång ett nytt brott tillkommer som motiverar en användning av tvångsmedlet (anförd prop. s. 32).

Tillämpningen av ett visst tvångsmedel kan också knytas till straffskalans nedre gräns på så sätt att ett visst lägsta straff måste vara föreskrivet för det aktuella brottet för att tvångsmedlet ska få användas. Denna metod kan sägas vara utgångspunkten i fråga om de hemliga tvångsmedlen (anförd prop. s. 32).

Som framgått av redogörelsen för gällande rätt (se avsnitt 6.2) är det vidare möjligt att kombinera t.ex. straffskalans nedre gräns och en brottskatalog.

En särskild metod som har använts i fråga om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning är en s.k. straffvärdeventil. Ventilen innebär att tvångsmedlet kan användas även i fråga om brott som har ett lägre minimistraff än det som anges i bestämmelsen förutsatt att det med hänsyn till omständigheterna kan antas att brottets konkreta straffvärde överstiger detta. När det gäller hemlig rumsavlyssning och hemlig dataavläsning som avser rumsavlyssningsuppgifter krävs dock utöver att straffvärdet kan antas överstiga fängelse i fyra år att det är fråga om ett av de brott som räknas upp i en brottskatalog i bestämmelsen om hemlig rumsavlyssning. Straffvärdeventilen kan alltså kombineras med en brottskatalog.

Utöver de angivna metoderna kan man även tänka sig andra sätt att avgränsa användningsområdet för ett visst hemligt tvångsmedel. Det är t.ex. tänkbart att lägga till kvalificerande faktorer, såsom att det ska vara uppenbart att brottet har ett straffvärde som överstiger ett visst fängelsestraff eller att brottet har vissa kännetecken.

6.4 Tidigare överväganden om straffvärdeventil

Hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning

Straffvärdeventilen avseende hemlig teleavlyssning (numera hemlig avlyssning av elektronisk kommunikation) och hemlig kameraövervakning infördes i enlighet med förslag i propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering (prop. 2002/03:74). Regeringen uttalade där att straffskalans nedre gräns även i fortsättningen borde vara utgångspunkten när det gäller dessa tvångsmedel men konstaterade samtidigt att den dåvarande regleringen, som inte innehöll någon straffvärdeventil, ledde till att t.ex. grov stöld inte kunde omfattas av hemliga tvångsmedel ens i sådana fall där det stod klart att brottets straffvärde klart överstiger två års fängelse. Regeringen framhöll att det är ett viktigt samhällsintresse att med hjälp av effektiva tvångsmedel kunna utreda brott som i det enskilda fallet har ett mycket högt straffvärde, men som har en vid straffskala med ett lågt straffminimum. Man föreslog därför införande av en straffvärdeventil, trots att Buggningsutredningen hade avstått från att lägga fram ett sådant förslag. Utredningen hade

ansett det alltför svårt att på ett tidigt stadium bedöma straffvärdet och även fäst vikt vid att olika domare kan göra olika bedömning i fråga om straffvärdet (SOU 1998:46 Om buggning och andra hemliga tvångsmedel, s. 380 och 381). Regeringen ansåg dock att utredningen hade övervärderat svårigheterna och nackdelarna med en sådan reglering och gjorde bedömningen att det inte torde vara någon avgörande skillnad mellan att på ett tidigt stadium bedöma om ett brott ska rubriceras på ett sådant sätt att en minimistraffregel är uppfylld och att göra en bedömning av detta brotts straffvärde. Regeringen hänvisade också till att det föreslagna systemet med offentliga ombud i ärenden om hemliga tvångsmedel ger förutsättningar för en mer allsidig belysning av de omständigheter som inverkar på frågan om tvångsmedlets tillåtlighet och också ger möjlighet att få beslut om tillstånd till hemliga tvångsmedel överprövade. Regeringen underströk att den omständigheten att utredningen i vissa fall kan vara mindre robust ska räknas den misstänkte till godo i form av ett lägre bevisvärde. Enligt regeringen skulle man kunna uttrycka detta så att en marginal till förmån för den misstänkte måste vägas in. (Prop. 2002/03:74 s. 33.)

I propositionen diskuterades även möjligheten att införa en straffvärdeventil vid seriebrottslighet, som skulle göra det möjligt att använda tvångsmedlen utifrån en bedömning av brottslighetens samlade straffvärde (anförd prop. s. 34). Regeringen anförde då att hemliga tvångsmedel skulle kunna användas för enskilda brott som har ett relativt blygsamt straffvärde. Med hänsyn till det integritetsintrång som användande av sådana tvångsmedel innebär gjorde regeringen bedömningen att en sådan ordning inte skulle införas.

Hemlig rumsavlyssning

Straffvärdeventilen i bestämmelserna om hemlig rumsavlyssning infördes i enlighet med förslag i propositionen Hemlig rumsavlyssning (prop. 2005/06:178). Regeringen hänvisade till de bedömningar som gjorts vid införandet av en sådan ventil när det gäller hemlig teleavlyssning och hemlig kameraövervakning och ansåg att det inte fanns anledning till någon annan principiell bedömning av de tillämpningsproblem som kan uppstå. Regeringen konstaterade dock vidare att införande av en generell straffvärdeventil för hemlig rumsavlyssning skulle innebära att tvångsmedlet skulle få ett omfattande tillämpnings-

område. Eftersom hemlig rumsavlyssning typiskt sett kan anses vara ett mycket mera integritetskränkande tvångsmedel än de tvångsmedel som nämnts i det föregående, ansåg regeringen att det finns skäl att vara mycket restriktiv med dess användande. Bedömningen var att straffvärdeventilen borde begränsas till att avse förundersökningar om vissa mycket allvarliga brott, där det finns ett beskrivet och känt behov av att kunna använda hemlig rumsavlyssning. Regeringen ansåg att det fanns ett sådant behov när det gäller viss grov organiserad brottslighet, och särskilt sådan som innefattar systemhotande verksamhet.

Till straffvärdeventilens brottskatalog fördes människohandel, vissa grova sexualbrott, grovt utnyttjande av barn för sexuell posering och grovt barnpornografibrott, grovt koppleri, grov utpressning, grovt övergrepp i rättssak, grovt narkotikabrott och grov narkotikasmuggling. Övervägandena finns på s. 53–55 i propositionen. Det konstaterades där att utredningar om narkotikabrott stod för cirka 70 procent av den telefonavlyssning som vid tidpunkten förekom i Sverige och att narkotikabrott inte sällan utgör en plattform för annan, organiserad brottslighet.

Regeringen lyfte vidare fram att hot och våld från personer i kriminella grupper mot vittnen och målsägande hade blivit allt vanligare och att det var högst angeläget att de brottsbekämpande myndigheterna har så effektiva verktyg som möjligt för att utreda sådan brottslighet. Det konstaterades att det ofta finns en stark koppling mellan sådana brott och organiserad brottslighet men att de också kan begås av en enskild gärningsman. Regeringen ansåg att det även i sådana fall bör finnas en möjlighet för polisen att kunna använda hemlig rumsavlyssning, om det inte går att föra utredningen framåt på något annat sätt.

I propositionen konstaterades det att den gränsöverskridande handeln med människor för exploatering var ett ökande fenomen som ofta innefattar ett hänsynslöst utnyttjande av kvinnors och barns särskilt sårbara situation och som inte sällan är av organiserat slag. Liksom när det gäller annan organiserad brottslighet ansågs möjligheten att använda olika former av straffprocessuella tvångsmedel vara av väsentlig betydelse för att kunna upptäcka och utreda människohandelsbrott.

Regeringen anförde vidare att det ofta finns ett tydligt samband mellan koppleri och organiserad brottslighet såsom människohandel på så sätt att de olika brotten endast utgör olika moment i en större

brottslig hantering. Sexuellt utnyttjande och övervåld torde enligt regeringen ofta förekomma i anslutning till eller som en följd av människohandel och grovt koppleri.

Några remissinstanser hade uttalat att det i enstaka fall kan finnas ett behov av att kunna använda hemlig rumsavlyssning även vid utredning av andra brott, som t.ex. grova förmögenhetsbrott. Regeringen ansåg emellertid att det finns skäl att vara mycket restriktiv med användandet av hemlig rumsavlyssning och att straffvärdeventilen därför skulle begränsas till de brott som angetts ovan.

I propositionen Hemliga tvångsmedel mot allvarliga brott (prop. 2013/14:237) övervägde regeringen på förslag i betänkandet Hemliga tvångsmedel mot allvarliga brott (SOU 2012:44) om straffvärdeventilens tillämpningsområde borde utvidgas (s. 85–87). Regeringen instämde visserligen i utredningens bedömning att det kunde finnas ett behov av hemlig rumsavlyssning även för brott – främst inom den grova organiserade brottsligheten – som inte ingick i brottskatalogen, men ansåg att det var oklart vilka konkreta brottstyper som den föreslagna förändringen tog sikte på. Det hade inte angetts några konkreta situationer där brottskatalogens utformning hade inneburit att straffvärdeventilen inte kunnat tillämpas, trots att detta skulle ha varit rimligt och proportionerligt. Med hänsyn till den särskilda restriktivitet som ska iakttas regeringen att det inte i vid den tidpunkten hade framkommit tillräckliga skäl som talar för att ta bort eller utöka brottskatalogen.

Grov människoexploatering lades till brottskatalogen i straffvärdeventilen i enlighet med förslag i propositionen Det straffrättsliga skyddet mot människohandel och människoexploatering (prop. 2017/18:123). I samband med det anförde regeringen bl.a. följande (prop. s. 52).

> Brottet grov människoexploatering är avsett att träffa bl.a. fall där exploatering sker i större omfattning. Sådan exploatering torde i praktiken inte sällan förutsätta en väl utvecklad organisation och föregås av noggrann planering mellan ett stort antal människor. Liksom när det gäller annan organiserad brottslighet skulle möjligheten att använda hemlig rumsavlyssning kunna vara av väsentlig betydelse i brottsutredningar om grov människoexploatering. Här kan nämnas de likheter som i angivet avseende kan finnas mellan grov människoexploatering och människohandel, där hemlig rumsavlyssning får användas. Regeringen bedömer därför att skälen för att tillåta hemlig rumsavlyssning vid grov människoexploatering uppväger det integritetsintrång som tvångsmedlet skulle medföra.

6.5 Utgångspunkter för övervägandena om nya straffvärdeventiler

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

6.6 Det finns ett behov av nya straffvärdeventiler för hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och motsvarande hemlig dataavläsning

Bedömning: Det finns ett behov av en ny straffvärdeventil vid förundersökningar om flerfaldig brottslighet avseende hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. Motsvarande behov finns i fråga om hemlig dataavläsning som gäller de slags uppgifter som avses i 2 § första stycket 1–4, 6 och 7 i lagen om hemlig dataavläsning.

Skälen för bedömningen

Grundläggande förutsättningar för utvidgade möjligheter att använda hemliga tvångsmedel

En grundläggande förutsättning för att man ska utvidga möjligheterna att använda hemliga tvångsmedel är att det finns ett reellt behov av en sådan utvidgning. När det gäller hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning avseende kommunikationsavlyssnings- och kameraövervakningsuppgifter har de brottsbekämpande myndigheterna anfört att det finns ett behov av att kunna använda tvångsmedlen vid misstanke om serie-

brottslighet som kan sägas vara organiserad eller systematisk, som upprepar sig på ett likartat sätt vid de olika brottstillfällena och där vart och ett av brotten inte når upp till det straffvärde som krävs enligt straffvärdeventilen för hemlig avlyssning av elektronisk kommunikation men där det samlade straffvärdet för brotten gör det. Myndigheterna har anfört att ett sådant behov finns även när det gäller hemlig övervakning av elektronisk kommunikation, i synnerhet i syfte att utreda vem som skäligen kan misstänkas för brottet (27 kap. 20 § andra stycket RB), samt motsvarande slags uppgifter gällande hemlig dataavläsning (2 § första stycket 2 och 3 lagen om hemlig dataavläsning). När det gäller hemlig dataavläsning har myndigheterna anfört att tillstånden även behöver kunna omfatta uppgifter som avses i 2 § första stycket 6 och 7 lagen om hemlig dataavläsning, dvs. uppgifter som finns lagrade i informationssystemet och uppgifter om hur informationssystemet används.

Ärenden där det finns skäl som talar för en ny straffvärdeventil för hemlig avlyssning

Det finns flera exempel på situationer där det är problematiskt att det inte går att använda hemlig avlyssning av elektronisk kommunikation och därmed inte heller hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas.

Ekobrottsmyndigheten och Åklagarmyndigheten har framhållit skattebrott och annan ekonomisk brottslighet som ett problemområde. Skattebrott och annan ekonomisk brottslighet begås inte sällan inom ramen för organiserad brottslighet. Många gånger är det fråga om brottsupplägg som omfattar flera olika brott. Ibland kan brotten begås i ett och samma bolag och i andra fall innebär upplägen att brotten begås i flera olika bolag för vilka samma person eller personer är ansvariga. I andra fall är skattebrottslighet eller ekonomisk brottslighet inte organiserad, men även i sådana fall begås den ofta upprepat. I många fall är de olika brotten dessutom tätt sammanknutna med varandra. Som exempel kan ett bokföringsbrott vara ett medel för att dölja ett skattebrott. Det kan då vara svårt att skilja brotten från varandra och att urskilja straffvärdet för de enskilda brotten. Det kan över huvud taget vara problematiskt att avgöra om det är fråga om flera brott av normalgraden eller ett grovt brott.

I domstolspraxis har skatteundandragande ibland bedömts som ett grovt skattebrott med ett straffvärde överstigande två år även om skatteundandragandet delats upp på flera tillfällen. Tillstånd har då lämnats till hemlig avlyssning av elektronisk kommunikation. I andra fall har ett liknande förfarande bedömts som flera brott. Det kan även då ha ansetts vara fråga om grova skattebrott med ett samlat straffvärde klart överstigande två år men där inte något av de ingående brotten kan anses ha ett straffvärde överstigande två år. Straffvärdeventilen är då inte tillämplig. Eftersom det i ett inledande skede av en förundersökning kan vara svårt att bedöma om det är fråga om ett eller flera brott är det sannolikt att åklagare och domstolar väljer att bedöma det som flera brott och alltså inte tillåter hemlig avlyssning även i fall som senare visar sig vara att bedöma som ett brott.

Åklagarmyndigheten har bl.a. lyft fram de allt vanligare bedrägeriärendena där flera målsägande har blivit uppringda och lurats att lämna ifrån sig inloggningsuppgifter eller förmåtts att öppna sina BankID med följd att de blivit av med penningmedel – ibland även större belopp. Det är inte ovanligt att brotten bedöms som grova med hänsyn till exempelvis att gärningen även innefattar olovlig identitetsanvändning eller urkundsförfalskning, begås systematiskt med en uttänkt brottsplan och/eller omfattar relativt stora belopp (se bl.a. Kalmar tingsrätts dom den 31 augusti 2021 i mål B 4869-20, Södertörns tingsrätts dom den 26 juli 2021 i mål B 6940-21 och Södertälje tingsrätts dom den 22 december 2020 i mål B 966-18). I ett sådant fall behöver de brottsutredande myndigheterna i ett första steg ofta kunna inhämta uppgift om vilket nummer som ringt upp målsäganden och kartlägga användningen av detta nummer för att man över huvud taget ska kunna identifiera en skäligen misstänkt. Hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet kräver att brottet är sådant att hemlig avlyssning får användas. I många av de aktuella ärendena är detta inte möjligt, vilket kan göra det svårt eller omöjligt att komma framåt i utredningen. Det är visserligen möjligt för en målsägande att från sin teleoperatör begära in uppgifter om telefonnummer som kontaktat målsägandens telefon, men detta är förknippat med en kostnad och det är inte heller givet att målsäganden vill detta. Ibland kan uppgiften inte heller fås fram genom en tömning av målsägandens telefon med målsägandens samtycke, eftersom uppgiften kan ha raderats. Ur den misstänktes synvinkel kan det vidare finnas ett intresse av att tillförlitliga upp-

gifter kan fås från teleoperatören. I de nu angivna fallen knyter frågan an till den fråga som diskuteras i kapitel 8, nämligen om det bör vara tillåtet med hemlig övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet. Vi kommer där fram till att detta bör vara möjligt. Frågan knyter även an till frågan om man bör kunna vidta en hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet. Vi föreslår i kapitel 9 att även detta ska vara möjligt, under vissa förutsättningar.

Andra brott som Åklagarmyndigheten har tagit upp är bidragsbrott, grova stölder av ligor, grova smugglingsbrott och grova penningtvättsbrott.

När det gäller det slags flerfaldig brottslighet som tagits upp i det föregående är det samlade straffvärdet många gånger överstigande två års fängelse samtidigt som varje enskilt brott har ett lägre straffvärde än fängelse i två år. Enligt gällande rätt är det därför inte möjligt att utnyttja hemlig avlyssning av elektronisk kommunikation och inte heller hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet (27 kap. 18 § andra stycket, 19 § fjärde stycket och 20 § andra stycket). Samtidigt skulle dessa tvångsmedel ofta ha ett särskilt värde i utredningen eftersom det är vanligt att elektronisk kommunikation är ett redskap för att begå brotten. När brotten begås inom ramen för den organiserade brottsligheten tillkommer dessutom särskilda utredningssvårigheter på grund av de inblandades riskmedvetenhet. De kan på olika sätt anpassa sitt agerande för att minimera risken för att utsättas för hemliga tvångsmedel. Det kan t.ex. handla om valet av mötesplatser och kommunikationsmedel, men även om att man anpassar sin brottslighet till de rådande gränserna för användning av sådana tvångsmedel.

Ärenden där det finns skäl som talar för en ny straffvärdeventil för hemlig kameraövervakning

Just riskmedvetenheten inom den organiserade brottsligheten och gängbrottsligheten har framhållits som ett skäl för att även hemlig kameraövervakning bör kunna användas vid seriebrottslighet där det samlade straffvärdet överstiger två år. En stor del av den lokala organiserade brottsligheten begås i utsatta områden (Myndighetsgemensam lägesbild om organiserad brottslighet 2019). I sådana områden

kan hemlig kameraövervakning många gånger vara en förutsättning för att brott ska kunna utredas, eftersom det inte är möjligt att bedriva traditionell spaning på grund av att poliserna omedelbart blir igenkända. Det kan av delvis samma skäl vara svårt eller omöjligt att genomföra framgångsrika husrannsakningar.

På Ekobrottsmyndighetens område kan brott på punktskatteområdet nämnas som ett typexempel på situationer där hemlig kameraövervakning kan ha en avgörande betydelse för att brottsligheten ska kunna utredas. Eftersom bl.a. tobaksvaror är belagda med höga punktskatter kan det snabbt bli fråga om skatteundandraganden i miljonklassen. Ett vanligt exempel på sådan brottslighet är att gärningsmännen för in tobaksvaror från utlandet och säljer dem vidare i landet utan att redovisa föreskriven punktskatt, eller att man endast redovisar punktskatt för en del av den verkliga mängden. Brottsupplägget kan exempelvis vara att man i enlighet med regelverket har underrättat Skatteverket om införseln och att varorna ska transporteras till ett skatteupplag men att varorna de facto aldrig kommer till upplaget utan i stället säljs vidare direkt och utan att punktskatten redovisas. Skatteupplagen är ofta avsides belägna på platser där det är i det närmaste omöjligt för den brottsbekämpande myndigheten att osedd bedriva spaning för att utreda vilka leveranser som anländer och lämnar upplaget och vilka personer som rör sig på platsen. Det kan då vara avgörande för möjligheten att utreda vad som faktiskt hänt att det finns en möjlighet till hemlig kameraövervakning. Ett liknande exempel är snustillverkning där den som ansvarar för verksamheten redovisar en mindre del av den faktiska försäljningen till Skatteverket, men säljer den större mängden utan att redovisa punktskatt. Som tidigare konstaterats kan det vara svårt att bedöma vad som utgör ett respektive flera brott och från gärningsmannens perspektiv saknar det ofta betydelse, eftersom det handlar om ett samlat brottsupplägg. När det gäller skattebrott kan det även finnas en möjlighet för gärningsmannen att på olika sätt disponera över om det blir fråga om ett eller flera brott, t.ex. genom att välja att redovisa mervärdesskatt månatligen och inte kvartalsvis. Gärningsmannen kan därigenom åstadkomma att det blir fråga om flera brott med ett lägre straffvärde per brott, än om redovisningen i stället hade skett per kvartal. Straffskalan för grova brott enligt lagen (1998:506) om punktskattekontroll av transporter m.m. av alkoholvaror, tobaksvaror och energiprodukter är fängelse i lägst sex månader och högst fyra år. Straffskalan för grovt

skattebrott enligt skattebrottslagen (1971:69) är fängelse i lägst sex månader och högst sex år.

Ett liknande exempel kan vara pågående smugglingsbrott där insmugglade varor, såsom alkohol, tobak eller dopningsmedel, förvaras i ett lager. En möjlighet till hemlig kameraövervakning kan då vara av stor vikt för möjligheten att utreda vilka personer som är inblandade i brottet och om det är fråga om kommersiell verksamhet. Minimistraffet för grov smuggling är fängelse i 6 månader och det är mycket sällsynt att straffvärdet för ett enstaka grovt smugglingsbrott överstiger två års fängelse.

Ekonomisk brottslighet är ofta svårutredd även av andra skäl. Många gånger är den person som utåt sett företräder verksamheten inte den verkliga företrädaren, och det kan vara synnerligen svårt att utreda vem som egentligen bestämmer, även när det finns någon som är skäligen misstänkt. Vidare kan det ofta saknas neutrala vittnen, eftersom de personer som har inblick i verksamheten som regel är delaktiga i brottsligheten eller har något att förlora på att den avslöjas. Som ett exempel kan nämnas svartarbeteshärvor och ärenden där personer har fått betala för arbetstillstånd och sedan måste arbeta under slavliknande förhållanden. De personer som arbetat svart eller som har betalat för arbetstillstånd är sällan villiga att tala med de brottsutredande myndigheterna. I andra fall handlar det om påhittade arbeten som används i syfte att personer på olika sätt ska kunna utnyttja välfärdssystemen och skattesystemet. Det kan då vara ytterst värdefullt med en möjlighet till hemlig kameraövervakning för att få klarhet bl.a. i vilka personer som vistas på eller besöker en viss plats.

De brottsbekämpande myndigheterna har vidare framhållit människoexploatering enligt 4 kap. 1 b § brottsbalken som ett mycket svårutrett brott. För människoexploatering döms den som, utan att det är fråga om människorov eller människohandel, genom olaga tvång, vilseledande eller utnyttjande av någons beroendeställning, skyddslöshet eller svåra situation exploaterar en person i tvångsarbete, arbete under uppenbart orimliga villkor eller tiggeri. Straffet för människoexploatering är fängelse i högst fyra år. Om målsäganden inte har fyllt arton år döms till ansvar även om det inte förekommit något olaga tvång, vilseledande eller utnyttjande av någons beroendeställning, skyddslöshet eller svåra situation. Detta gäller även om den som begår en sådan gärning inte haft uppsåt till men varit oaktsam beträffande omständigheten att den andra personen inte fyllt arton år. Brottet

har även en grov variant där straffskalan börjar på två års fängelse och slutar på tio års fängelse. Vid bedömningen av om brottet är grovt ska det särskilt beaktas om gärningen avsett en verksamhet som bedrivits i större omfattning, medfört betydande vinning eller inneburit ett särskilt hänsynslöst utnyttjande av annan.

Anmälningarna för människoexploatering är relativt få och antalet utredningar som lett till åtal och fällande dom är ännu färre. En bidragande orsak är att offer för arbetskraftsexploatering inte är anmälningsbenägna, eftersom de riskerar att bli av med arbetstillstånd och uppehållstillstånd om de anger sin arbetsgivare (jfr vad som nyss sagts om ekonomisk brottslighet där personer fått betala för arbetstillstånd). Offren befinner sig alltså i regel i en stark beroendeställning till gärningsmannen, som denne utnyttjar för att kunna exploatera offren. Mörkertalet befaras vara mycket stort och särskilt i verksamheter som t.ex. restaurang, biltvättar, nagel- och massagesalonger och byggen. Polisen får tips via framför allt Migrationsverket och ibland också från allmänheten och vid arbetsplatsinspektioner och inre utlänningskontroller, men inledningsvis är det svårt att nå upp till en sådan nivå att det går att visa att det rör sig om grov människoexploatering, dvs. brott på en sådan nivå att hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning kan tillgripas. För att polisen ska kunna klarlägga antalet offer och omfattningen av verksamheten krävs det vanligtvis omfattande och utdragna spaningsinsatser. Typiskt för arbetskraftsexploatering är att offren arbetar varje dag i veckan och ibland upp till 14 timmar om dygnet utan raster. Det kräver i sin tur att polisen har spaningsgrupper som arbetar i skift och dessutom kan täcka in flera veckor i sträck för att man ska få ett tillräckligt bra underlag för bedömning av verksamheten. Situationen är likartad när det gäller tiggerifallen av människoexploatering. Mot denna bakgrund har de brottsbekämpande myndigheterna anfört att en möjlighet att använda hemlig kameraövervakning för organiserad eller systematisk människoexploatering hade inneburit en stor resursbesparing samtidigt som det också gett ett säkrare underlag. En svårighet i sammanhanget är att det finns mycket få avgöranden och ännu färre fällande domar avseende människoexploatering, vilket gör det osäkert hur straffvärdebedömningarna kommer att utfalla. Detta innebär dels en viss osäkerhet i fråga om hur många fall som kan aktualiseras, dels svårigheter för den som ska tillämpa ventilen.

Ett annat exempel kan vara återkommande grova stölder från en arbetsplats. Det kan då finnas anledning att montera en kamera för att fånga gärningspersonen på bar gärning och således fastställa vem som skäligen kan misstänkas för brottet. Man kan också tänka sig att motsvarande behov kan finnas vid återkommande grova stölder hos äldre personer med samma hemtjänst, där man misstänkte att någon ur hemtjänstpersonalen stjäl men man inte vet vem.

Det finns ett behov av en ny straffvärdeventil för flerfaldig brottslighet

Sammantaget bedömer vi att en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet och hemlig kameraövervakning skulle ha stor betydelse för möjligheten att utreda vissa typer av flerfaldig brottslighet där det samlade straffvärdet är högt samtidigt som de ingående brotten sedda för sig har ett lägre straffvärde än som krävs enligt de s.k. straffvärdeventilerna i 27 kap. 18 § andra stycket 4 och 20 a § andra stycket 4 RB. De brottsbekämpande myndigheterna har angett att en möjlighet att använda de aktuella tvångsmedlen skulle kunna leda till att betydligt fler brott i de angivna kategorierna kan klaras upp än i dag. Det handlar då inte bara om möjligheten att hålla någon ansvarig för brottet utan också om möjligheten att identifiera de verkliga huvudpersonerna. Ett vanligt problem i brottsutredningar, och inte minst i utredningar om ekonomisk brottslighet, är att man lyckas utreda misstankar mot personer med en mindre roll i brottsligheten samtidigt som man inte kommer åt de verkliga huvudmännen.

Vi kan inte se att motsvarande resultat skulle kunna uppnås med några andra tillgängliga tvångsmedel eller andra, mindre ingripande, utredningsåtgärder.

I sammanhanget finns det även skäl att lyfta fram att det nuvarande regelverket i vissa fall ger en möjlighet för gärningspersonerna att anpassa sin brottsliga verksamhet till regelverket och därigenom undvika risken att utsättas för hemliga tvångsmedel. En sådan möjlighet har vi nämnt i samband med skattebrottslighet, där gärningspersonen exempelvis genom att välja redovisningsperiod kan påverka om det blir fråga om ett eller flera brott. Det är otillfredsställande att personer som ägnar sig åt organiserad eller systematisk brottslig-

het på detta sätt kan påverka de brottsbekämpande myndigheternas möjligheter att utreda brotten.

Åklagarmyndigheten har även lyft fram en internationell dimension på frågan. Myndigheten framhåller att dagens reglering kan hindra svenska myndigheter från att genom rättslig hjälp bistå andra länders brottsbekämpande myndigheter med hemliga tvångsmedel vid seriebrottslighet, t.ex. när det gäller stölder av stöldligor som kommer till Sverige. Enligt Åklagarmyndigheten gäller i många andra länder att hemliga tvångsmedel alltid kan användas vid organiserad brottslighet, varför den svenska regleringen kan uppfattas som svag.

Med hänsyn till det anförda gör vi bedömningen att det finns ett behov av en möjlighet för de brottsbekämpande myndigheterna att använda hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet och hemlig kameraövervakning även i vissa fall av flerfaldig brottslighet där de enskilda ingående brotten har ett straffvärde som inte når upp till de nuvarande straffvärdeventilerna.

Behovet gäller även hemlig dataavläsning

De argument som anförts i fråga om behovet av hemlig avlyssning och hemlig övervakning av elektronisk kommunikation samt hemlig kameraövervakning gör sig i lika hög grad gällande i fråga om hemlig dataavläsning som avser kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter, platsuppgifter och kameraövervakningsuppgifter. Uppgifterna är nämligen till sin typ sådana som får hämtas in genom hemlig avlyssning respektive hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning. Behovet av uppgifterna är alltså detsamma. Ett huvudsyfte med införandet av hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter var att motverka att de andra hemliga tvångsmedlen hade förlorat mycket av sin effektivitet på grund av den tekniska utvecklingen och den ökade användningen av bl.a. kryptering och anonymisering (prop. 2019/20:64 s. 69–72). Det ansågs även behövligt med en ny metod för att genomföra kommunikationsövervakning och kameraövervakning (anförd prop. s. 72–74).

Om det införs en ny straffvärdeventil i fråga om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet och hemlig kameraövervakning, utan att motsvarande straffvärdeventil även införs i fråga om hemlig dataavläsning, finns det en uppenbar risk för att den önskade effekten av den nya straffvärdeventilen till stor del uteblir. Bestämmelserna om hemlig dataavläsning bör därför i det nu aktuella avseendet korrespondera med bestämmelserna om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas och hemlig kameraövervakning.

Vi anser att det även finns behov av en möjlighet att använda hemlig dataavläsning i syfte att hämta in uppgifter av de slag som regleras i 2 § första stycket 6 och 7 lagen om hemlig dataavläsning, dvs. uppgifter som finns lagrade i ett informationssystem och uppgifter som visar hur ett informationssystem används. Dessa uppgiftstyper kan i dag hämtas in vid utredningar om samma slags brott som kan leda till hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. Om användningsområdet för hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning utvidgas finns det starka systematiska skäl för att motsvarande utvidgning görs i fråga om de nu aktuella uppgiftstyperna. De brottsbekämpande myndigheterna har vidare anfört att tillstånd till åtgärder enligt punkterna 6 och 7 ofta är ett viktigt komplement till de uppgifter som avses i punkterna 1–4. Hemlig dataavläsning kan verkställas på olika sätt och mot olika former av avläsningsbara informationssystem. Med detta avses inte bara exempelvis fysiska informationsbärare såsom datorer och mobiltelefoner utan också molnbaserade användarkonton, såsom webbmejlkonton och webbchattar. Som framgått i det föregående är ett av syftena med hemlig dataavläsning att man ska kunna komma åt viss information som inte är tillgänglig med t.ex. hemlig avlyssning av elektronisk kommunikation. Typexempel kan vara krypterade appar och e-postkonton. För att i praktiken kunna avläsa t.ex. kommunikationsavlyssningsuppgifter kan det krävas att man först tar reda på vilka programvaror eller applikationer som användaren har installerade på informationsbäraren och som används för kommunikation med andra. Ett sätt att komma fram till detta är att inhämta uppgifter som visar hur ett avläsningsbart informationssystem används, dvs. sådana uppgifter som avses i 2 § första stycket 7

lagen om hemlig dataavläsning. För verkställigheten av hemlig dataavläsning för uppgiftstyperna under punkterna 1–4 är det därtill i vissa fall till stor nytta att ta reda på lösenord och användarnamn för vissa applikationer och liknande genom inhämtning av sådana uppgifter som avses i p. 6, dvs. uppgifter som finns lagrade i ett avläsningsbart informationssystem. Det anförda kan illustreras med följande exempel.

I ett typiskt fall tillämpar de brottsbekämpande myndigheterna först hemlig avlyssning av elektronisk kommunikation i syfte att se om en viss telefon används i någon större utsträckning för datatrafik. Om så är fallet kan det vara lönt att gå vidare med en ansökan om tillstånd till hemlig dataavläsning. Ansökan avser då vanligen inte enbart exempelvis kommunikationsavlyssningsuppgifter, utan även uppgifter som avses i 2 § första stycket 6 och 7. I praktiken går det då ofta till så att man genom avläsning enligt punkten 7 kan få kunskap om vilka appar eller andra molntjänster av olika slag som är intressanta att rikta in sig mot. När man vet vilka molntjänster, e-postkonton eller liknande som är av intresse för utredningen kan man i nästa skede rikta sig direkt mot dessa. Dessa utgör i sig sådana avläsningsbara informationssystem som nya beslut om hemlig dataavläsning kan avse. Vilken telefon som den misstänkte använder är då inte längre av primärt intresse och det spelar ingen roll om den misstänkte sedan byter telefon för sin åtkomst till dessa konton och molntjänster.

Med hänsyn till det anförda gör vi bedömningen att behovet gäller inte bara uppgifter enligt punkterna 1–4 utan också de uppgifter som avses i punkterna 6 och 7.

6.7 Utformningen av en ny straffvärdeventil för hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning

Bedömning: Om en ny straffvärdeventil införs, bör den vara tillämplig på flerfaldig brottslighet som kan antas ha utövats i organiserad form eller systematiskt och som har ett sammanlagt straffvärde som kan antas överstiga fängelse i två år. Vid sammanläggningen bör man endast få beakta brott som kan antas utgöra ett led i denna brottslighet och för vilka det är förskrivet fängelse i ett år eller däröver och försök, förberedelse eller stämpling till sådana brott.

Skälen för bedömningen

Nästa fråga är hur en eventuell straffvärdeventil vid flerfaldig brottslighet bör utformas i fråga om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning avseende sådana uppgifter som kan åtkommas genom dessa tvångsmedel samt uppgifter enligt punkterna 6 och 7. Vi måste då ta ställning till i vilka situationer och vid vilka straffvärden en sådan möjlighet bör kunna tillämpas om den införs.

Misstankarna bör röra en och samma person

Vi gör till att börja med bedömningen att det måste vara fråga om flera misstankar som avser en och samma misstänkta gärningsman. Teoretiskt går det visserligen att tänka sig att man lägger samman misstankar som riktar sig mot flera personer som ingår i en viss kriminell organisation eller liknande sammanslutning, men något sådant framstår som främmande för hur den svenska regleringen är uppbyggd och väcker allvarliga principiella betänkligheter. Vi anser därför att en sådan lösning kan avfärdas utan vidare. Det bör alltså handla om flera brottsmisstankar mot en och samma person.

Frågan är vad ovanstående innebär i fall där hemliga tvångsmedel används i syfte att utreda vem som skäligen kan misstänkas. En sådan möjlighet finns redan i dag avseende hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning som gäller motsvarande slags uppgifter. Vi föreslår vidare i kapitel 9 att det införs en möjlighet att i vissa fall använda hemlig avlyssning av elektronisk kommunikation och motsvarande hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas. Det kan, med hänsyn till syftet med åtgärden och utredningsläget då den kan användas, knappast krävas att det är visat att en och samma person begått gärningarna. Dock bör det krävas att det finns konkreta omständigheter som talar för att så är fallet. Det kan t.ex. handla om situationer där ett visst nummer ringer upp en och samma målsägande flera gånger och målsäganden uppger att han eller hon känner igen rösten, eller där tillvägagångssättet eller sambanden mellan brotten är sådant att det finns anledning att anta att misstankarna avser en och samma person eller flera personer som gemensamt och i samförstånd begår brotten.

Det samlade straffvärdet bör överstiga fängelse i två år

Nästa fråga är hur högt det samlade straffvärdet bör vara för att en eventuell straffvärdeventil ska vara tillämplig. En utgångspunkt är att detta samlade straffvärde minst måste motsvara det som gäller enligt den nuvarande straffvärdeventilen i 27 kap. 18 § andra stycket 4, dvs. att straffvärdet kan antas överstiga fängelse i två år. En lägre gräns framstår inte som godtagbar av principiella och systematiska skäl och skulle enligt vår bedömning endast kunna komma i fråga om man även justerar övriga straffvärdetrösklar i bestämmelserna om hemliga tvångsmedel. Något sådant ryms inte inom vårt uppdrag och skulle fodra överväganden som vi inte heller har möjlighet att göra.

Det är dock inte självklart att gränsen ska dras just vid ett samlat straffvärde överstigande två års fängelse. Man kan nämligen även tänka sig att det ställs högre krav i fråga om det samlade straffvärdet när det är fråga om flerfaldig brottslighet, i syfte att straffvärdeventilen enbart ska kunna komma till användning i de mest kvalificerade fallen. Samtidigt får kraven inte sättas alltför högt, eftersom det skulle innebära att en eventuell ny straffvärdeventil blir en chimär. En straffvärdeventil som får ett alltför snävt tillämpningsområde kan inte förväntas leda till de förbättrade möjligheter att utreda brott som man önskar åstadkomma. Här måste man särskilt beakta att svensk straffmätningspraxis är sådan att domstolarna sällan utnyttjar den övre delen av straffskalan och även principerna för bestämmande av straffvärdet för flera brott (se avsnitt 6.2.2). Som vi kommer att återkomma till i avsnitt 6.10 skulle en gräns för brott där det krävs mer av det sammanlagda straffvärdet än att det överstiger två års fängelse utgöra en påtaglig begränsning av användningsområdet. Vidare bör man undvika alltför många olika gränser i den redan komplicerade regleringen.

Av det sagda framgår att vi i praktiken bedömer det som uteslutet att föreskriva om en lägre straffvärdetröskel och att en högre tröskel skulle leda till att ändringen inte får önskad effekt. Vår bedömning är dock även att ett krav på att det samlade straffvärdet överstiger två år är väl avvägt, sammantaget med de ytterligare krav som vi föreslår i det följande. Vi föreslår i nästa avsnitt att en eventuell straffvärdeventil endast ska vara tillämplig i fråga om brottslighet som begås systematiskt eller organiserat, vilket är i sig kvalificerande.

Det bör krävas att brottsligheten är organiserad eller systematisk

Vidare anser vi att en sammanläggning av flera brottsmisstankar på det sätt som nu är aktuellt endast är rimlig om det finns ett tydligt samband mellan brotten utöver det faktum att brottsmisstankarna avser en och samma person, och att detta samband i sig är kvalificerande. En eventuell ventil bör inte vara tillämplig på t.ex. de klassiska ”missbrukarfallen”, där en och samma person begår ett stort antal stölder, ringa narkotikabrott, grova olovliga körningar, grova rattfyllerier och annan liknande brottslighet. Det bör därför krävas ytterligare kvalificerade faktorer utöver det faktum att en och samma person är misstänkt för flera brott med ett visst samlat straffvärde.

De brottsbekämpande myndigheternas behovsbeskrivning talar för att behovet av en eventuell straffvärdeventil för flerfaldig brottslighet främst gäller förundersökningar som avser brottslighet som har utövats i organiserad form eller systematiskt.

Det finns inte någon legaldefinition av begreppet organiserad brottslighet och inte heller någon enhetlig definition. I straffskärpningsbestämmelsen i 29 kap. 2 § 6 BrB talas om ”brott som utgjort ett led i en brottslighet som utövats i organiserad form”. Enligt förarbetena avses med detta brottslighet som har begåtts inom ramen för en struktur där flera personer samverkat under en inte helt obetydlig tidsperiod för att begå brott. Det är vidare inte tillräckligt att det aktuella brottet har skett i samverkan utan personerna ska ha ingått i en sammanslutning eller ett nätverk av viss kontinuitet vars syfte att begå brott sträckt sig längre än till enbart det ifrågavarande brottet (se avsnitt 6.2.3). Bestämmelsen träffar tveklöst brottslighet som begås inom ramen för kriminella nätverk med en tydlig struktur, såsom mc-gäng. I viss utsträckning kan den även träffa brott som begås inom andra slags kriminella nätverk, såsom det som kan benämnas lokala kriminella nätverk. Det framgår dock av olika kartläggningar att många av dagens kriminella nätverk är löst sammansatta och föränderliga och att det inte alls är givet att de personer som deltar i brottsligheten själva anser att de är medlemmar i en organisation eller ett gäng (se bl.a. SOU 2021:68 s. 52–61). Långtifrån alla brott som begås inom kriminella nätverk omfattas av straffskärpningsgrundens definition av brott som begås organiserat. Mot denna bakgrund har Gängbrottsutredningen haft i uppdrag att överväga om straffskärpningsbestämmelsen bör utvidgas. Man har kommit fram till att nack-

delarna med en ändring överväger fördelarna och anför bl.a. följande (SOU 2021:68 s. 220 och 221).

> För att straffvärdet för ett brott ska kunna skärpas med stöd av den aktuella punkten krävs det att det är utrett att brottsligheten har skett inom ramen för en sådan struktur som avses i bestämmelsen (se avsnitt 8.2.3). Det har hävdats att bestämmelsen kan tillämpas i förhållande till sådan gängbrottslighet som förekommer i vissa förorter. Det bör dock stå klart att sådana löst sammansatta kriminella nätverk i utsatta områden, vilka är av särskilt intresse för vårt arbete och som till stor del kan knytas till de senaste årens skjutningar och sprängningar, inte alltid har en sådan organiserad form som avses i bestämmelsen (se bl.a. avsnitt 7.2 och 3.3.2). Under alla förhållanden torde det i många fall vara svårt att bevisa att de nuvarande förutsättningarna i punkten är uppfyllda i förhållande till sådana, och andra, kriminella nätverk med en lägre grad av organisation …
>
> Enligt vår mening framstår det dock inte som lämpligt att utmönstra eller förändra det aktuella kravet i sjätte punkten. Det vill säga kravet att det dels ska vara fråga om att den aktuella gärningen ingått som ett led i viss brottslighet, dels att denna brottslighet ska ha skett i organiserad form. Om det skulle göras behöver dessa förutsättningar kompletteras eller ersättas med något annat slags krav. Till exempel att brottsligheten skett i ett kriminellt nätverk eller av en gärningsperson som på något sätt ingår i ett sådant nätverk.
>
> En sådan till synes enkel lösning (som t.ex. hänvisar till att det ska vara fråga om brott i ett kriminellt nätverk) skulle dock riskera att medföra tolkningsproblem och bli för oprecis från förutsebarhetssynpunkt, om det inte samtidigt definieras vad ett kriminellt nätverk är. Det är i sin tur en uppgift som är förenad med uppenbara svårigheter. Begreppet är till sin natur brett och omfattar ett stort antal företeelser, vilket har behandlats i avsnitt 3.3.1. Som utvecklats i nämnda avsnitt finns inte någon definition av begreppet i svensk rätt i dag och det vore, med hänsyn till begreppets omfång, svårt att införa en sådan i lag (se även avsnitt 7.2).
>
> I andra nordiska länder finns visserligen definitioner avseende organiserade kriminella sammanslutningar. Dessa framstår dock som införda i huvudsak mot bakgrund av mer traditionell och välstrukturerad organiserad brottslighet (se avsnitt 5.1, 5.3.1 och 5.4.1).
>
> I praktiken skulle det dessutom fortfarande ofta bli fråga om att åklagaren på något sätt behöver knyta en person eller gärning till en gruppering eller verksamhet, vilket kan bli svårt när det gäller brottslighet i sådana löst sammansatta konstellationer som i dag är vanliga och som utgör en tydlig del av problembilden.
>
> Det kan även ifrågasättas om brottets skada eller fara regelmässigt blir allvarligare endast utifrån det förhållande i sig att brottet skett i eller med anknytning till ett kriminellt nätverk, om det samtidigt inte ställs något slags kvalificerade krav på gruppens utformning eller på hur den brottsliga verksamheten bedrivs. Också detta talar emot en ändring av bestämmelsen.

Vi instämmer i Gängbrottsutredningens bedömning att det inte framstår som lämpligt att försöka skapa någon annan definition av organiserad brottslighet eller kriminella nätverk. Det är vidare uppenbart att det, inte minst i ett tidigt skede av en förundersökning, kan vara svårt att lägga fram bevisning om att en viss brottslighet utgör ett led i organiserad brottslighet. Däremot menar vi att det, i de fall en sådan utredning finns och det handlar om brottslighet som är organiserad i den mening som avses i 29 kap. 2 § 6 BrB är rimligt att den samlade brottsligheten och inte enbart varje enskilt brott för sig kan beaktas vid ställningstagandet av om hemliga tvångsmedel ska kunna användas. Även om tillämpningsområdet i praktiken kan förväntas bli relativt begränsat anser vi därför att en eventuell straffvärdeventil för flerfaldig brottslighet bör omfatta brott som utgör ett led i en brottslighet som begås organiserat, i den bemärkelse som avses i straffskärpningsbestämmelsen. Vi återkommer till frågan om vilken bevisning som bör krävas för att straffvärdeventilen ska bli tillämplig.

Straffskärpningsgrunden i 29 kap. 2 § 6 BrB omfattar även bl.a. brott som utgjort ett led i en brottslighet som utövats systematiskt. Med bestämmelsen avses brottslighet där ett visst tillvägagångssätt upprepats ett flertal gånger av antingen en ensam gärningsman eller av flera personer i samförstånd. Som ett exempel nämns i förarbetena att någon vid upprepade tillfällen förmått annan till utbetalning av en förmån som han eller hon inte har haft rätt till. Ett annat exempel som nämns är om flera personer rånat olika butiker eller banker och då gått till väga på ett likartat sätt vid varje tillfälle. Detta slags seriebrottslighet som upprepar sig på ett likartat sätt kan sägas utgöra kärnan i de fall som de brottsbekämpande myndigheterna har pekat ut i sin beskrivning av behovet av en straffvärdeventil för flerfaldig brottslighet. Vi bedömer att det är både lämpligt och rimligt att straffvärdet för de brott som ingår i en sådan brottslighet bedöms samlat när det handlar om möjligheten att använda hemliga tvångsmedel. Även i dessa fall väcks dock frågan om vilken bevisning som bör krävas för att straffvärdeventilen ska kunna tillämpas. Vi återkommer till den frågan i det följande.

Eftersom det här handlar om bedömning av flera brott bör det krävas inte bara att det är fråga om organiserad eller systematisk brottslighet, utan även att vart och ett av de brott som omfattas av sammanläggningen har utgjort ett led i den organiserade eller systematiska brottsligheten. Det bör alltså krävas att varje ingående brott har haft

ett naturligt samband med brottsligheten. Om en person misstänks dels för flera brott som utövats systematiskt eller i organiserad form, dels något brott som inte ingår i den brottsligheten, bör det sistnämnda brottet enligt vår mening alltså inte räknas in i sammanläggningen. Däremot hindrar ingenting att hemlig avlyssning används i fråga om det brottet förutsatt att detta är möjligt på någon annan grund, t.ex. för att det har ett minimistraff på två års fängelse eller däröver. Vidare bör ingenting hindra att olika slags brott, som ingår som ett led i en systematisk brottslighet, sammanläggs. Som ett exempel kan nämnas att systematiska grova stölder och grova hälerier avseende stöldgods. I det fallet framstår hälerierna som en del av ett gemensamt brottsupplägg. Detsamma kan gälla vid skattebrott och bokföringsbrott, där bokföringsbrottet är en del av brottsupplägget, eller grova bedrägerier där olovlig identitetsanvändning ingår i brottsupplägget. Det kan förekomma att någon misstänks för en organiserad eller systematisk brottslighet där något eller några av gärningarna kan leda till hemlig avlyssning medan några av gärningarna inte har ett tillräckligt högt minimistraff eller straffvärde. Förutsatt att villkoren i övrigt är uppfyllda bör även sådan brottslighet kunna bedömas samlat och föranleda hemlig avlyssning m.m. även i fråga om de brott som inte sedda för sig har denna dignitet.

Vi har övervägt om det i en eventuell straffvärdeventil bör krävas att brottsligheten ska vara både organiserad och systematisk. Vi konstaterar att brottslighet kan vara allvarlig och organiserad utan att för den sakens skull ske systematiskt. Vidare kan allvarlig brottslighet ske systematiskt av en ensam gärningsman eller annars i former som inte kan betecknas som organiserade. Ett typexempel på detta kan vara ekonomisk brottslighet som ofta utövas systematiskt men utan att den är organiserad. Ett krav på att brottsligheten är både organiserad och systematisk skulle således leda till att många av de brott som nya straffvärdeventiler skulle ta sikte på inte fångas in. Det bör därför, om nya ventiler införs, vara tillräckligt att brottsligheten är antingen organiserad eller systematisk.

Beviskravet

Straffskärpningsgrunden i 29 kap. 2 § 6 är utformad på ett sådant sätt att dess tillämpning förutsätter att det är styrkt att förhållandena är sådana som avses med bestämmelsen. Under en förundersökning kan antas att det oftast är omöjligt att förebringa full bevisning om att det förhåller sig så. I själva verket är det många gånger en av de omständigheter som förundersökningen syftar till att klarlägga. Ett krav på att det är styrkt att brottsligheten är organiserad eller systematisk och att varje brott är ett led i sådan brottslighet skulle enligt vår bedömning innebära att en ny straffvärdeventil får ett synnerligen begränsat användningsområde. Kravet måste därför sättas lägre, om en straffvärdeventil ska bli effektiv.

Frågan är då var nivån bör läggas för att en eventuell straffvärdeventil ska bli tillräckligt effektiv, samtidigt som det ställs tillräckligt höga krav på bevisning i fråga om att brottsligheten är sådan att det är godtagbart att straffvärdet bedöms samlat vid tillämpning av bestämmelser om hemliga tvångsmedel. Vår bedömning är att beviskravet bör vara att det *kan antas* att vart och ett av brottet har utgjort ett led i en organiserad eller systematisk brottslighet. Ett högre ställt krav skulle enligt vår mening leda till att bestämmelserna sällan kan tillämpas i praktiken, och således förlorar alltför mycket av sin tänkta effektivitet.

De ingående brotten bör vara häktningsgrundande

Slutligen är frågan om det bör ställas något krav avseende allvaret hos de ingående brotten. Ett skäl som talar emot det är att syftet med en straffvärdeventil är just att kunna utreda även mindre allvarliga brott som ingår i ett större sammanhang. En bärande tanke är att de mindre allvarliga brotten kvalificeras genom att de ingår i detta större sammanhang. Samtidigt menar vi att det trots detta finns en nedre gräns för hur lindriga brott som bör kunna omfattas av hemliga tvångsmedel, även när de ingår i en organiserad eller systematisk brottslighet. Man kan visserligen argumentera för att en sådan gräns redan finns utan att man särskilt behöver föreskriva om det, genom de principer som gäller för bedömning av straffvärdet för flerfaldig brottslighet. Eftersom dessa innebär att man utgår ifrån straffvärdet för det allvarligaste brottet och sedan lägger till en successivt minskande kvotdel av övriga brott är det i realiteten knappast möjligt att

lägga samman enbart bagatellartade brott och komma upp i ett samlat straffvärde som överstiger två års fängelse. Man kan dock tänka sig att en person misstänks för såväl något eller några allvarligare brott med ett högt straffvärde som ett flertal lindriga brott och att det samlade straffvärdet då överstiger två år. Hemliga tvångsmedel skulle då kunna komma att vara möjliga även för dessa lindriga brott om de ingår i en sammanläggning. Vi anser att detta är tveksamt från principiella utgångspunkter. Vidare är det viktigt att regler om hemliga tvångsmedel är särskilt tydliga och förutsebara och innehåller garantier mot ett alltför vidsträckt tillämpningsområde. Detta talar för att nya straffvärdeventiler för flerfaldig brottslighet, om de införs, begränsas på så sätt att endast brott av en viss svårhet får tas med i sammanläggningen. I viss mån finns det även skäl att beakta att regeringen aviserat en skärpt syn på straff för flerfaldig brottslighet och gett en särskild utredare i uppdrag att lämna förslag till hur detta ska åstadkommas (dir. 2021:56). Vad en eventuell skärpning kan komma att innebära är i dagsläget oklart, men det är givetvis önskvärt att våra förslag står sig även om principerna för straffvärdebedömningen vid flerfaldig brottslighet skulle komma att ändras. Med beaktande av det anförda anser vi att det bör ställas upp ett särskilt krav i fråga om de brott som får ingå i en sammanläggning enligt en eventuell ny straffvärdeventil. De alternativ som framstår som tänkbara är då

1. att det ställs krav på att brottet har ett visst lägsta minimistraff, t.ex. fängelse i sex månader,
2. att det ställs krav på att varje enskilt brott kan antas ha ett visst lägsta straffvärde,
3. att endast brott som ingår i en särskild brottskatalog omfattas av straffvärdeventilen, eller
4. att det för brottet är föreskrivet ett visst högsta straff (jfr 24 kap. 1 § häktning) eller att fängelse är föreskrivet för brottet.

Det första alternativet, dvs. krav på att brottet har ett visst lägsta minimistraff, har fördelar. Om man i så fall skulle sätta gränsen vid att minimistraffet är sex månaders fängelse eller mer skulle det täcka in flera av de fall som kan aktualiseras, såsom flerfaldiga grova bokföringsbrott, grova skattebrott, grova stölder och grova bedrägerier. Samtliga dessa brott har nämligen minimistraffet fängelse i sex måna-

der. Det finns dock även vissa brott som har ett lågt minimistraff men en vid straffskala. Vid flerfaldig brottslighet av detta slag kan det förekomma att de ingående enskilda gärningarna har ett högt straffvärde, som dock inte når upp till de nuvarande straffvärdeventilerna för enstaka brott. Ett exempel kan vara upprepade fall av sabotage mot blåljusverksamhet (13 kap. 5 c § BrB). Man kan eventuellt tänka sig att upprepade fall av sådan brottslighet av allvarligt slag men som inte når upp till gränsen för grovt brott skulle kunna ha ett samlat straffvärde som överstiger fängelse i två år. Även sådana brott bör enligt vår mening kunna inräknas. Vidare förekommer det ärenden med ett stort antal brott där vissa av dem är grova, t.ex. grova bedrägerier, medan andra är av normalgraden och alltså inte har ett minimistraff på sex månaders fängelse eller mer. Förutsatt att det samlade straffvärdet överstiger två år bör även normalgradsbrotten enligt vår mening kunna inräknas. En gräns vid att minimistraffet som lägst är sex månaders fängelse framstår med hänsyn till det anförda som mindre lämpligt. Att lägga tröskeln vid att brottet har fängelse i straffskalan skulle innebära att även bagatellartade brott såsom ringa narkotikabrott och grov olovlig körning skulle kunna ingå i sammanläggningen, vilket som vi redan nämnt inte är önskvärt. Mot denna bakgrund framstår det inte som en optimal väg att använda ett visst lägsta minimistraff som ett villkor för att en eventuell ny straffvärdeventil ska kunna tillämpas.

Det andra alternativet, dvs. att varje enskilt brott har ett visst lägsta antaget straffvärde framstår som en mer framkomlig väg. Eftersom det handlar om ett betydande integritetsintrång som dessutom inte bara kan drabba den misstänkte är det viktigt att inte alltför obetydliga brott kan föranleda hemliga tvångsmedel. Det är nödvändigt att göra en preliminär bedömning av de enskilda brottens straffvärde för att kunna bedöma brottslighetens samlade straffvärde. Som vi har framhållit tidigare är detta dock förknippat med särskilda problem när det gäller den ekonomiska brottsligheten och skattebrottsligheten. Vi ser därför att ett sådant krav kan ställa till svårigheter i en hel del av de fall som en ny straffvärdeventil särskilt skulle ta sikte på. Det är också en ordning med mindre stadga och förutsebarhet än en ordning som knyter an till exempelvis straffskalan för brottet.

Det tredje alternativet är att man knyter den eventuella nya straffvärdeventilen till en viss brottskatalog, som är inriktad på de brott som typiskt sett ingår i det slags brottslighet som nu är aktuell. Fördelen med en brottskatalog är att det skapar viss stadga och förut-

sebarhet. En avsevärd nackdel är dock att det också är svårt att exakt förutse för vilka brott det kan finnas ett behov. Detta kan leda till att det framstår som slumpmässigt när den eventuella nya straffvärdeventilen kan tillämpas och inte. Vidare skulle lösningen med en brottskatalog innebära att det uppstår en viss tröghet och otymplighet som innebär att de brottsbekämpande myndigheternas möjligheter att utreda brotten inte hänger med när den organiserade brottsligheten förändras, något som kan ske snabbt i takt med att de kriminella anpassar sig till ny teknik, de brottsbekämpande myndigheternas möjligheter att vidta åtgärder och andra förändringar i samhället. Det har gång efter annan visat sig att de kriminella har förmåga att ligga steget före lagstiftaren, exempelvis när det gäller narkotiska preparat. Trots att lösningen har vissa fördelar anser vi att nackdelarna överväger, varför vi inte föreslår denna metod.

Det fjärde och sista alternativet är att man knyter möjligheten att använda hemliga tvångsmedel med stöd av en ny straffvärdeventil till vilket straff brottet kan leda till, dvs. det strängaste straff som är föreskrivet för brottet. Denna metod används i dagsläget inte när det gäller de hemliga tvångsmedlen men däremot i fråga om häktning (jfr 24 kap. 1 § RB). För häktning krävs att fängelse i ett år eller däröver är föreskrivet för brottet. För husrannsakan krävs i stället misstanke om ett brott på vilket fängelse kan följa (28 kap. 1 § RB). Metoden att knyta möjligheten att använda hemliga tvångsmedel till det högsta straff som kan följa på brottet används i den danska retsplejeloven. Där gäller bl.a. att hemlig telefonavlyssning får ske endast för brott som kan föranleda sex års fängelse (§ 781 retsplejelov). För hemlig dataavläsning ställs samma krav eller att gärningen avser brott mot vissa bestämmelser om bl.a. landsförräderi och andra brott mot Danmarks självständighet och säkerhet. Metoden att utgå från det strängaste straffet i straffskalan används även i finsk rätt. Bland annat får teleövervakning ske om förundersökningen gäller ett brott för vilket det föreskrivna strängaste straffet är fängelse i minst fyra år eller ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste straffet är fängelse i minst två år (10 kap. 6 § tvångsmedelslagen). Paragrafen innehåller också en brottskatalog. Metoden används även i norsk rätt. Som ett exempel kan nämnas att hemlig kameraövervakning på en privat plats får användas i fråga om ett brott eller ett försök till brott

som kan medföra tio års fängelse eller mer eller som omfattas av en brottskatalog (§ 202 a. straffeprocessloven).

Av det föregående framgår att vi bedömer att alternativ 1 och 3 har vissa nackdelar. Det andra alternativet, dvs. ett krav på att varje ingående brott har ett visst lägsta straffvärde, är tänkbart men vi anser att det finns fler fördelar med det fjärde alternativet, dvs. att man knyter möjligheten att använda den nya ventilen till straffskalans övre gräns för de ingående brotten. Vi bedömer då att det är lämpligt att kräva att de brott som ingår i sammanläggningen är häktningsgrundande, dvs. att minst ett års fängelse är föreskrivet för vart och ett av dem. Detta är samma krav som gäller för häktning (24 kap. 1 § RB). Häktning är ett ingripande tvångsmedel, varför det framstår som rimligt att använda samma gräns i fråga om vilka brott som över huvud taget kan föranleda exempelvis hemlig avlyssning, under förutsättning att de ingår i en flerfaldig brottslighet som sammantaget framstår som allvarlig. Eftersom åklagare och domstolar är mycket vana vid att hantera häktningsfrågor är det även en gräns som är väl etablerad och kan förväntas vara lätt att tillämpa. Det är visserligen inte självklart att samtliga brott som kan vara häktningsgrundande alltid utgör grov brottslighet i den bemärkelse som enligt EU-domstolens praxis krävs för att det ska vara tillåtet med allvarliga ingrepp i de grundläggande rättigheter som anges i artiklarna 7 och 8 i EU:s rättighetsstadstadga i brottsbekämpande syfte (se bl.a. dom av den 2 mars 2021, Prokuratuur, C-746/18, punkt 33). Straffskalan sammantagen med det förhållandet att brottsligheten är systematisk eller organiserad innebär dock enligt vår bedömning att kravet på att brottsligheten ska vara grov är uppfyllt.

Vi återkommer i avsnitt 6.14 till hur man bör se på försök, förberedelse och stämpling till häktningsgrundande brott.

6.8 Det finns ett behov av en ny straffvärdeventil för hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter

Bedömning: Det finns ett behov av en ny straffvärdeventil avseende hemlig rumsavlyssning och hemlig dataavläsning i syfte att läsa av eller ta upp rumsavlyssningsuppgifter.

Skälen för bedömningen

Grundläggande förutsättningar

Det som sagts i föregående avsnitt om de grundläggande förutsättningarna för införande av utvidgade möjligheter att använda hemliga tvångsmedel gäller även i fråga om rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter. Här måste dock särskilt beaktas att hemlig rumsavlyssning och motsvarande form av hemlig dataavläsning anses vara de typiskt sett mest integritetskänsliga av de hemliga tvångsmedlen.

Ärenden där det finns skäl som talar för en ny straffvärdeventil

Åklagarmyndigheten har anfört att även straffvärdeventilen för hemlig rumsavlyssning bör ändras så att detta tvångsmedel kan användas vid flerfaldig brottslighet där brotten kan sägas ha utgjort ett led i en brottslighet som utövats i organiserad form eller systematiskt när straffvärdet för brottsligheten överstiger fängelse i fyra år. Myndigheten menar vidare att straffvärdeventilen både vid enstaka brott och flerfaldig brottslighet bör vara tillämplig oavsett brottstyp.

Som skäl för sin begäran om utvidgade möjligheter att använda hemlig rumsavlyssning har Åklagarmyndigheten anfört i huvudsak följande. Det finns situationer där hemlig rumsavlyssning inte får användas samtidigt som det kan finnas ett starkt behov av sådan avlyssning för att de brottsbekämpande myndigheterna ska kunna utreda allvarliga brott eller allvarlig samlad brottslighet. Det som gäller i fråga om hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning om seriebrottslighet som kan sägas vara organiserad eller systematisk och som upprepar sig på ett likartat sätt vid de olika brottstillfällena kan gälla även en samlad brottslighet av mycket allvarligt slag där det samlade straffvärdet överstiger fyra år. Vidare förekommer det att nätverk inom den organiserade brottsligheten växlar sin verksamhet mellan olika typer av brott beroende på tillfälle och möjlighet till utbyte. Detta gäller i än högre grad i dag än förut. Till detta kommer att andra hemliga tvångsmedel, såsom hemlig avlyssning av elektronisk kommunikation, numera kan vara verkningslösa i de kriminella miljöer där mycket allvarliga brott begås. De personer som är inblandade i den sortens brottslighet är nämligen, som

redan konstaterats, mycket riskmedvetna och tenderar att anpassa sitt beteende utifrån risken att deras elektroniska kommunikation avlyssnas.

Även utanför den organiserade brottsligheten kan det enligt vår bedömning finnas ett starkt behov av hemlig rumsavlyssning vid utredningar av allvarliga brott som begås systematiskt, oavsett vilken typ av brott det är fråga om. Här kan exempelvis nämnas allvarlig skattebrottslighet och annan ekonomisk brottslighet, såsom grova bokföringsbrott – som inte sällan begås i syfte att dölja den grova skattebrottsligheten. Ett typiskt exempel är undandragande av punktskatt avseende tobak. Eftersom både punktskatten och efterfrågan på billig tobak är hög, finns det stora pengar att tjäna samtidigt som skatteundandragandet snabbt blir betydande. Enligt lagen (1994:1563) om tobaksskatt är den som yrkesmässigt för in eller tar emot snus från ett annat EU-land skattskyldig för snuset. Skattskyldigheten inträder när snuset förs in till Sverige. Den som är skattskyldig ska redovisa punktskatten i en särskild deklaration som ska ha kommit in till Skatteverket senast fem dagar efter införseln. Skatten tas ut per kilo snus. Det förekommer allt oftare att personer vid ett stort antal tillfällen för in snus i landet utan att deklarera och redovisa för den punktskatt som belöper på snusinförseln, eller att endast en mindre del av den införda mängden redovisas. Den totala punktskatten som undandras genom förfarandet kan uppgå till tiotals miljoner kronor, vilket innebär att den sammanlagda brottsligheten har ett mycket högt straffvärde. Betraktar man varje enskilt införseltillfälle som ett brott har detta dock ett lägre straffvärde. I ett exempel från rättspraxis som vi tagit del av var det fråga om cirka 80 införseltillfällen och totalt 200 ton snus, vilket motsvarade ett totalt skatteundandragande på närmare 80 miljoner kronor. Straffvärdet är då uppemot sex års fängelse, medan straffvärdet för varje ingående införsel sedd för sig motsvarar mellan sex månaders och arton månaders fängelse.

Ett annat exempel på brott där det kan finnas ett behov av hemlig rumsavlyssning är upprepade sexuella övergrepp som begås digitalt, och då kanske särskilt övergrepp på barn. Det är förekommer i praxis att sådana övergrepp bedöms ha ett mycket högt sammanlagt straffvärde, som med marginal överstiger fyra års fängelse. Däremot är det ovanligt att ett enstaka sexuellt övergrepp online bedöms ha ett så högt straffvärde att hemlig rumsavlyssning kan komma i fråga, och regeringens redogörelse för användningen av hemliga tvångsmedel visar också att det är mycket sällsynt att sådana tvångsmedel används

vid misstanke om sexualbrott, fastän flera sådana brott omfattas av brottskatalogen i 27 kap. 20 d § andra stycket 4 RB. Hemlig rumsavlyssning skulle exempelvis kunna bli aktuellt när det finns en skälig misstanke om att en viss person begår systematiska övergrepp online, men att det inte finns tekniska möjligheter att med hjälp av hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning få tillgång till bevisning om övergreppen. Det kan då tänkas att en hemlig rumsavlyssning kan generera sådan bevisning, vilket kan leda till att övergrepp kan avbrytas, fortsätta övergrepp förhindras och till att gärningspersonen lagförs för redan begångna övergrepp. Det är vanligt att brottsligheten är systematisk på så sätt att gärningspersonen utarbetar ett tillvägagångssätt och sedan gång på gång använder sig av detta mot sina offer. Brottsligheten kan ha föregåtts av en noggrann planering. Gärningspersonen kan då exempelvis ha kartlagt offrets liv, familjemedlemmar och sociala kontakter i syfte att på olika sätt utnyttja detta mot offret. I grövre fall är det vanligt att gärningspersonen begår ett stort antal övergrepp och har åtskilliga offer. Det kan även förekomma att brotten begås organiserat av flera personer.

Som ytterligare ett exempel kan nämnas flerfaldig vapensmuggling som är grov men inte synnerligen grov smuggling. Sådan brottslighet utövas ofta organiserat eller systematiskt.

6.9 Utformningen av en ny straffvärdeventil för hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter

Bedömning: Om en ny straffvärdeventil införs för hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter, bör den vara tillämplig på flerfaldig brottslighet som kan antas ha utövats i organiserad form eller systematiskt, och som har ett sammanlagt straffvärde som överstiger fängelse i fyra år. Det bör inte krävas att de enskilda brotten ingår i en viss brottskatalog men däremot att vart och ett av brotten har ett minimistraff på sex månaders fängelse eller mer. Vidare bör det krävas att brotten kan antas utgöra ett led i den systematiska eller organiserade brottsligheten.

Förslag: Brottskatalogen i den straffvärdeventil som finns i rättegångsbalkens bestämmelse om hemlig rumsavlyssning slopas.

Skälen för bedömningen

Avstamp

De ställningstaganden som gjorts i fråga om de övriga tvångsmedel som omfattas av denna del av uppdraget är relevanta även när det gäller hemlig rumsavlyssning. Vi gör alltså bedömningen att även bestämmelserna om hemlig dataavläsning avseende rumsavlyssningsuppgifter bör korrespondera med bestämmelserna om hemlig rumsavlyssning. Vi gör vidare bedömningen att det måste röra sig om misstankar mot en och samma person och om brottslighet som är systematisk eller organiserad för att en eventuell ny straffvärdeventil vid flerfaldig brottslighet ska vara tillämplig.

Två frågor återstår. Den första är vilket samlat straffvärde för brottsligheten som bör utgöra den nedre gränsen för att en eventuell straffvärdeventil för flerfaldig brottslighet ska kunna tillämpas. Den andra är om det bör krävas någon ytterligare kvalifikation av de brott som ingår i brottsligheten för att en eventuell ventil ska kunna tillämpas i fråga om hemlig rumsavlyssning och hemlig dataavläsning som avser rumsavlyssningsuppgifter. Här skiljer sig förutsättningarna åt i förhållande till de tvångsmedel som diskuterats i avsnitt 6.6 och 6.7, dels på det sättet att det straffvärde som krävs för att den nuvarande ventilen ska kunna tillämpas är fängelse överstigande fyra år, dels att brottet måste ingå i bestämmelsens brottskatalog.

Det ingår i vårt uppdrag inte bara att överväga om den nya straffvärdeventilen bör vara förenad med en brottskatalog utan också om brottskatalogen i den befintliga ventilen bör avskaffas. Frågorna hör så intimt samman att vi hanterar dem samlat. Frågan hänger givetvis även intimt samman med den allmänna frågan om vilka ytterligare kvalificerande faktorer som eventuellt bör krävs, utöver det samlade straffvärdet och att det är fråga om organiserad eller systematisk brottslighet.

Det samlade straffvärdet bör överstiga fängelse i fyra år

På samma skäl som anförts i avsnitt 6.7 gör vi bedömningen att det inte kan komma i fråga att sätta en lägre gräns i fråga om det samlade straffvärdet än vad som gäller enligt de nuvarande straffvärdeventilerna för hemlig rumsavlyssning och hemlig dataavläsning avseende rums-

avlyssningsuppgifter. Vi anser att gränsen inte heller bör sättas högre. Om kraven i fråga om samlat straffvärde för brottsligheten ställs högre är risken nämligen stor för att ventilen inte kommer att kunna användas i de fall där den mest behövs. Redan ett krav på straffvärde överstigande fyra år medför att tillämpningsområdet enligt vår mening blir tillräckligt begränsat. Vi bedömer vidare att det blir alltför komplicerat att tillämpa bestämmelserna om de två straffvärdeventilerna ställer olika krav på straffvärde.

Straffvärdeventilen bör inte knytas till en brottskatalog

När det gäller ytterligare kvalificerande faktorer har det betydelse att rumsavlyssning och motsvarande hemlig dataavläsning anses vara de typiskt sett mest integritetskränkande av de hemliga tvångsmedlen. Det kan därför hävdas att det är av särskild vikt att tvångsmedlet inte kommer i fråga vid förundersökningar om en omfattande brottslighet där de ingående brotten sedda för sig inte framstår som allvarliga. Samtidigt kan det, som nyss sagts, konstateras att redan ett krav på att det samlade straffvärdet överstiger fängelse i fyra år utgör en kraftigt begränsande faktor. Även om inga ytterligare krav ställs skulle det enligt de brottsbekämpande myndigheterna kunna handla om ett fåtal ärenden per år. Med hänsyn till den metod som tillämpas vid straffvärdebedömningar av flerfaldig brottslighet (den s.k. asperationsprincipen, se avsnitt 6.2.2), är det knappast möjligt att lägga ihop ett antal bagatellartade brott och nå upp till ett straffvärde som överstiger fyra års fängelse. Risken för att en ny straffvärdeventil leder till att man använder hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter för mindre allvarliga brott är därför liten. Dock kan det tänkas att en viss organiserad eller systematisk brottslighet innefattar dels något eller några mycket allvarliga brott, dels några som är mindre allvarliga, och att det samlade straffvärdet överstiger fyra års fängelse. Det bör då inte vara möjligt att inräkna dessa mindre allvarliga brott i sammanläggningen, och inte heller att använda hemliga tvångsmedel avseende dessa brott.

Med hänsyn till det anförda och av principiella skäl är det viktigt att det i lagtexten fastslås tydliga gränser som garanterar att tvångsmedlen enbart används i de allvarliga fall där det är motiverat. Kravet på att det sammanlagda straffvärdet för brottsligheten överstiger

fyra års fängelse och att varje brott kan antas vara ett led i en brottslighet som är organiserad eller systematisk bör därför kombineras med någon ytterligare kvalificerande faktor.

Frågan om en eventuell ny straffvärdeventil bör kombineras med en brottskatalog ställer sig något annorlunda än när det gäller exempelvis hemlig avlyssning av elektronisk kommunikation. Lagstiftaren har i fråga om hemlig rumsavlyssning valt att kombinera den nuvarande straffvärdeventilen med en brottskatalog. Syftet är att säkerställa att hemlig rumsavlyssning används restriktivt och endast är möjlig vid förundersökningar om vissa mycket allvarliga brott där det finns ett beskrivet och känt behov av att kunna använda tvångsmedlet (prop. 2005/06:178 och prop. 2013/14:237). Vi bedömer att de skäl som kan anföras för respektive emot en brottskatalog är i huvudsak desamma oavsett om det handlar om den befintliga straffvärdeventilen eller en eventuell ny straffvärdeventil för flerfaldig brottslighet. De nackdelar med användande av brottskataloger som vi har framhållit i avsnitt 6.7 gör sig gällande även här. Det är en otymplig metod som gör det möjligt för kriminella med goda insikter i de brottsbekämpande myndigheternas verktyg att anpassa sitt beteende efter regleringen. Det skapar en tröghet i systemet när kriminella hittar nya vägar att begå allvarliga brott. Hemlig rumsavlyssning används nästan uteslutande vid förundersökningar om narkotikabrott, narkotikasmuggling och våldsbrott (jfr Regeringens skrivelse 2020/21:59 Redovisning av användningen av hemliga tvångsmedel under 2019). För vissa brott i brottskatalogen har tvångsmedlet aldrig använts. Exempelvis har man aldrig använt hemlig rumsavlyssning för att utreda grovt utnyttjande av underårig för sexuell posering. Vidare finns det synnerligen allvarliga brott som enligt dagens reglering inte kan föranleda hemlig rumsavlyssning. Ett exempel är grovt sabotage mot blåljusverksamhet (13 kap. 5 c § andra stycket BrB), som har livstids fängelse i straffskalan men ett minimistraff på två års fängelse. Det kan också vara så att behovet uppstår i ett enstaka speciellt och mycket allvarligt fall, som sedan sällan eller aldrig upprepas. Det anförda visar på svårigheten att träffsäkert förutse vilka brott som bör ingå.

Med hänsyn till de avsevärda nackdelar som det innebär anser vi det inte lämpligt att utöver kravet på ett straffvärde eller samlat straffvärde som överstiger fyra års fängelse dessutom kräva att brottet eller brotten i fråga ingår i en brottskatalog. Vi anser inte heller att det är nödvändigt för att man ska begränsa tillämpningsområden till mycket

allvarlig brottslighet. Vi anser däremot att det, för att tydliggöra tillämpningsområdet och skapa garantier för att tvångsmedlet endast används vid allvarlig brottslighet, bör ställas andra krav i fråga om de ingående enskilda brotten.

Det lägsta föreskrivna straffet för vart och ett av de ingående brotten bör vara sex månaders fängelse eller mer

Ett alternativ till en brottskatalog är att man ställer krav i fråga om de enskilda brottens straffvärde sedda för sig. Av samma skäl som anförts i avsnitt 6.7 anser vi att en sådan metod är mindre lämplig.

Ett annat alternativ är att man ställer krav i fråga om brottets minimistraff, t.ex. på så sätt att man kräver att det lägsta föreskrivna straffet ska vara fängelse i sex månader, ett år eller två år.

Det tredje och sista alternativet är att man ställer krav i fråga om straffskalans övre gräns. Vi har förordat en sådan lösning när det gäller hemlig avlyssning av elektronisk kommunikation och de övriga tvångsmedel som diskuteras i avsnitt 6.7. Där har vi förordat alternativet att de ingående brotten ska vara häktningsgrundande, dvs. att ett års fängelse ingår i straffskalan.

Eftersom hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter även i fortsättningen bör vara förbehållet mycket allvarlig brottslighet bedömer vi att metoden att knyta straffvärdeventilen till det förskrivna minimistraffet är en framkomlig väg, förutsatt att man inte sätter gränsen så högt att många av de brott som föranleder ett behov av en ny straffvärdeventil faller utanför. Vi bedömer att en begränsning till brott med lägst två års fängelse som minimistraff innebär en alltför stor begränsning, som skulle leda till att den nya straffvärdeventilen inte kan användas effektivt. Även ett års minimistraff framstår som en alltför stor begränsning. Däremot skulle man genom att sätta gränsen vid brott som har ett minimistraff om lägst sex månaders fängelse sortera bort mindre allvarliga brott och samtidigt fånga upp organiserade och systematiska fall av exempelvis grova bokföringsbrott. Ett annat exempel är organiserade och systematiska fall av förmögenhetsbrott såsom grov stöld och grovt bedrägeri. Detta alternativ innebär ett högre ställt krav än att brottet enbart ska vara häktningsgrundande.

En konsekvens av den nyss diskuterade lösningen är att vissa brott som har ett lågt minimistraff men en vid straffskala utesluts från

tillämpningsområdet. Ett exempel är upprepade fall av sabotage av blåljusverksamhet som inte är grova men ändå bedöms ha ett högt straffvärde. Straffskalan för sabotage mot blåljusverksamhet börjar vid allmänt fängelseminimum och slutar på fängelse i fyra år. Det är ett brott som är mycket angeläget att man kan utreda och där det kan tänkas att samma person misstänks för upprepade brott. Brottet kan vidare ha koppling till brottslighet som begås inom kriminella nätverk (SOU 2021:68 s. 101). Ett annat exempel är människoexploatering, som har samma straffskala. Det kan i ett tidigt skede av en utredning vara svårt att få klarhet i om brottet är grovt eller inte, samtidigt som det är oerhört angeläget att det kan utredas. Detta brott har inte sällan koppling till organiserad brottslighet. Det kan i sammanhanget nämnas att Gängbrottsutredningen nyligen har föreslagit att utnyttjande av unga i brottslighet tas med i bestämmelsen om människoexploatering (SOU 2021:68 s. 250–260).

Det anförda talar i viss mån emot en begränsning till brott med ett minimistraff överstigande sex månaders fängelse. Samtidigt har det inte framkommit att behovet av hemlig rumsavlyssning är påtagligt framträdande när det gäller just de anförda brotten. Vidare gör vi bedömningen att endast en koppling till ett visst lägsta minimistraff utgör en tillräckligt stark garanti för att hemlig rumsavlyssning begränsas till tillräckligt allvarlig brottslighet. Även om det finns fördelar med en enhetlig metod anser vi det viktigare att nivån blir rätt. Vår bedömning är således att en eventuell ny straffvärdeventil bör utformas på det sättet att vart och ett av de brott som läggs samman ska ha ett minimistraff på sex månaders fängelse eller mer. Vi återkommer i avsnitt 6.14 till hur man bör se på försök, förberedelse och stämpling till sådana brott.

Brottskatalogen i den nuvarande straffvärdeventilen slopas

De skäl som vi har anfört till stöd för bedömningen att en eventuell ny straffvärdeventil inte ska kopplas till en brottskatalog gör sig gällande även i fråga om den nuvarande brottskatalogen i 27 kap. 20 d § RB andra stycket 4. Ett brott med ett straffvärde som överstiger fyra års fängelse är per definition mycket allvarligt. Någon ytterligare begränsning i fråga om enstaka brott med ett så högt straffvärde framstår enligt vår bedömning inte som nödvändigt och är dessutom, som

vi tidigare utvecklat, förknippat med betydande nackdelar inte minst på det sättet att det är oerhört svårt att förutse när tvångsmedlet kan vara nödvändigt för att ett allvarligt brott ska kunna utredas. Vi föreslår därför att brottskatalogen tas bort.

6.10 Nya straffvärdeventiler förväntas vara effektiva

Bedömning: En utvidgad möjlighet att vid viss flerfaldig brottslighet kunna utföra hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning förväntas göra det möjligt för de brottsbekämpande myndigheterna att få tillgång till uppgifter som dessa myndigheter har ett påtagligt behov av vid förundersökningar om organiserad och systematisk brottslighet. En sådan möjlighet bör därigenom kunna leda till att betydligt fler brott av detta slag kan klaras upp. Detsamma förväntas gälla hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet. Åtgärderna kommer dock inte att kunna genomföras i alla ärenden där det finns ett behov av dem.

Skälen för bedömningen

För att det ska vara motiverat att utvidga användningsområdet för de hemliga tvångsmedlen i förundersökningar, krävs det att man kan förvänta sig att det är en effektiv åtgärd såväl kvantitativt som kvalitativt.

En första fråga är då om de nya straffvärdeventiler som övervägs skulle komma till användning i tillräckligt många fall för att det ska vara motiverat att införa dem. Det måste då först och främst diskuteras om det är möjligt att redan under förundersökningen göra en tillräckligt bra straffvärdebedömning för flerfaldig brottslighet. När de nuvarande straffvärdeventilerna infördes, var just svårigheten att på ett tidigt stadium bedöma straffvärde en av de invändningar som framfördes. Regeringen gjorde då bedömningen att det inte torde vara någon avgörande skillnad mellan att på ett tidigt stadium bedöma om ett brott ska rubriceras på ett sådant sätt att en minimistraffregel är uppfylld och att bedöma detta brotts straffvärde (prop. 2002/03:74 s. 33). Systemet med offentliga ombud framhölls som en garant för

en allsidig belysning och den omständigheten att utredningen i vissa fall kan vara mindre robust ansågs innebära att en marginal till förmån för den misstänkte måste vägas in (anförd prop. s. 33 och 34). Kravet på att straffvärdet inte bara ska nå upp till utan även överstiga en viss nivå skapar en säkerhetsmarginal för den misstänkte. När det är fråga om flerfaldig brottslighet bör man räkna med att svårigheterna för tillämparen är större, liksom osäkerheten i bedömningen. Den metod som används, kallad asperationsprincipen, går ut på att rätten först fastställer ett straffvärde för vart och ett av brotten. Därefter utgår man från det allvarligaste brottet och lägger till en varefter minskande kvotdel av straffvärdet av den övriga brottsligheten. Avslutningsvis görs en samlad rimlighetsbedömning för att säkerställa att slutresultatet blir väl avvägt. Eftersom det handlar om att på angivet sätt lägga samman straffvärdet av flera brott kan en felaktig värdering för vart och ett av brotten få ett större utslag på det totala straffvärdet. Som framhållits i tidigare lagstiftningsärenden bör varje osäkerhet komma den misstänkte till godo. Vidare bör det som vi tidigare utvecklat gälla ett krav på att det sammanlagda straffvärdet ska överstiga två respektive fyra års fängelse, vilket skapar en säkerhetsmarginal till skydd för den misstänkte. Tillämpningssvårigheterna kan inte förväntas bli så stora att de nya straffvärdeventilerna får ett alltför snävt tillämpningsområde för att kunna motiveras.

Det är knappast möjligt att ta fram ett statistiskt underlag som visar hur många ytterligare utredningar som skulle kunna leda till åtal och fällande dom om man inför nya straffvärdeventiler med den utformning som vi bedömt vara lämplig (se avsnitt 6.7 och 6.9). Vi gör dock bedömningen att en sådan möjlighet bör kunna leda till att betydligt fler brott som utövats i organiserad form eller systematiskt kan klaras upp. En minst lika viktig effekt kan enligt de brottsbekämpande myndigheterna förväntas bli att möjligheterna ökar att framgångsrikt utreda vem eller vilka personer som är de egentliga huvudmännen i sådan brottslighet. Det är nämligen ett stort problem att man ofta enbart kan lagföra personer längre ner i organisationen medan de personer som har det bestämmande inflytandet går fria.

Samtidigt är det viktigt att upprepa att redan de straffvärdegränser vi föreslår innebär en påtaglig begränsning av tillämpningsområdet för nya straffvärdeventiler. Vi bedömer att hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter endast kan komma att aktualiseras i ett begränsat antal fall per år. Hemlig

avlyssning och hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning som inte gäller rumsavlyssningsuppgifter kan beräknas förekomma betydligt oftare, men ett betydande antal förundersökningar om organiserad eller systematisk brottslighet kan ändå förväntas falla utanför tillämpningsområdet eftersom det sammanlagda straffvärdet inte kan antas överstiga fängelse i två år. Med utgångspunkt i de behovsbeskrivningar som de brottsbekämpande myndigheterna gjort bedömer vi trots detta att användningsområdet blir tillräckligt stort för att nya straffvärdeventiler ska anses vara effektiva från kvantitativ synpunkt.

En kvalitativt effektiv metod är en metod som när den används i ett enskilt fall kan förväntas ge de uppgifter den används för att hämta in (se propositionen Hemlig dataavläsning, prop. 2019/20:64 s. 80). Motsvarande resonemang kan inte föras när det gäller frågan om införande av nya straffvärdeventiler, eftersom det handlar om tvångsmedel som redan används och som har bedömts vara tillräckligt kvalitativt effektiva för att vara tillåtna. Att tvångsmedlen är effektiva från kvalitativ synpunkt är således redan klarlagt. De svårigheter som kan vara förknippade med verkställigheten av bl.a. hemlig dataavläsning kan inte förväntas vara större i det slags ärenden som skulle omfattas av en straffvärdeventil än vad som gäller generellt.

Den omständigheten att kriminella och i synnerhet personer som ägnar sig åt organiserad och systematisk brottslighet har en hög riskmedvetenhet och därför anpassar sitt beteende på ett sätt som kan försvåra verkställighet av hemliga tvångsmedel, eller göra att de uppgifter man eftersöker inte fås fram genom verkställigheten (se bl.a. prop. 2019/20:64 s. 83), är inte någon nyhet och därför inte heller något tungt argument mot införande av nya straffvärdeventiler. Däremot kan detta anföras som ett skäl för att möjligheterna att använda olika slags tvångsmedel bör korrespondera så långt det är lämpligt med tanke på det integritetsintrång som tvångsmedlet innebär. En sådan reglering gör det nämligen svårare för de kriminella att undvika hemliga tvångsmedel genom att anpassa sitt beteende.

Det kommer att krävas ökade resurser för att genomföra hemliga tvångsmedel i fler fall. Resursåtgången varierar från ärende till ärende och beroende på vilket tvångsmedel det är fråga om. Faktorer av betydelse är bl.a. hur omfattande förberedelser som krävs i form av exempelvis spaning eller andra åtgärder för att kartlägga den misstänktes aktiviteter, få tillgång till lösenord, installation av mjukvara,

hårdvara eller annan utrustning. I propositionen Hemlig dataavläsning bedömde regeringen att hemlig dataavläsning i många fall kan jämföras med den resursåtgång som hemlig rumsavlyssning kräver (prop. 2019/20:64 s. 82). Under den tid då tvångsmedlet har varit tillgängligt har det dock visat sig att det använts i långt fler fall än väntat. Enligt uppgift från de brottsbekämpande myndigheterna varierar det stort från fall till fall hur resurskrävande det är att genomföra en hemlig dataavläsning, beroende bl.a. på vilken metod som kan användas och vilken slags uppgifter man avser få tillgång till. Hemlig övervakning av elektronisk kommunikation torde allmänt sett vara det minst resurskrävande av de hemliga tvångsmedlen, men kan likväl kräva en avsevärd personalinsats om det handlar att gå igenom exempelvis omfattande samtalslistor.

Det måste här framhållas att hemliga tvångsmedel endast får användas när åtgärden är av synnerlig vikt för utredningen. Detta krav innebär att det som kan åstadkommas genom tvångsmedlet i princip inte får vara åtkomligt med hjälp av mindre ingripande metoder eller i varje fall att hindret för att använda sådana metoder är sådant att det inte skäligen kan krävas att man ska avstå från att använda tvångsmedlet, t.ex. på grund av att alternativen innebär en orimligt hög arbetsinsats eller är förenad med avsevärd risk för att den pågående utredningen avslöjas för tidigt (propositionen Hemliga tvångsmedel mot allvarliga brott, prop. 2013/14:237 s. 94 och 95). Med hänsyn till detta och till att behovs- och proportionalitetsprinciperna gäller vid all tvångsmedelsanvändning, måste man utgå ifrån att tvångsmedlen används restriktivt, även om nya straffvärdeventiler vid flerfaldig brottslighet införs. Den utformning som vi förordar innebär i sig att tillämpningen begränsas till allvarlig brottslighet. Många gånger är användning av hemliga tvångsmedel den enda möjliga eller rimliga vägen att få tillgång till den information som behövs för att föra utredningen framåt. Eftersom nya straffvärdeventiler kan förväntas leda till att betydligt fler förundersökningar om brott som utövats i organiserad form eller systematiskt resulterar i åtal och fällande dom, och att man i fler fall kan lagföra de verkliga huvudmännen och inte enbart personer längre ner i hierarkin, bedöms den ökade resursåtgången vara motiverad.

Sammantaget gör vi bedömningen att nya straffvärdeventiler med den utformning som vi presenterat i avsnitt 6.7 och 6.9 skulle vara effektiva.

6.11 Risker för den personliga integriteten

Bedömning: Nya straffvärdeventiler innebär, vid en jämförelse med nuvarande användning av hemliga tvångsmedel, att fler enskilda utsätts för intrång i den personliga integriteten. Däremot uppstår inte några nya risker för den personliga integriteten.

Skälen för bedömningen

I propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 84) ansåg regeringen att bedömningen om hemlig dataavläsning innebär ökade risker för den personliga integriteten skulle göras med utgångspunkt i de gällande reglerna. För att minimera riskerna för den personliga integriteten framhöll regeringen att det är av stor vikt att regleringen av ett nytt tvångsmedel utformas på ett sådant sätt att missbruk omöjliggörs och gränsförskjutningar inte förekommer. Dessa ställningstaganden utgör även vår utgångspunkt vid bedömningen av konsekvenserna för den personliga integriteten till följd av en ny straffvärdeventil avseende viss flerfaldig brottslighet.

Eftersom det inte är fråga om något nytt tvångsmedel bedömer vi att det inte uppstår några i egentlig mening nya risker för den personliga integriteten. Däremot skulle införandet av straffvärdeventiler vid viss flerfaldig brottslighet innebära att fler personer utsätts för hemliga tvångsmedel. Det handlar då både om brottsmisstänkta personer och andra som inte är misstänkta för något brott. Utomstående kan drabbas exempelvis genom att de kommunicerar elektroniskt med den misstänkte och därför kommer att omfattas av hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning som avser kommunikationsavlyssningsuppgifter. De kan även omfattas av hemlig kameraövervakning och hemlig rumsavlyssning samt hemlig dataavläsning som avser kameraövervakningsuppgifter respektive rumsavlyssningsuppgifter om de befinner sig på den övervakade eller avlyssnade platsen. Hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter är de tvångsmedel som anses typiskt sett allra mest integritetskänsliga, varför varje utökning av möjligheterna att använda detta tvångsmedel får anses särskilt påverka de utsattas personliga integritet. Här har det bl.a. betydelse att det finns en risk att andra än den misstänkte avlyssnas i sitt hem och att

myndigheterna i vissa fall måste göra intrång i hemmet för att kunna verkställa tvångsmedlet.

6.12 Nya straffvärdeventiler är proportionerliga

Bedömning: Det är proportionerligt att införa nya straffvärdeventiler för flerfaldig brottslighet som utövats i organiserad form eller systematiskt under förutsättning att tillämpningsområdet förses med lämpliga avgränsningar.

Skälen för bedömningen

Kravet på proportionalitet

En förutsättning för att utvidga möjligheterna att använda hemliga tvångsmedel är att det utvidgade tillämpningsområdet är proportionerligt i förhållande till behov, effektivitet och integritet. Det måste då beaktas att vissa hemliga tvångsmedel anses mer integritetskränkande än andra. I de föregående avsnitten kommer vi fram till att det finns ett behov av nya straffvärdeventiler och att det skulle vara en effektiv åtgärd som kan förväntas leda till fler åtal och fällande domar i fråga om organiserad och systematisk brottslighet. Vi har också kommit fram till att straffvärdeventilerna inte leder till några nya risker för den personliga integriteten men däremot att fler personer kommer att utsättas för intrång i den personliga integriteten om det införs straffvärdeventiler för viss flerfaldig brottslighet.

Utöver den omständigheten att fler enskilda kan komma att utsättas för hemliga tvångsmedel har det betydelse att tröskeln i fråga om det enskilda brottets allvar sänks. Detta skulle utgöra en ändring i förhållande till hur lagstiftaren hittills har sett på förutsättningarna för att använda hemliga tvångsmedel (se propositionerna Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering, prop. 2002/03:74 s. 34 och Hemlig rumsavlyssning, prop. 2005/06:178). Vi gör följande överväganden.

Ändrade förhållanden sedan straffvärdeventilerna infördes

Uttalandena i de nyss nämnda propositionerna gjordes i samband med att straffvärdeventilerna infördes. Det var alltså då en ny och oprövad metod, som dessutom – när det gäller hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning – infördes i strid med Buggningsutredningens uppfattning (se prop. 2002/03:74 s. 33 och SOU 1998:46 s. 380 och 381). Straffvärdeventilerna har nu funnits i närmare tjugo år och har i allt väsentligt visat sig fungera väl, även i de fall då åklagare interimistiskt beslutar om hemliga tvångsmedel. De farhågor som framfördes i samband med ventilernas införande tycks inte ha förverkligats. Det har däremot blivit allt tydligare att det är ett problem i den brottsbekämpande verksamheten att endast det enskilda brottets och inte den samlade brottslighetens straffvärde får beaktas, ens när brotten begås organiserat eller systematiskt. Sedan straffvärdeventilernas införande har brottsligheten ändrat karaktär. Vi ser bl.a. en ökning av gängrelaterad brottslighet som i varierande grad är organiserad eller systematisk. Det handlar inte sällan om en omfattande brottslighet med ett högt samlat straffvärde, men där varje enskilt brott har ett straffvärde som inte överstiger två respektive fyra års fängelse. En annan förändring är att det blivit vanligare att de personer som utsätts för eller annars har kännedom om brott inte vill eller vågar berätta om det som de varit med om eller vet. Detta kan bl.a. hänga samman med s.k. tystnadskulturer, som vi går närmare in på i kapitel 7. Denna förändring har medfört ett behov av andra verktyg för att kunna utreda brott.

Även om de enskilda brotten inte har ett straffvärde som överstiger två respektive fyra års fängelse handlar det många gånger om allvarlig brottslighet med stora skadeverkningar för enskilda och samhället. Som ett exempel kan man nämna systematiska grova bedrägerier där människor exempelvis luras att lämna ifrån sig koder eller att logga in på sitt bankkonto. Sådana brott drabbar många människor och riktas inte sällan mot äldre. Beloppen kan från den enskildes perspektiv vara betydande, om än inte tillräckligt höga för att ensamt medföra ett straffvärde som överstiger två år. Samma sak kan sägas om organiserade grova stölder och annan organiserad eller systematisk förmögenhetsbrottslighet.

Ett annat exempel är organiserad eller systematisk handel med narkotika. Narkotikahandeln utgör en basinkomst för de kriminella aktörerna i utsatta områden och har en stark koppling till våldsamma konflikter i den kriminella miljön (Myndighetsgemensam lägesbild om organiserad brottslighet 2019). Den organiserade och öppna narkotikahandeln påverkar invånarnas känsla av trygghet och uppfattas som ett tecken på de kriminella aktörernas makt. Den omständigheten att handeln är upprepad leder många gånger till att brottet bedöms som grovt, vilket innebär att hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter är tillåten. Däremot är en rubricering som grovt brott inte tillräckligt för att hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter ska kunna ske, förutom om straffvärdet för brottet dessutom kan antas överstiga fyra års fängelse. Det kan skada förtroendet för rättsväsendet och minska människors trygghet när omfattande organiserad eller systematisk brottslighet inte kan utredas och de kriminella upplevs kunna styra över möjligheterna att utreda brott och därmed undgå ansvar.

Även grov skattebrottslighet är en viktig inkomstkälla för den organiserade brottsligheten och det kan i vissa fall handla om totala skatteundandraganden om mycket stora belopp. Många gånger används bokföringsbrott för att dölja skattebrottsligheten. Det varierar om domstolarna har bedömt brottsligheten som ett grovt brott med ett straffvärde överstigande två år, eller som flera brott med ett brott som understiger detta straffvärde. I många fall har dock domstolarna bedömt förfarandet som ett brott och tillåtit användning av hemliga tvångsmedel med tillämpning av straffvärdeventilen, även om skatteundandragandet delas upp på flera deklarationer eller penningströmningarna på flera överföringar så länge dessa hänger ihop och ingår i samma systematik, brottsplan och brottsliga upplägg (se avsnitt 6.6). Det är av stor vikt att lagstiftningen om hemliga tvångsmedel är tydlig och att tillämpningen är förenlig med lagens ordalydelse. Det får inte finnas osäkerhet hos allmänheten, domstolar och åklagare om var gränserna för användning av respektive tvångsmedel går. En sådan osäkerhet kan leda både till att reglerna tillämpas när det egentligen inte är tillåtet och till att man avstår i onödan av rädsla för att göra fel.

Ett annat exempel som vi tagit upp i behovsbeskrivningarna är systematiska eller organiserade sexualbrott, och i synnerhet sådana som begås digitalt mot barn. Även denna typ av brottslighet har ökat

i spåren av den ökade digitaliseringen. Det är fråga om en typ av brottslighet som anses särskilt förkastlig, vilket bl.a. kommer till uttryck genom att den ingår i brottskatalogen för hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter. Det är vidare inte ovanligt att brotten begås upprepat, på ett likartat sätt och har föregåtts av en noggrann planering. Samtidigt kan straffvärdet för de enstaka gärningarna vara otillräckligt för att en hemlig rumsavlyssning eller hemlig dataavläsning avseende rumsavlyssningsuppgifter ska kunna ske även om det sammanlagda straffvärdet är högt. Vi lämnar i avsnitt 7.4 förslag som går ut på att sexualbrott mot barn och barnpornografi ska kunna leda till hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning avseende bl.a. kommunikationsavlyssningsuppgifter. Detta innebär dock inte i sig att hemlig rumsavlyssning eller hemlig dataavläsning avseende rumsavlyssningsuppgifter blir möjligt.

Från principiella utgångspunkter anser vi att det starkt kan ifrågasättas om det i situationer där brottsligheten begås organiserat eller systematiskt är rimligt att upprätthålla en sträng åtskillnad mellan det enskilda brottet och den samlade brottsligheten när det är fråga om hemliga tvångsmedel. Ur ett samhällsperspektiv torde det i sådana fall framstå som mindre viktigt om det rättsligt är fråga om ett eller flera brott.

Kriminella kan anpassa sig till regleringen

Den nuvarande regleringen gör det möjligt för kriminella att anpassa sin brottslighet efter möjligheterna att använda hemliga tvångsmedel. Exempel har getts i avsnitt 6.7 när det gäller t.ex. vissa skattebrott, men samma sak kan sägas om t.ex. omfattande grova bedrägerier med hjälp av mobila bank-ID etc. En brottslig sammanslutning kan välja ett upplägg som går ut på att man begår många brott som hamnar under gränsen för när den nuvarande straffvärdeventilen är tillämplig i stället för att begå färre brott till större belopp. Man kan alltså utnyttja kunskap om regelverket till sin fördel. Som vi nyss framhållit kan det dock ur ett samhällsperspektiv ifrågasättas om det inte är lika angeläget att bekämpa organiserade eller systematiskt begångna brott som drabbar många, som att kunna utreda enstaka brott med ett högre enskilt straffvärde.

Det finns omfattande rättssäkerhetsgarantier

Vi konstaterar vidare att de hemliga tvångsmedlen omgärdas av omfattande rättssäkerhetsgarantier. Enligt artikel 13 i Europakonventionen ska var och en, vars i konventionen angivna fri- och rättigheter kränkts, ha tillgång till ett effektivt rättsmedel inför en nationell myndighet och detta även om kränkningen förövats av någon under utövning av offentlig myndighet. Som vi utvecklat i kapitel 4 föreligger en rätt till domstolsprövning och, förutom när det gäller hemlig övervakning av elektronisk kommunikation, deltagande av offentliga ombud. De hemliga tvångsmedlen är vidare föremål för tillsyn av SIN och extraordinär tillsyn som utförs av Justitieombudsmannen och Justitiekanslern. Till det kommer den parlamentariska efterhandskontroll som utövas av riksdagen och underrättelseskyldigheten till enskild. För enskilda innebär en sådan underrättelseskyldighet en möjlighet att själv reagera genom att t.ex. kräva ersättning för skada på grund av fel eller försummelse vid myndighetsutövning.

Nya straffvärdeventiler är proportionerliga

Nya straffvärdeventiler kommer att innebära en inskränkning av de rättigheter och det skydd som tillkommer enskilda enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga. De skäl som föreligger för att begränsa dessa rättigheter är hänförliga till intresset av att förebygga och beivra brott. Detta är sådana intressen som får ligga till grund för begränsningar av rättigheterna, se 2 kap. 21 § regeringsformen, artikel 8.2 Europakonventionen och artikel 52.1 EU:s rättighetsstadga. Den bortre gränsen för i vilken grad skyddet för den personliga integriteten i Sverige får inskränkas framgår av 2 kap. 21 § regeringsformen. Där anges bland annat att en begränsning får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar.

Nya straffvärdeventiler kan också innebära ett ytterligare ingrepp i enskildas egendomsskydd. Av 2 kap. 15 § regeringsformen följer bl.a. att varje medborgares egendom är tryggad genom att ingen kan tvingas avstå sin egendom till det allmänna eller till någon enskild

genom expropriation eller annat sådant förfogande eller tåla att det allmänna inskränker användningen av mark eller byggnad utom när det krävs för att tillgodose angelägna allmänna intressen. Regeringsformens regler skyddar alltså inte mot inskränkningar i användningen av egendom annat än när det gäller mark eller byggnad. Av artikel 1 i första tilläggsprotokollet till Europakonventionen följer att varje fysisk eller juridisk person ska ha rätt till respekt för sin egendom. Ingen får berövas sin egendom annat än i det allmännas intresse och under de förutsättningar som anges i lag och i folkrättens allmänna grundsatser. Det följer dock av artikeln att skyddet inte inskränker en stats rätt att genomföra sådan lagstiftning som staten finner nödvändig för att bl.a. reglera nyttjandet av viss egendom i överensstämmelse med det allmännas intresse. Egendomsskyddet regleras också på motsvarande sätt i artikel 17 EU:s rättighetsstadga, där det framgår att ingen får berövas sin egendom utom då samhällsnyttan kräver det, i de fall och under de förutsättningar som föreskrivs i lag och mot rättmätig ersättning för sin förlust i rätt tid. Hemliga tvångsmedel, främst hemlig dataavläsning kan innebära en inskränkning i lagringsutrymme och kapacitet på ett tekniskt hjälpmedel. Detta gäller dock typiskt sett under en begränsad tid och avser inte egendomen i sin helhet.

Eftersom det är fråga om långtgående inskränkningar av de rättigheter och det skydd som tillkommer enskilda kan de inskränkningar som diskuteras endast vara godtagbara i syfte att bekämpa grov brottslighet. För att den ökade totala inskränkning som nya straffvärdeventiler innebär av främst rätten till privatliv men även i viss mån egendomsskyddet ska vara godtagbar krävs det vidare att regleringen kringgärdas av starka rättssäkerhetsgarantier och innehåller tydliga ramar som tillämparen har att hålla sig inom. Möjligheten att använda hemliga tvångsmedel får inte gå längre än att den kan accepteras av allmänheten som ett nödvändigt och godtagbart verktyg för de brottsbekämpande myndigheterna.

Av EU-domstolens avgörande i bl.a. Tele2-domen framgår att myndigheter, när det gäller brottsbekämpning, endast får ges tillgång till trafik- och lokaliseringsuppgifter som lagrats av en leverantör av elektroniska kommunikationstjänster om syftet är bekämpning av vad som omväxlande kallas grov eller allvarlig brottslighet – i den engelska språkversionen ”serious crime”. Ytterligare uttalanden finns i EU-domstolens dom den 2 mars 2021 i mål C-746/18. Där görs följande precisering.

> Artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009, jämförd med artiklarna 7, 8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna, ska tolkas så, att den utgör hinder mot nationell lagstiftning som gör det möjligt för offentliga myndigheter att få tillgång till vissa trafik- eller lokaliseringsuppgifter – vilka kan ge information om kommunikation som en användare har utfört medelst elektronisk kommunikationsutrustning eller om lokaliseringen av terminalutrustning som denna användare har använt, och ligga till grund för slutsatser beträffande användarens privatliv – i syfte att förebygga, undersöka, avslöja och väcka åtal för brott, utan att det uppställs något krav på att det ska röra sig om grov brottslighet eller förebyggande av allvarliga hot mot allmän säkerhet, oberoende av hur lång tid myndigheterna får tillgång till de lagrade uppgifterna och oberoende av omfattningen och arten av de uppgifter som omfattas av denna tidsperiod.

Uttalandena är i första hand relevanta i fråga om hemlig övervakning av elektronisk kommunikation, men har även betydelse för hemlig avlyssning av elektronisk kommunikation eftersom historisk inhämtning av meddelanden innebär att myndigheterna ges tillgång till lagrade uppgifter. Någon generell definition av vad som menas med grov eller allvarlig brottslighet finns inte i svensk rätt och inte heller inom EU-rätten. Utredningen om datalagring och EU-rätten ansåg dock i betänkandet Datalagring – brottsbekämpning och integritet (SOU 2017:75 s. 254–256) att de nuvarande reglerna i rättegångsbalken om tillgång till lagrade uppgifter avser allvarliga/grova brott och att reglerna därför är förenliga med EU-rätten. Några ändringar av bestämmelserna om hemlig övervakning av elektronisk kommunikation till följd av Tele2-domen och senare praxis från EU-domstolen har hittills inte föreslagits. En särskild utredare har dock fått i uppdrag att bl.a. analysera hur dagens regler om lagring och tillgång till uppgifter om elektronisk kommunikation förhåller sig till ny praxis på området, överväga och ta ställning till vilka möjligheter som finns till förändringar av reglerna om lagring och tillgång till uppgifter om elektronisk kommunikation i syfte att tillgodose de brottsbekämpande myndigheternas möjligheter att upprätthålla och stärka sin förmåga, samtidigt som skyddet för de mänskliga rättigheterna säkerställs (dir. 2021:58). Uppdraget ska redovisas senast den 6 februari 2023.

Vi konstaterar att syftet med de nya straffvärdeventilerna skulle vara att förbättra förutsättningarna att utreda viss organiserad och systematisk brottslighet. Detta är i sig ett godtagbart och tungt vägande intresse. Organiserad och systematisk brottslighet är till sin karaktär allvarlig, och särskilt angelägen att bekämpa. Vi har därutöver, i avsnitt 6.7 och 6.9, föreslagit ytterligare begränsningar i fråga om såväl det samlade straffvärdet för brottsligheten som i fråga om straffskalan för vart och ett av de sammanräknade brotten. Vidare innehåller lagstiftningen redan nu krav på såväl misstankegrad som att tvångsmedlet ska vara av synnerlig vikt för utredningen. Vår bedömning är att den utformning av straffvärdeventilerna som vi föreslagit i de nyss nämnda avsnitten dels innebär att förslaget begränsas till allvarlig brottslighet, dels innebär en godtagbar avvägning mellan intresset av att man effektivt kan bekämpa systematisk eller organiserad brottslighet och enskildas fri- och rättigheter. Den brottslighet som kan omfattas av respektive ventil bedöms alltså vara så allvarlig att den kan motivera de ingrepp som respektive tvångsmedel innebär. Den föreslagna utformningen bedöms även ge tillämparen tillräckligt tydliga ramar, även om det innebär en viss ökad svårighet att det måste göras en samlad bedömning av flera brott. Den osäkerhet som detta kan innebära ska dock, som vi angett tidigare, alltid tillgodoräknas den som man önskar rikta tvångsmedlet mot. Det saknas enligt vår bedömning mindre ingripande alternativ för att komma åt de uppgifter som det finns behov av för att fler förundersökningar gällande organiserad och systematisk brottslighet ska kunna leda till åtal och fällande dom och för att man ska komma åt rätt personer.

Vi har redan konstaterat att det finns starka rättssäkerhetsgarantier till skydd för enskilda. Vi återkommer i kapitel 14 till frågan om något ytterligare behöver göras för att stärka skyddet för den personliga integriteten.

Sammantaget anser vi att det är proportionerligt att införa nya straffvärdeventiler med den utformning som vi föreslagit.

6.13 Förhållandet till avlyssningsförbudet

Bedömning: Nya straffvärdeventiler som kan tillämpas vid förundersökningar om viss flerfaldig brottslighet skulle innebära att avlyssningsförbudet i 27 kap. 22 § RB respektive 27 § andra stycket lagen om hemlig dataavläsning blir tillämpligt i fler fall.

Skälen för bedömningen

Enligt 27 kap. 22 § första stycket RB får hemlig avlyssning av elektronisk kommunikation inte avse telefonsamtal eller andra meddelanden där någon som yttrar sig inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena RB. Enligt paragrafens andra stycke gäller detsamma vid hemlig rumsavlyssning för samtal eller annat tal där någon som angetts i första stycket talar.

Hänvisningen i 27 kap. 22 § RB till 36 kap. 5 § andra–sjätte styckena RB innebär att avlyssning som huvudregel inte får ske vid samtal med personer som tillhör vissa yrkeskategorier, under förutsättning att samtalet har samband med deras yrkesutövning och omfattas av tystnadsplikt. Exempel på sådana yrkeskategorier är advokater, läkare, tandläkare, barnmorskor, sjuksköterskor, psykologer och psykoterapeuter samt tolkar och översättare som har biträtt dessa personer.

För präster och andra med motsvarande ställning inom ett trossamfund är avlyssningsförbudet absolut. Förbudet gäller vid samtal som avser bikt eller enskild själavård. Avlyssningsförbudet är absolut även för en försvarare när denne utövar sitt uppdrag och gäller både för offentliga och privata försvarare.

För samtliga yrkeskategorier som omfattas av bestämmelserna i 36 kap. 5 § andra–sjätte styckena RB – utom försvarare och präster eller personer med motsvarande ställning inom ett trossamfund – finns undantag som innebär en skyldighet att under vissa angivna förutsättningar vittna om uppgifter som anförtrotts dem i deras yrkesutövning eller som de erfarit i samband därmed. Regleringen innebär att advokater och deras biträden är skyldiga att vittna endast om det är medgivet i lag, om den till vars förmån tystnadsplikten gäller samtycker till det eller om vittnesmålet ska avges i mål om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Andra

yrkeskategorier som omfattas av 36 kap. 5 § andra eller tredje stycket RB är skyldiga att vittna i mål angående brott för vilket det inte är föreskrivet lindrigare straff än fängelse i ett år och försök till brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. De är även skyldiga att vittna i mål om försök till brott för vilket det inte är föreskrivet lindrigare straff än fängelse i ett år när gärningen innefattat försök till överföring av sådan allmänfarlig sjukdom som avses i 1 kap. 3 § smittskyddslagen (2004:168). Skyldighet att vittna gäller vidare för vissa yrkeskategorier i mål om brott enligt 3, 4 eller 6 kap. BrB eller som avses i lagen (1982:316) med förbud mot könsstympning, när brottet riktats mot någon som inte fyllt 18 år. I 3 kap. 3 § tryckfrihetsförordningen och 2 kap. 3 § yttrandefrihetsgrundlagen finns det särskilda bestämmelser om undantag från tystnadsplikt.

Eftersom möjligheten att använda hemlig avlyssning av elektronisk kommunikation som utgångspunkt endast gäller för allvarliga brott där miniministraffet är lägst två års fängelse är det i allmänhet bara försvarare, präster och själavårdare som i praktiken omfattas av avlyssningsförbudet. Dock är det i vissa fall möjligt att utföra avlyssning vid en förundersökning om brott där minimistraffet är lägre än ett års fängelse, t.ex. vid tillämpning av straffvärdeventilen. I ett sådant fall kan avlyssningsförbudet aktualiseras även i fråga om andra yrkesgrupper. Om man inför nya straffvärdeventiler vid förundersökningar om viss flerfaldig brottslighet innebär det att utrymmet ökar för att tillämpa hemlig avlyssning av elektronisk kommunikation i fall där minimistraffet understiger ett års fängelse. Det innebär i sin tur att avlyssningsförbudet kan aktualiseras i fler fall än i dag. Vi anser inte att detta är något skäl mot att man inför nya straffvärdeventiler, utan ser tvärtom att avlyssningsförbudet ger ett viktigt skydd för förtrolig kommunikation och den enskildes personliga integritet. Det förtjänar dock i parentes att anmärkas att reglerna om avlyssningsförbud är komplexa och svårbegripliga, vilket även Säkerhets- och integritetsskyddsnämnden har påtalat (se beslut den 28 mars 2018 i ärende dnr 158/2017). Vi anser att det vore lämpligt med en översyn av reglerna, i syfte att göra dem lättare att tillämpa.

Motsvarande bestämmelser gäller i fråga om hemlig dataavläsning som gäller kommunikationsavlyssnings- eller rumsavlyssningsuppgifter (27 § andra och tredje stycket lagen om hemlig dataavläsning). Det som vi anfört i fråga om hemlig avlyssning gör sig gällande även i fråga om hemlig dataavläsning.

6.14 Nya straffvärdeventiler införs

Förslag: Det införs en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning avseende uppgifter som avses i 2 § andra stycket 1–4 samt 6 och 7 lagen om hemlig dataavläsning vid förundersökningar om flerfaldig brottslighet som kan antas ha utövats i organiserad form eller systematiskt och som kan antas ha ett samlat straffvärde överstigande fängelse i två år. Förslaget innebär också att möjligheten att använda hemlig övervakning av elektronisk kommunikation ökar. Vid sammanläggningen ska endast häktningsgrundande brott och försök, förberedelse eller stämpling till häktningsgrundande brott kunna inräknas. Varje brott som inräknas ska kunna antas vara ett led i den organiserade eller systematiska brottsligheten.

Det införs även en möjlighet att använda hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter vid förundersökningar om flerfaldig brottslighet som kan antas ha utövats i organiserad form eller systematiskt och som kan antas ha ett samlat straffvärde överstigande fängelse i fyra år. Vid sammanläggningen ska endast brott med ett minimistraff om sex månaders fängelse eller mer och försök, förberedelse eller stämpling till sådana brott kunna inräknas. Varje brott som inräknas ska kunna antas vara ett led i den organiserade eller systematiska brottsligheten.

Skälen för förslagen

Vi har i föregående avsnitt kommit fram till att det finns ett behov av nya straffvärdeventiler som avser flerfaldig brottslighet som har

- utövats i organiserad form eller systematiskt och de sammanräknade brotten utgör ett led i denna brottslighet,
- ett samlat straffvärde överstigande två års fängelse, eller i fråga om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter, fyra års fängelse, samt
- att vart och ett av de ingående brotten är häktningsgrundande, eller i fråga om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter har lägst sex månaders fängelse som minimistraff.

Vi har även kommit fram till att sådana ventiler skulle vara effektiva och att det är proportionerligt att införa dem, förutsatt att möjligheten att använda dem avgränsas på det sätt som vi förordar.

Bedömningen har gjorts att det inte är lämpligt eller nödvändigt att straffvärdeventilen i fråga om hemlig rumsavlyssning begränsas genom en brottskatalog. Bedömningen gäller både den nuvarande straffvärdeventilen och en straffvärdeventil för flerfaldig brottslighet.

Sammantaget bedömer vi att skälen för ett införande av nya straffvärdeventiler med den angivna utformningen klart överväger de skäl som talar emot. Vi föreslår därför att det i bestämmelserna om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning införs nya straffvärdeventiler som kan tillämpas på flerfaldig brottslighet som kan antas ha utövats i organiserad form eller systematiskt, och som har ett sammanlagt straffvärde överstigande fängelse i två år, eller när det gäller hemlig rumsavlyssning fyra år. Därutöver föreslår vi att vart och ett av de ingående brotten ska vara häktningsgrundande, eller i fråga om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter, har lägst sex månaders fängelse som minimistraff. För att det ska vara rimligt med en samlad bedömning av straffvärdet bör det även krävas att det kan antas att vart och ett av brotten har utgjort ett led i den systematiska eller organiserade brottsligheten. Detta innebär inte att alla brott inom en systematisk brottslighet måste vara av samma slag. Som vi angett tidigare bör olika brottsrubriceringar kunna ingå, förutsatt att de utgör en del av samma brottsupplägg.

Eftersom ett tillstånd till hemlig avlyssning av elektronisk kommunikation också ger rätt till hemlig övervakning av elektronisk kommunikation, innebär våra förslag per automatik att även möjligheten att utföra en hemlig övervakning utökas. En annan följd av förslagen är att det blir möjligt i fler fall att använda hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet, eftersom förutsättningarna för den åtgärden överensstämmer med hemlig avlyssning av elektronisk kommunikation. Som framgått i avsnitt 6.6 finns det ett behov av en sådan möjlighet. Det kan här särskilt framhållas att en hemlig övervakning av elektronisk kommunikation ofta är första steget för att man över huvud taget ska veta mot vilken person man kan rikta andra hemliga tvångsmedel mot.

Motsvarande ändringar bör även göras i fråga om hemlig dataavläsning och detta även i fråga om uppgifter som avses i 2 § första stycket 6 och 7. Vi har då beaktat att det rör sig om en ny metod för att kunna samla in uppgifter som inte kunnat samlas in genom de andra tvångsmedlen och att lagen om hemlig dataavläsning är en tidsbegränsad försökslag, vilket skulle kunna tala emot att man låter punkterna 6 och 7 omfattas av den nya straffvärdeventilen. Vi anser dock att skälen som talar för att de ska omfattas påtagligt överväger.

Försök, förberedelse och stämpling

Om det är särskilt föreskrivet är det straffbart även med försök, förberedelse och stämpling till brott (23 kap. 1 och 2 §§ brottsbalken). Straff för försök bestäms högst till vad som gäller för fullbordat brott och får ej sättas under fängelse, om det lägsta straffet för det fullbordade brottet är fängelse i två år eller däröver. Straffet för förberedelse eller stämpling ska bestämmas under den högsta och får sättas under den lägsta gräns som gäller för fullbordat brott. Högre straff än fängelse i två år får bestämmas endast om fängelse i sex år eller mer kan följa på det fullbordade brottet.

Enligt den nuvarande regleringen är det möjligt med hemliga tvångsmedel vid försök, förberedelse eller stämpling förutsatt att en sådan gärning är belagd med straff. I de fall där en ansökan om hemlig avlyssning av elektronisk kommunikation eller hemlig kameraövervakning grundas på tillämpning av straffvärdeventilen krävs att brottets straffvärde, trots att det inte är fråga om ett fullbordat brott, överstiger två års fängelse. Om ansökan gäller hemlig rumsavlyssning med tillämpning av straffvärdeventilen krävs att gärningen, som måste ingå i katalogen i 27 kap. 20 d § andra stycket 4, är belagd med straff och att det kan antas att brottets straffvärde överstiger fängelse i fyra år.

Redan av principiella skäl bör samma sak gälla vid tillämpning av en ny straffvärdeventil för vissa flerfaldiga brott. Även osjälvständiga brottsformer bör alltså kunna leda till beslut om hemliga tvångsmedel förutsatt att gärningen är straffbelagd och att det sammanlagda straffvärdet överstiger två respektive fyra år. I praktiken innebär de principer som gäller för bedömning av straffvärde vid flerfaldig brottslighet att endast försök, förberedelse och stämpling avseende mycket allvarlig brottslighet kommer att ge något större utslag på straffvärdet.

Detta behöver inte anges särskilt för att gälla (jfr 27 kap. 18 § andra stycket 3 och 4).

6.15 Bestämmelserna om hemlig övervakning av elektronisk kommunikation behöver anpassas

Förslag: Det ska vara möjligt att besluta om hemlig övervakning av elektronisk kommunikation vid förundersökning om sådana brott eller sådan brottslighet som kan leda till hemlig avlyssning av elektronisk kommunikation, även om ett beslut om hemlig avlyssning inte fattas.

Skälen för förslaget

Vi har under arbetets gång uppmärksammat att hemlig övervakning av elektronisk kommunikation enligt bestämmelsernas ordalydelse inte förefaller vara tillåten om brottet inte är sådant som avses i 27 kap. 19 § RB och det inte finns anledning att besluta om hemlig avlyssning av elektronisk kommunikation. Saken kan aktualiseras om det skulle finnas förutsättningar att besluta om hemlig avlyssning av elektronisk kommunikation med stöd av en straffvärdeventil samtidigt som brottet inte har ett minimistraff om lägst sex månaders fängelse och inte heller är sådant som sägs i 27 kap. 19 § RB. Situationer av detta slag lär sällan uppkomma i praktiken med den nuvarande straffvärdeventilen, eftersom det torde vara sällsynt att enstaka brott med lägre straffminimum än sex månaders fängelse har ett straffvärde överstigande två års fängelse. Saken kommenterades inte i den proposition som ledde till införandet av straffvärdeventilerna (prop. 2002/03:74) och vi har inte kännedom om att förhållandet hittills skulle ha skapat några problem i den brottsutredande verksamheten.

Om man inför en straffvärdeventil för flerfaldig brottslighet kan man tänka sig att den samlade brottsligheten innefattar brott som inte i sig kan ligga till grund för en hemlig övervakning av elektronisk kommunikation. Sannolikheten för att de brottsbekämpande myndigheterna ställs inför en situation där det är tillåtet med hemlig avlyssning men inte hemlig övervakning av elektronisk kommunikation skulle därför öka. En sådan ordning framstår som inkonsekvent och

principiellt tveksam, eftersom hemlig övervakning av elektronisk kommunikation är det mindre ingripande av de två tvångsmedlen och då ett beslut om hemlig avlyssning ger rätt att vidta även hemlig övervakning. Det kan inte vara rätt att de brottsbekämpande myndigheterna kan bli tvungna att ansöka om tillstånd till hemlig avlyssning enbart för att kunna få tillgång till övervakningsuppgifter. Vi föreslår därför att det i regleringen klart och tydligt ska framgå att det är möjligt att vidta hemlig övervakning av elektronisk kommunikation för alla brott som kan leda till hemlig avlyssning av elektronisk kommunikation.

7 Utvidgade brottskataloger och angränsande frågor

7.1 Uppdraget

Att den som utsatts för eller bevittnat ett brott av olika skäl inte vill lämna upplysningar om brottet är ett problem. Brottsförebyggande rådet (Brå) har på regeringens uppdrag i rapporten Tystnadskulturer – En studie om tystnad mot rättsväsendet (rapport 2019:10) studerat tystnadskulturer och övergrepp i rättssak. Enligt rapporten kan de kriminella tystnadskulturerna ha spridningseffekter till personer utanför miljön genom medierapportering eller ryktesspridning som förmedlar grupperingarnas skrämselkapital. Konsekvensen kan bli att personer utanför den kriminella miljön inte vågar anmäla brott eller vittna om de har skäl att tro att gärningspersonen tillhör ett kriminellt nätverk (s. 11 och 12).

Vissa brottstyper är enligt Åklagarmyndigheten särskilt svårutredda eftersom de typiskt sett begås i en miljö där det råder en tystnadskultur. Myndigheten anger i skrivelsen Framställning om ändringar i lagstiftningen om hemliga tvångsmedel i 27 kap. rättegångsbalken (Ju2019/03572/Å s. 5) att utpressning, övergrepp i rättssak, mened och skyddande av brottsling kan vara sådana brott.

I våra direktiv framhåller regeringen att det är av största vikt att samhället tar tydlig ställning mot beteenden som påverkar möjligheterna att upprätthålla straffsystemets effektivitet. Vi har mot denna bakgrund i uppdrag att undersöka om vissa ytterligare brott ska ingå i brottskatalogerna i bestämmelserna om hemlig avlyssning av elektronisk kommunikation (27 kap. 18 § RB) och hemlig övervakning av elektronisk kommunikation (27 kap. 19 § RB). I uppdraget ingår att

- ta ställning till om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation bör få användas vid fler brott, t.ex. utpressning, övergrepp i rättssak, mened och skyddande av brottsling, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Som angetts i avsnitt 6.1 ankommer det på utredningen att säkerställa att en välfungerande systematik upprätthålls i regelverket om hemliga tvångsmedel och att bedöma behovet av följdändringar i annan relevant lagstiftning. Vi har även möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska utredas. Som kommer att utvecklas närmare i avsnitt 7.6 kan hemlig kameraövervakning användas för samma slags brott som hemlig avlyssning av elektronisk kommunikation. Av bl.a. systematiska skäl överväger vi därför även om brottskatalogen för hemlig kameraövervakning bör utvidgas i motsvarande mån.

Som anförts i det nyss nämnda avsnittet får hemlig dataavläsning – med undantag för hemlig dataavläsning som gäller rumsavlyssningsuppgifter – användas vid förundersökning om samma slags brott som hemlig avlyssning av elektronisk kommunikation, se 4 § första stycket lagen (2020:62) om hemlig dataavläsning. Hemlig dataavläsning kan vara ett sätt för de brottsbekämpande myndigheterna att få tillgång till samma slags uppgifter som avses med hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning. Det finns alltså ett starkt sakligt och systematiskt samband mellan de tvångsmedel som uttryckligen omfattas av vårt uppdrag i denna del och hemlig dataavläsning som avser samma slags uppgifter. Regeringen uttalade vid införandet att det är av väsentlig betydelse att hemlig dataavläsning kan användas i motsvarande fall som de befintliga hemliga tvångsmedlen, eftersom det annars finns en risk för att vissa allvarliga brott inte kan utredas när det visar sig vara omöjligt att använda befintliga hemliga tvångsmedel (se prop. 2019/20:64 s. 124). Vi har därför valt att låta våra överväganden i detta kapitel omfatta även hemlig dataavläsning förutom rumsavlyssningsuppgifter.

7.2 Gällande rätt

Hemlig avlyssning av elektronisk kommunikation får användas vid en förundersökning om brott för vilket det föreskrivna minimistraffet är två års fängelse eller mer eller vid ett antal särskilt uppräknade brott samt försök, förberedelse eller stämpling till sådana brott om en sådan gärning är straffbelagd. Därutöver kan tvångsmedlet användas med stöd av den s.k. straffvärdeventilen i 27 kap. 18 § andra stycket 4 RB. Vi har noga redogjort för straffvärdeventilen i kapitel 6 och går därför inte närmare in på den här, utan fokuserar på den bestämmelse som är aktuell, nämligen brottskatalogen. Brottskatalogen finns i skrivande stund i 27 kap. 2 § andra stycket RB. Enligt förslag i propositionen Modernare regler för användning av hemliga tvångsmedel (prop. 2021/22:119) ska den dock flyttas till 18 §.

I katalogen ingår vissa brott mot rikets säkerhet, allmänfarliga brott, högmålsbrott och terroristbrott. Vissa men inte alla av de uppräknade brotten har två års fängelse eller mer som minimistraff. I tre fall finns böter i straffskalan, nämligen när det gäller obehörig befattning med hemlig uppgift, olovlig underrättelseverksamhet mot främmande makt och företagsspionerі. Det är fråga om brott som har ansetts som särskilt samhällsfarliga på så sätt att de direkt eller indirekt hotar vitala samhällsintressen. Beträffande flera av brotten har det också framhållits att de regelmässigt är svårutredda. (Prop. 2007/08:163 Åtgärder för att utreda vissa samhällsfarliga brott, m.m., s. 39 och 50 f.)

Under förutsättning att brottet innefattar en sabotagehandling som uppfyller rekvisiten i 13 kap. 4 § brottsbalken (förkortad BrB) omfattas

- mordbrand (fängelse två till åtta år) och grov mordbrand (fängelse i sex till arton år eller livstid) samt mindre allvarlig mordbrand (fängelse i ett till tre år),
- allmänfarlig ödeläggelse (fängelse i två till åtta år eller om brottet är mindre allvarligt ett till tre år),
- kapning (fängelse i högst fyra år eller om brottet är grovt fängelse i två till arton år, eller på livstid) och
- sjö-, luftfarts- eller flytplatssabotage (fängelse i högst fyra år eller om brottet är grovt fängelse i två till arton år, eller på livstid).

Därutöver omfattas

- sabotage (fängelse i högst fyra år) eller grovt sabotage (fängelse i två till arton år, eller på livstid),
- uppror (fängelse i tio till arton år, eller på livstid eller, om faran var ringa, till fängelse fyra till tio år),
- väpnat hot mot laglig ordning (fängelse i sex till tio år),
- brott mot medborgerlig frihet (fängelse i högst sex år),
- högförräderi (fängelse i tio till arton år, eller på livstid eller, om faran var ringa, till fängelse i fyra till tio år),
- krigsanstiftan (fängelse i två till åtta år),
- spionerі (fängelse i högst sex år) och grovt spionerі (fängelse i fyra till högst arton år, eller på livstid),
- obehörig befattning med hemlig uppgift (böter eller fängelse i högst två år) och grov obehörig befattning med hemlig uppgift (fängelse i högst fyra år),
- olovlig underrättelseverksamhet mot Sverige (fängelse i högst två år eller om brottet är grovt till fängelse i sex månader till fyra år), mot främmande makt (böter eller fängelse i högst ett år, eller om brottet är grovt fängelse i sex månader till fyra år) eller mot person (fängelse i högst ett år eller om brottet är grovt fängelse i sex månader till fyra år),
- företagsspionerі enligt 26 § lagen (2018:558) om 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 (böter eller fängelse i högst två år eller, om brottet är grovt, till fängelse i sex månader till sex år),
- 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 (brott enligt 3 § leder till fängelse i högst två år eller, om brottet är grovt, i sex månader till sex år medan brott enligt 3 a § leder till fängelse i högst två år), eller brott enligt lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och

annan särskilt allvarlig brottslighet (fängelse i högst två år eller, om brottet är grovt, i sex månader till sex år).[1]

Det är tillåtet att använda hemlig övervakning av elektronisk kommunikation vid betydligt fler brottstyper än hemlig avlyssning av elektronisk kommunikation. För att hemlig övervakning ska få förekomma krävs enligt huvudregeln att förundersökningen avser ett brott med ett minimistraff om lägst fängelse i sex månader. Det innebär att tvångsmedlet får användas vid flertalet brottsbalksbrott som rubriceras som grova och även ett stort antal brott på specialstraffrättens område. Vidare innefattar brottskatalogen de brott som avses i 27 kap. 2 § andra stycket 2–7, dvs. den katalog som av allt att döma kommer att flyttas till 18 §. Därutöver får hemlig övervakning av elektronisk kommunikation användas vid ytterligare ett fåtal särskilt angivna brott (27 kap. 19 § tredje stycket RB). Det handlar till att börja med om brott som ofta begås i organiserade former och där behovet av hemlig övervakning av elektronisk kommunikation har ansetts vara särskilt framträdande, såsom narkotikabrott och narkotikasmuggling (Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas, 4 uppl, s. 542). Brottskatalogen innehåller även vissa brott som ofta begås med digitala hjälpmedel, såsom dataintrång och barnpornografibrott som inte är ringa. Om den hemliga övervakningen syftar till att man ska utreda vem som skäligen kan misstänkas för brottet får åtgärden dock endast användas i fråga om brott som kan föranleda hemlig avlyssning av elektronisk kommunikation (27 kap. 19 § fjärde stycket RB). Hemlig övervakning får även användas vid förundersökning om försök, förberedelse eller stämpling till angivna brott om en sådan är belagd med straff.

Förutsättningarna för hemlig dataavläsning överensstämmer med förutsättningarna för hemlig avlyssning av elektronisk kommunikation (4 § lagen om hemlig dataavläsning) och detta även om avläsningen avser kommunikationsövervakningsuppgifter eller platsuppgifter, dvs.

[1] I prop. 2021/22:133 En samlad straffrättslig terrorismlagstiftning föreslås införande av en ny terroristbrottslag. Den nya lagen ska ersätta de nuvarande lagarna och reglera straffansvar för terroristbrott, samröre med en terroristorganisation, finansiering av terrorism eller särskilt allvarlig brottslighet, offentlig uppmaning till terrorism eller särskilt allvarlig brottslighet, rekrytering till terrorism eller särskilt allvarlig brottslighet, utbildning för terrorism eller särskilt allvarlig brottslighet och resa för terrorism eller särskilt allvarlig brottslighet. Därutöver föreslås bl.a. följande att alla svenska uppsåtliga brott och försök till brott kunna vara terroristbrott, förutsatt att de allvarligt kan skada ett land eller en mellanstatlig organisation och begås med terrorismsyfte och skärpta straff för de flesta av brotten i den föreslagna lagen. Förslaget föranleder även ändringar i brottskatalogen.

uppgifter som motsvarar en hemlig övervakning av elektronisk kommunikation. Om den hemliga dataavläsningen gäller rumsavlyssningsuppgifter krävs dock att det är fråga om en förundersökning om brott vilket kan utredas med hjälp av hemlig rumsavlyssning (6 § lagen om hemlig dataavläsning). Vidare ställs vissa särskilda krav i fråga om kopplingen mellan informationssystemet och brottet i fall då den hemliga dataavläsningen utförs i syfte att utreda vem som skäligen kan misstänkas för brottet, något som är tillåtet när det gäller kommunikationsövervaknings- och platsuppgifter (5 §).

7.3 Tidigare överväganden om brottskatalogerna

Hemlig övervakning av elektronisk kommunikation

Bestämmelserna om hemlig övervakning av elektronisk kommunikation fördes in i rättegångsbalken år 1989. Från början träffade reglerna endast brott med ett minimistraff om sex månader samt narkotikabrott och narkotikasmuggling. Som skäl för att det valdes en särlösning för narkotikabrott och narkotikasmuggling anförde regeringen att behovet av effektiva tvångsmedel för att kunna utreda sådana brott övervägde de invändningar som fanns (Regeringens proposition 1988/89:124 om vissa tvångsmedelsfrågor s. 50).

I det lagstiftningsärende som ledde till att straffvärdeventiler infördes för bl.a. hemlig avlyssning av elektronisk kommunikation, övervägde regeringen om en sådan ventil borde införas även för hemlig övervakning av elektronisk kommunikation, då kallat hemlig teleövervakning (propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering, prop. 2002/03:74 s. 35 och 36). Regeringen konstaterade dock att en straffvärdeventil åtminstone i teorin skulle innebära att tvångsmedlet får ett omfattande tillämpningsområde och även omfatta brott som normalt ger bötesstraff. Man gick därför inte fram med ett förslag om införande av straffvärdeventil. I stället lade man i brottskatalogen till barnpornografibrott som inte är ringa och dataintrång. Som skäl anfördes att det vid utredningar om sådana brott typiskt sett är av stor betydelse att ta del av de teleadresser mellan vilka meddelanden har utväxlats.

Rikspolisstyrelsen hade i det nyss nämnda lagstiftningsärendet anfört att det även vid bl.a. utredningar om olaga hot eller ofredande som begåtts genom telemeddelanden kan vara av intresse att ta del

av de teleadresser mellan vilka meddelanden har utväxlats. Regeringen framhöll att det under de angivna brottsbeteckningarna ryms ett stort antal fall som är av en sådan karaktär att det inte bör komma i fråga att använda hemliga tvångsmedel, varför man valde att i det läget inte lägga fram något förslag.

Hemlig avlyssning av elektronisk kommunikation

Rättegångsbalkens reglering om det som numera benämns hemlig avlyssning av elektronisk kommunikation omfattade från början endast brott med ett minimistraff om fängelse i två år eller mer. Den s.k. straffvärdeventilen infördes enlighet med förslag i propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering (prop. 2002/03:74). Hänvisningen till brottskatalogen i 27 kap. 2 § infördes genom propositionen Hemliga tvångsmedel mot allvarliga brott (prop. 2013/14:237). Det hade dock redan tidigare varit möjligt att med stöd av lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott, som i sin tur ersatte äldre reglering, använda hemliga tvångsmedel vid utredningar om särskilt samhällsfarliga brott som inte med tillämpning av huvudreglerna om straffvärde eller straffminimum hade kunnat leda till hemlig tvångsmedelstillämpning. Ändringen innebar att möjligheterna att använda hemliga tvångsmedel enligt 2008 års utredningslag fördes över till rättegångsbalken, med den skillnaden att hemlig kårverksamhet inte längre omfattades av en möjlighet att använda hemliga tvångsmedel. Regeringen konstaterade i propositionen Hemliga tvångsmedel mot allvarliga brott dels att de brott som fanns i brottskatalogen i 2008 års lag är samhällsfarliga och typiskt sett mycket svårutredda, dels att användningen av hemliga tvångsmedel kan antas medföra beaktansvärd nytta vid förundersökningar om brotten (prop. 2013/14:237 s. 82 och 83).

Hemlig dataavläsning

I propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 114–116) uttalade regeringen att hemlig dataavläsning bör kunna användas för samma slags brott som hemlig avlyssning av elektronisk kommunikation. Bedömningen innebär att den nedre gränsen för att med hjälp av hemlig dataavläsning hämta in kommunikationsövervakningsuppgifter

och platsuppgifter har satts högre än den nedre gränsen för att hämta in motsvarande slags uppgifter genom hemlig övervakning av elektronisk kommunikation. Det ansågs även att inhämtande av rumsavlyssningsavgifter med hjälp av hemlig dataavläsning var att jämställa med hemlig rumsavlyssning och därför bara bör få ske vid förundersökning om samma slags brott.

7.4 Brottskatalogerna utvidgas

Förslag: Det införs en möjlighet att använda hemlig avlyssning av elektronisk kommunikation vid förundersökningar om grovt dataintrång, sexuellt utnyttjande av barn, sexuellt övergrepp mot barn, grovt sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering, grovt utnyttjande av barn för sexuell posering, utnyttjande av barn genom köp av sexuell handling, sexuellt ofredande som gäller barn, kontakt för att träffa ett barn i sexuellt syfte, utpressning som inte är att anse som ringa, grov utpressning, mened som inte är att anse som ringa, övergrepp i rättssak som inte är att anse som ringa, barnpornografibrott som inte är ringa och grovt barnpornografibrott, grovt jaktbrott och grovt insiderbrott.

Det införs även en möjlighet att för angivna brott använda hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter samt uppgifter som finns lagrade i ett avläsningsbart informationssystem eller som visar hur ett sådant informationssystem används.

Bedömning: Den utökade möjligheten att använda hemlig avlyssning av elektronisk kommunikation medför att även möjligheten att använda hemlig övervakning av elektronisk kommunikation utvidgas.

Möjligheten att använda hemliga tvångsmedel bör inte omfatta förundersökningar om brott som anses som ringa. Det bör inte införas en möjlighet att använda hemliga tvångsmedel vid förundersökningar om skyddande av brottsling.

Skälen för bedömningen

Grundläggande förutsättningar för ett utvidgat tillämpningsområde

Som vi har framhållit i avsnitt 6.5 kräver ett utökat användningsområde för hemliga tvångsmedel att det görs noggranna avvägningar beträffande behovet av åtgärden, åtgärdens förväntade effektivitet och nytta samt vilka integritetsintrång som åtgärden kan förväntas medföra. En möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning vid förundersökning om andra brott än i dag måste motsvaras av ett faktiskt behov och anses som en effektiv åtgärd. Vidare ska behovet och effekten vägas mot vikten av att värna rättssäkerhet och personlig integritet samt, i viss mån, egendomsskyddet.

Förhållandet mellan de aktuella tvångsmedlen

Vi har i avsnitt 6.15 föreslagit att det alltid ska vara möjligt att besluta om en hemlig övervakning av elektronisk kommunikation för sådana brott som kan föranleda en hemlig avlyssning av elektronisk kommunikation. Det ska alltså inte krävas att det fattas ett beslut om hemlig avlyssning för att det ska vara möjligt att exempelvis hämta in uppgifter om var en viss kommunikationsutrustning finns eller har funnits. Detta innebär att varje ändring av brottskatalogen avseende hemlig avlyssning av elektronisk kommunikation samtidigt påverkar tillämpningsområdet för hemlig övervakning av elektronisk kommunikation.

Enligt dagens reglering kan alla de brott som kan leda till en hemlig avlyssning av elektronisk kommunikation även leda till hemlig dataavläsning, förutom sådan dataavläsning som gäller rumsavlyssningsuppgifter (4 § första stycket lagen om hemlig dataavläsning). Som vi har utvecklat närmare i avsnitt 6.6 gör vi bedömningen att denna överensstämmelse bör gälla även i fortsättningen. I den mån brottskatalogerna för de hemliga tvångsmedlen i rättegångsbalken utvidgas bör alltså utgångspunkten vara att brottskatalogen i lagen om hemlig dataavläsning utvidgas på motsvarande sätt. Hemlig kameraövervakning och hemlig dataavläsning som gäller kameraövervakningsuppgifter behandlas i avsnitt 7.6.

Fokus på vissa särskilt svårutredda brott

I direktiven och den tidigare nämnda framställningen från Åklagarmyndigheten nämns särskilt utpressning, övergrepp i rättssak, mened och skyddande av brottsling som sådana brott som man bör överväga att inkludera i brottskatalogerna. I Åklagarmyndighetens skrift nämns även grovt jaktbrott. De brott som tas upp har utpekats som särskilt svårutredda, bl.a. eftersom målsägande och vittnen många gånger är obenägna att lämna uppgifter till polisen och att vittna i domstol. Ekobrottsmyndigheten har till utredningen framfört att även grova insiderbrott är mycket svåra att utreda.

Som angetts inledningsvis har Brå studerat fenomenet tystnadskulturer och redovisat resultatet i rapporten Tystnadskulturer. En studie om tystnad mot rättsväsendet (Brå 2019:10). Bakgrunden till uppdraget var att rättsväsendet lyft fram att det blivit svårare att få personer att anmäla och vittna om brott, och att det talas om tystnadskulturer i delar av befolkningen. Med tystnadskulturer avsågs i studien normsystem hos ett avgränsat kollektiv om att inte samarbeta med rättsväsendet. I studien tittade man även närmare på individuella skäl för tystnad, fristående från sådana tystnadskulturer. Brå konstaterar i rapporten att ett brottsoffer ofta har flera parallella skäl till sin tystnad. Bland de mekanismer som väger särskilt tungt finns bl.a. skuld och skam, rädsla för hot och våld samt lojalitet eller samhörighet med gärningspersonen. Brå konstaterar vidare att även föreställningar om brott och rättsväsendet kan spela in.

Under vårt arbete har de brottsbekämpande myndigheterna även framhållit komplexa cyberbrott och sexualbrott mot barn samt barnpornografibrott som ytterst svåra att utreda utan en möjlighet till hemlig avlyssning och hemlig övervakning av elektronisk kommunikation.

Övergrepp i rättssak

Ett av de brott som särskilt lyfts fram är övergrepp i rättssak. Brottet innebär att någon, vanligen genom hot eller våld, försöker hindra en person från att anmäla ett brott, lämna uppgifter i en brottsutredning eller vittna i en rättegång (17 kap. 10 § BrB). Brottet kan också gälla situationer där någon redan har medverkat och därefter utsätts för hot, våld eller någon liknande gärning. Påföljden för brott av normalgraden är fängelse i högst fyra år. Om brottet är ringa döms

till böter eller fängelse i högst sex månader och om brottet är grovt döms till lägst två och högst åtta års fängelse.

Kriminalstatistiken visar i korthet att omkring 5 000 övergrepp i rättssak polisanmäls varje år. Det är någorlunda oförändrat de senaste åren. År 2020 anmäldes 5 616 övergrepp i rättssak, vilket var en viss minskning jämfört med föregående år. Antalet lagförda brott var 617.[2]

Övergrepp i rättssak har en vid straffskala som börjar vid fängelseminimum, dvs. 14 dagars fängelse. I normalfallet är det därför inte möjligt med vare sig hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning vid brott av normalgraden. Övergrepp i rättssak är ett brott av sådan art att starka skäl talar för att fängelse ska väljas som påföljd i normalfallet (se prop. 2001/02:59 Hets mot folkgrupp, m.m., s. 61). Det tycks inte vara vanligt att straffet överstiger två års fängelse (jr Martin Borgeke, Catharina Månsson och Georg Sterzel, Studier rörande påföljdspraxis med mera, femte uppl. s. 731 och Catharina Månsson, Björn Hansson och Martin Borgeke, Studier rörande påföljdspraxis med mera, elektronisk version 2021, s. 1115). Eftersom brottet inte har lägst sex månaders minimistraff och inte räknas upp i brottskatalogen i 27 kap. 19 § tredje stycket RB, kan hemlig övervakning av elektronisk kommunikation inte heller användas förutom i de undantagsfall då det med stöd av straffvärdeventilen fattas ett beslut om hemlig avlyssning av elektronisk kommunikation eller förutsättningarna för sådan avlyssning är uppfyllda och övervakningen ska äga rum i syfte att man ska utreda vem som skäligen kan misstänkas för brottet (27 kap. 18 § tredje stycket och 19 § fjärde stycket RB). Samtliga tre tvångsmedel kan användas vid grovt brott som har två års fängelse som minimistraff.

Övergrepp i rättssak är ett mycket allvarligt brott. För det första minskar det möjligheterna att utreda och lagföra det grundbrott som övergreppet i rättssak handlar om. För det andra kan risken för att utsättas för hot och våld minska benägenheten i allmänhet att medverka i brottsutredningar och rättegångar. Brottet kan alltså få allvarliga spridningseffekter, som kan förväntas vara större ju större risken att utsättas för hot och våld upplevs vara. Övergrepp i rättssak bidrar till utvecklingen av parallella samhällsstrukturer i utsatta områden (Myndighetsgemensam lägesbild om organiserad brottslighet

[2] Med lagförda brott avses samtliga brott som enskilda individer lagförts för. Dessa bygger på antal brott i lagföringsbeslut vilket innebär att om samma brott begicks av tre personer tillsammans så räknas de som tre lagförda brott.

2019 s. 28). Brottet kan alltså vara systemhotande. Med hänsyn till det anförda är det av ytterst stor vikt att de brottsbekämpande myndigheterna har goda möjligheter att utreda övergrepp i rättssak. Samtidigt ligger det i sakens natur att det är vanligt att målsäganden inte vill eller vågar medverka i utredningen. Frågan är då om en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter skulle förbättra möjligheterna att utreda sådana brott.

Det är enligt Brå vanligt att övergrepp i rättssak förövas direkt i samband med grundbrottet, som oftast är misshandel eller rån (Brå 2019:10 s. 36 och 37). I sådana fall är det förmodligen mer ovanligt att övergreppet i rättssak lämnar digitala spår, även om det givetvis kan förekomma att personen i efterhand diskuterar saken med någon annan. Men brottet kan också utövas muntligt via telefon eller i skrift, t.ex. via sms, chatt eller sociala medier (Brå 2019:10 s. 37). I sådana fall kan en möjlighet att avlyssna elektronisk kommunikation eller att utföra hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter vara avgörande för utredningen. Det relativt låga antalet lagföringsbeslut i förhållande till antalet anmälningar talar för att utredningsmöjligheterna behöver förbättras. Med hänsyn till det och till vad som framkommit i fråga om domstolarnas bedömning av straffvärdet, gör vi bedömningen att det finns ett behov av att lägga till övergrepp i rättssak i de relevanta brottskatalogerna för att skapa en möjlighet att i fler fall än i dag kunna använda hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter liksom även sådana uppgifter som avses i 2 § punkterna 6 och 7 i lagen om hemlig dataavläsning. Vi bedömer även att det skulle vara effektiva åtgärder som skulle kunna leda till att betydligt fler brott kan utredas och fler gärningspersoner lagföras.

Slutligen är frågan om det skulle vara proportionerligt att använda de nu aktuella hemliga tvångsmedlen vid utredningar om övergrepp i rättssak. Vi konstaterar då till att börja med att det inte är fråga om några nya hemliga tvångsmedel utan endast om ett utvidgat tillämpningsområde för befintliga tvångsmedel. Några nya risker för den personliga integriteten bedöms därför inte uppkomma. Däremot inne-

bär ett utvidgat tillämpningsområde att fler personer kan komma att utsättas för hemliga tvångsmedel (jfr våra resonemang i avsnitt 6.11). Vi konstaterar vidare att brottet har ett högt maxstraff och till sin karaktär är systemhotande. Det är ett brott som i normalfallet föranleder fängelse, även när straffvärdet är förhållandevis lågt. Många övergrepp i rättssak anmäls men relativt få lagförs. Det är mycket allvarligt om det sprids en uppfattning att man straffritt kan hota målsägande och vittnen för att hindra dem från att medverka i brottsutredning och rättsprocess. Vid en sammanvägning anser vi att det är proportionerligt och förenligt med relevanta bestämmelser i såväl regeringsformen som EU:s rättighetsstadga och Europakonventionen att införa en möjlighet att använda de nu aktuella tvångsmedlen vid förundersökningar om övergrepp i rättssak. Vår bedömning är att en sådan möjlighet bör införas. Som alltid bör det givetvis i det enskilda fallet krävas att åtgärden är proportionerlig och av synnerlig vikt för utredningen. Möjligheten att använda hemlig dataavläsning bör med utgångspunkt i behovet avse kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter samt uppgifter som finns lagrade i ett avläsningsbart informationssystem eller som visar hur ett sådant informationssystem används (2 § första stycket 1–3 samt 6 och 7 lagen om hemlig dataavläsning).

I lagrådsremissen En stärkt rättsprocess och en ökad lagföring (s. 37–40) föreslås att minimistraffet för övergrepp i rättssak av normalgraden ska höjas till fängelse i sex månader. Den särskilda graden ringa övergrepp i rättssak, som har straffskalan böter eller fängelse i högst sex månader, ska tas bort och ersättas med en möjlighet att bestämma straffet till fängelse i högst ett år vid mindre allvarliga fall av övergrepp i rättssak. Det föreslås vidare att en ny och mer preciserad kvalifikationsgrund för grovt brott införs (s. 41 och 42). I remissen bedöms förslaget leda till att fler personer döms för grovt övergrepp i rättssak och till en generell höjning av straffnivån för övergrepp i rättssak. Detta skulle i sin tur kunna innebära att hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning kan aktualiseras i fler fall än i dag. Vår bedömning är att en möjlighet att använda hemliga tvångsmedel vid utredningar om brott av normalgraden är motiverad även om lagrådsremissens förslag genomförs.

Mened

Brottet mened begås av den som under ed lämnar en osann uppgift eller förtiger sanningen (15 kap. 1 § BrB). Straffskalan är fängelse i högst fyra år eller, om brottet är ringa, böter eller fängelse i högst sex månader. Minimistraffet för grovt brott är fängelse i två år och det är möjligt att döma ut så mycket som fängelse i åtta år. Närbesläktade brott är osann partsutsaga och ovarsam utsaga (15 kap. 2 och 3 §§ BrB).

Enligt kriminalstatistiken för 2020 polisanmäldes det under året 276 brott enligt 15 kap. 1–3 §§ BrB, vilket innebar en viss ökning jämfört med föregående år. Samma år lagfördes 44 menedsbrott (40 år 2019)[3].

Straffskalorna för mened överensstämmer med straffskalorna för övergrepp i rättssak. Som utgångspunkt bör dock övergrepp i rättssak anses som ett allvarligare brott. I rättspraxis bestäms fängelsestraff oftast till några månader och det synes ovanligt att straffet bestäms till mer än två års fängelse (se Martin Borgeke, Catharina Månsson och Georg Sterzel, Studier rörande påföljdspraxis med mera, femte uppl. s. 665 och Catharina Månsson, Björn Hansson och Martin Borgeke, Studier rörande påföljdspraxis med mera, elektronisk version 2021 s. 1022–1029). För de personer som år 2014–2019 dömdes till fängelse för mened som huvudbrott var den genomsnittliga längden på fängelsestraffet 3 månader.[4] Det som i avsnittet om övergrepp i rättssak sagts om förutsättningarna för att använda hemliga tvångsmedel är alltså aktuellt även i fråga om mened av normalgraden. Det innebär att det i normalfallet inte är möjligt att använda vare sig hemlig avlyssning av elektronisk kommunikation, hemlig dataavläsning eller hemlig övervakning av elektronisk kommunikation. Däremot kan hemlig avlyssning och hemlig övervakning av elektronisk kommunikation och även hemlig dataavläsning användas vid grovt brott som har två års fängelse som minimistraff. Av Brå:s kriminalstatistik framgår emellertid att under tidsperioden 2007–2020 har bestämmelsen om grov mened inte tillämpats i något fall.

Även mened är ett allvarligt brott som innebär ett åsidosättande av respekten för rättsväsendet och som påverkar möjligheterna att

[3] Med lagförda brott avses samtliga brott som enskilda individer lagförts för. Dessa bygger på antal brott i lagföringsbeslut vilket innebär att om samma brott begicks av tre personer tillsammans så räknas de som tre lagförda brott.
[4] Avrundat till närmsta hela månad.

upprätthålla rättssystemets effektivitet och tillförlitlighet (se t.ex. Högsta domstolens avgörande NJA 1999 s. 561). Mened är på den grunden ett brott av sådan art att normalpåföljden ska vara fängelse och att domstolen kan välja ett alternativ till fängelse endast om starka skäl talar emot fängelse (se bl.a. det nyss nämnda avgörandet). Det är därför mycket viktigt att brottet kan utredas och den som är skyldig lagföras. Det är allvarligt och samhällsskadligt om det sprids en uppfattning att man straffritt kan ljuga under ed.

Samtidigt är brottet notoriskt svårt att utreda. Misstankar om mened gäller ofta personer som rör sig i miljöer där det råder en tystnadskultur, t.ex. inom kriminella nätverk eller andra grupperingar vars medlemmar förväntas skydda varandra. Ofta görs bedömningen att det inte ens finns förutsättningar att inleda en förundersökning. Det kan vidare begås av personer som inte har något intresse i fråga om grundbrottet, utan som råkat bevittna grundbrottet eller något som har anknytning till detta. Personen i fråga kan vara utsatt för övergrepp i rättssak eller andra påtryckningar, och kan därför vara både vittne till grundbrottet, målsägande avseende ett övergrepp i rättssak och gärningsperson i fråga om menedsbrottet. Många gånger kan den enda möjligheten att bevisa menedsbrottet vara att man kan visa på kontakter mellan den som är misstänkt för grundbrottet eller någon person med kopplingar till denne och det vittne som misstänks för mened. Det kan då vara avgörande att det är möjligt att få tillgång till uppgifter om elektroniska meddelanden, om innehållet i sådana meddelanden eller om att vissa personer befunnit sig på samma plats vid en viss tid. Sådana uppgifter kan man få fram genom övervakning av elektronisk kommunikation, avlyssning av elektronisk kommunikation eller hemlig dataavläsning. Enligt uppgift från åklagare är det vanligt att man får lägga ner utredningar om mened i brist på bevis.

Det anförda talar, tillsammans med det relativt låga antalet fällande domar i relation till anmälda brott, för att det finns ett behov av en möjlighet att använda hemliga tvångsmedel. Det bör framhållas att förekomsten av eventuella påtryckningar kan vara till fördel för menedsvittnet vid domstolens bedömning av straffvärdet. Behovet av en förbättrad möjlighet att utreda menedsbrott handlar alltså inte bara om att personen ska kunna hållas ansvarig för brottet, utan även om att han eller hon ska få en rättvis prövning där alla relevanta omständigheter kan beaktas. Sammantaget bedömer vi alltså att det finns

ett behov av en möjlighet att kunna använda de nu aktuella hemliga tvångsmedlen vid förundersökningar om mened. Vi bedömer även att det skulle vara effektiva åtgärder som skulle kunna leda till att fler menedsbrott kan utredas och fler gärningspersoner lagföras.

När det gäller frågan om proportionalitet gör sig samma argument gällande som när det gäller övergrepp i rättssak, även om man kan hävda att menedsbrottet bör vara att anse som något mindre allvarligt än övergrepp i rättssak (jfr SOU 2021:35 s. 137). Straffskalan är emellertid densamma och det rör sig även här om ett systemhotande brott. Bedömningen utfaller därför på samma sätt, dvs. vi gör bedömningen att det är proportionerligt och förenligt med relevanta bestämmelser till skydd för den enskilde att införa en möjlighet att vid förundersökningar om mened använda övervakning av elektronisk kommunikation, avlyssning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter. Vi föreslår alltså att det införs en möjlighet att använda dessa tvångsmedel vid förundersökningar om mened. Möjligheten att använda hemlig dataavläsning bör avgränsas på samma sätt som när det gäller övergrepp i rättssak.

I lagrådsremissen En stärkt rättsprocess och en ökad lagföring (s. 30–33) föreslås införande av en ny kvalifikationsgrund som anger att det vid bedömningen av om ett brott är grovt särskilt ska beaktas om meneden begåtts med uppsåt att försvåra eller förhindra utredningen eller lagföringen av allvarlig brottslighet. Den brottslighet som meneden avser bör regelmässigt anses som allvarlig om den innefattar ett brott som har ett minimistraff på minst två års fängelse eller om straffvärdet av brottsligheten i det enskilda fallet bedöms uppgå till eller överstiga fängelse i två år. Den del av den befintliga kvalifikationsgrunden som tar sikte på att gärningspersonen haft uppsåt att en oskyldig ska fällas till ansvar för ett allvarligt brott föreslås bli ändrad så att uttrycket allvarligt brott byts ut mot uttrycket allvarlig brottslighet med den innebörd uttrycket har i den nya kvalifikationsgrunden. Regeringen bedömer att förslagen kommer att medföra att straffskalan för grov mened kommer att tillämpas i praktiken. Inga ändringar i straffskalorna föreslås.

Vår bedömning är att en möjlighet att använda hemliga tvångsmedel vid utredningar om brott av normalgraden är motiverad även om lagrådsremissens förslag genomförs.

Skyddande av brottsling

Brottet skyddande av brottsling innebär att någon döljer en brottsling, hjälper brottslingen att komma undan, undanröjer bevis om brottet eller på annat liknande sätt motverkar att brottet uppdagas eller beivras (17 kap. 11 § BrB). Syftet med bestämmelsen är framför allt att skydda statens brottsutredande verksamhet och dess verkställande av påföljd för brott (se prop. 1992/93:141 om ändring i brottsbalken m.m., s. 48). Som exempel på döljande eller hjälpande av brottsling har i förarbetena angetts att gömma någon, låna ut en bil, själv ange sig för brottet eller aktivt leda polisen på villospår (se a. prop. s. 48). Ett typiskt exempel på skyddande av brottsling är att ge en efterspanad person skjuts med bil (se t.ex. NJA 2015 s. 31). Att hjälpa en brottsling att undkomma verkställighet av påföljden eller på annat liknande sätt undandra honom sådan verkställighet faller också under bestämmelsen. Om brottslingen har frihetsberövats döms dock i stället för främjande av flykt enligt 17 kap. 12 § BrB. (Se Agneta Bäcklund m.fl., Brottsbalken, En kommentar, [2021-12-01 JUNO], kommentaren till 17 kap. 11 §.)

Straffet är böter eller fängelse i högst ett år för brott av normalgraden. Om brottet är grovt är minimistraffet sex månaders fängelse och maximistraffet fängelse i högst fyra år. Den som inte insåg men hade skälig anledning att anta att den andre var brottslig, döms till böter. Ansvar ska inte dömas ut om gärningen är att anse som ringa med hänsyn till gärningsmannens förhållande till brottslingen och övriga omständigheter.

Av kriminalstatistiken från Brå[5] framgår att för skyddande av brottsling (såväl normalgraden som grovt brott) lagfördes under åren 2014–2019 i genomsnitt i 15,5 fall. För skyddande av brottsling som huvudbrott dömdes under åren 2014–2019 i genomsnitt i 6,5 fall och i 1 av dessa bestämdes påföljden till fängelse. För skyddande av brottsling, grovt brott, som huvudbrott dömdes under motsvarande år i genomsnitt i 5 fall och i 3,5 av dessa bestämdes påföljden till fängelse.

För de som år 2014–2019 dömdes till fängelse för skyddande av brottsling av normalgraden som huvudbrott var den genomsnittliga längden på fängelsestraffet 4 månader dvs. något längre än det genomsnittliga straffet för mened. Detta är något förvånande med tanke på den lindrigare straffskalan. För de som under motsvarande tidsperiod

[5] Redovisningen är hämtad från SOU 2021:35 En stärkt rättsprocess och en ökad lagföring.

dömdes för skyddande av brottsling, grovt brott, som huvudbrott var den genomsnittliga längden på fängelsestraffet 12,5 månader.[6]

Straffskalan för brottet av normalgraden innebär att hemliga tvångsmedel inte är tillåtna med tillämpning av huvudregeln. För det grova brottet kan hemlig övervakning av elektronisk kommunikation förekomma, men däremot enligt huvudregeln inte hemlig avlyssning av elektronisk kommunikation och andra hemliga tvångsmedel med samma eller strängare villkor för användningen. Undantaget är om en straffvärdeventil är tillämplig. Utifrån praxis lär detta dock sällan vara möjligt i praktiken.

Skyddande av brottsling begås vanligen av någon som har en stark lojalitet mot den som han eller hon vill skydda. I vissa fall kan det handla om att man hör till samma kriminella gruppering, inom vilken det råder en tystnadskultur. Enligt de brottsbekämpande myndigheterna är det vanligaste dock att brottet begås av någon närstående till den brottsliga personen. Den närstående kan givetvis ingå i samma kriminella gruppering men behöver inte göra det. Under alla omständigheter innebär bl.a. lojalitetsförhållandena att brotten ofta är svårutredda. Detta kan tala för en möjlighet att använda hemliga tvångsmedel. Vi konstaterar samtidigt att det är ett relativt ovanligt brott. Även om brottet kan leda till att ett annat brott blir svårare är utreda eller att lagföringen försvåras, har det inte samma negativa effekter som övergrepp i rättssak eller mened. Detta återspeglas i en betydligt lindrigare straffskala än de angivna brotten. Straffskalan är i dagsläget lindrigare än straffskalan för samtliga de brott som i dag kan föranleda hemliga tvångsmedel, med undantag för olovlig underrättelseverksamhet mot främmande makt som också kan föranleda böter eller fängelse i högst ett år. Den överensstämmer med straffskalan för bl.a. ringa barnpornografibrott, som lagstiftaren undantagit från möjligheten att använda hemlig övervakning av elektronisk kommunikation (prop. 2002/03:74 s. 35).

I lagrådsremissen En stärkt rättsprocess och en ökad lagföring föreslås att straffskalan för skyddande av brottsling ska skärpas (s. 43–45). För skyddande av brottsling av normalgraden föreslås straffskalan vara böter eller fängelse i högst två år. För grovt brott föreslås straffskalan vara fängelse i lägst ett och högst sex år. Det grova brottet föreslås också få en egen brottsbeteckning, grovt skyddande av brottsling. Avsikten med förslaget är att åstadkomma en förhöjd straffnivå och

[6] Straffläng derna är avrundade till närmsta halva månad.

samtidigt bibehålla en viss straffvärdemässig skillnad mot ännu allvarligare brott såsom övergrepp i rättssak.

Förslaget innebär en strängare syn på skyddande av brottsling än den som nuvarande reglering ger uttryck för. Om förslagen genomförs kan det tala för att brottet tas in i brottskatalogerna. Vi bedömer emellertid att varken brottets allvar, förekomst eller utredningssvårigheterna är sådana att de motiverar att man gör det möjligt att använda hemliga tvångsmedel vid förundersökning om skyddande av brottsling, och detta oavsett om straffet skärps i enlighet med lagrådsremissens förslag eller inte. Med hänsyn till det anförda anser vi att skyddande av brottsling inte bör läggas till i någon av brottskatalogerna.

Utpressning

Brottet utpressning innebär att någon genom olaga tvång förmår någon till en handling eller underlåtenhet som innebär vinning för gärningsmannen och skada för den tvingade eller någon i vars ställe denne är (9 kap. 4 § BrB). Straffet är fängelse i högst två år. Om brottet är ringa, döms för ringa utpressning till böter eller fängelse i högst sex månader. Om brottet är grovt döms för grov utpressning till fängelse i lägst ett år och sex månader och högst sex år.

Antalet anmälda fall av utpressning har ökat kraftigt under de senaste decennierna. År 2000 anmäldes 699 fall av utpressning. Under år 2019 anmäldes drygt 9 750 utpressningsbrott. År 2020 uppgick anmälningarna till drygt 7 000. Antalet anmälningar har alltså mer än tiodubblats. Brå anför i studien Utpressning i Sverige. Tvistelösning, bestraffning och affärsidé (Brå 2012:6 s. 21 f.) att ökningen sannolikt beror på en kombination av en allmänt ökad anmälningsbenägenhet och att antalet gärningar faktiskt har ökat. Samtidigt är lagföringarna relativt få. Antalet lagförda brott av normalgraden uppgick under 2020 till 397 och grova brott till 225.[7]

Huvudregeln för hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning är att minimistraffet för det brott som utredningen gäller måste vara två års fängelse eller mer. Huvudregeln är alltså inte uppfylld när det gäller utpressning av normalgraden. När fängelse döms ut är straffet i de allra flesta fall kortare

[7] Med lagförda brott avses samtliga brott som enskilda individer lagförts för. Dessa bygger på antal brott i lagföringsbeslut vilket innebär att om samma brott begicks av tre personer tillsammans så räknas de som tre lagförda brott.

än två år (se Martin Borgeke, Catharina Månsson och Georg Sterzel, Studier rörande påföljdspraxis med mera, femte uppl. s. 571 och Catharina Månsson, Björn Hansson och Martin Borgeke, Studier rörande påföljdspraxis med mera, elektronisk version 2021 s. 862). Det kan därför antas att man vanligen inte heller kan tillämpa straffvärdeventilen i respektive bestämmelse. Eftersom utpressning av normalgraden inte har lägst sex månaders minimistraff och inte räknas upp i brottskatalogen i 27 kap. 19 § tredje stycket RB, kan hemlig övervakning av elektronisk kommunikation inte heller användas förutom i de undantagsfall då förutsättningarna är uppfyllda för hemlig avlyssning av elektronisk kommunikation.

Vid grov utpressning kan hemlig övervakning av elektronisk kommunikation användas redan med stöd av huvudregeln om sex månaders minimistraff. Däremot når straffskalan inte upp till kravet på att det lägsta föreskrivna straffet ska vara fängelse i två år. Hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning kan därför inte användas med tillämpning av huvudregeln i respektive bestämmelse. Däremot kan det förekomma allvarliga fall där straffvärdeventilen är tillämplig.

Enligt Brå fyller utpressning tre olika funktioner (Brå 2012:6 s. 13 och 14. En funktion är tvistlösning. I sådana fall har utpressningen sin grund i tvister som uppstått i en nära relation, i samband med en anställning eller någon form av affär eller avtal. I sådana fall är utpressningen en alternativ metod för tvistlösning där utövaren försöker få rätt genom att själv, eller med hjälp av andra personers skrämselkapital, tvinga den andre till eftergift. I andra fall är utpressning en form av bestraffning mot någon som man anser gjort något fel. Detta förekommer inom kriminella grupperingar och har även spridit sig till ungdomar. Det kan då exempelvis förekomma att man ”bötfäller” personer som lämnat uppgifter till myndigheter. Slutligen kan utpressning vara en sorts affärsidé. I sådana fall bedrivs utpressningen som regel systematiskt och ofta av personer från en kriminell miljö som har ett etablerat skrämselkapital. En sådan affärsidé är att köpa upp verkliga skulder och driva in dem med oskäligt hög ränta. I Brås studie Otillåten påverkan mot företag (Brå 2012:12 s. 46) framkom det att utpressaren tillhörde grupperingar inom organiserad brottslighet i 59 procent av de studerade förundersökningarna. Ofta är då flera personer inblandade.

Utpressning är ett allvarligt brott som bidrar till otrygghet i samhället. Vidare kan utpressning vara systemhotande när den bedrivs som alternativ tvistlösning, som bestraffning för att personer lämnat uppgifter till myndigheterna eller när personer i det legala samhället använder indrivningstjänster eller betalar för beskydd i stället för att använda legala lösningar (Brå 2012:6 s. 13 och 14). Det är därför mycket angeläget att de brottsbekämpande myndigheterna har tillräckliga verktyg för att effektivt utreda utpressning. Samtidigt är utpressningsbrotten svåra att utreda. Detta har flera förklaringar. En av förklaringarna är att den som är eller har varit utsatt för utpressning inte sällan är obenägen att medverka i utredningen. Skälet kan vara rädsla för gärningspersonen och att denne ska förverkliga tidigare framförda hotelser, som kan ha förnyats under förundersökningens gång. De personer som ligger bakom eller som faktiskt utövar utpressningen har inte sällan ett stort skrämselkapital, eller så ger de sken av att ha det (Brå 2012:12 s. 115). Oavsett om det i verkligheten finns kapacitet och vilja att förverkliga framförda hotelser, kan situationen skapa en stark rädsla inte bara för vad som händer om man inte gör som förövaren begär utan också för vad som skulle bli följden av att man medverkar i förundersökningen och rättsprocessen. I vissa fall är både förövare och offer aktiva inom den organiserade brottsligheten och omfattas av dess tystnadskultur. En annan svårighet är att det ofta saknas stödbevisning, vilket kan göra det svårt att styrka brott även när målsäganden medverkar (Brå 2012:12 s. 96).

Med hänsyn till det anförda bedömer vi att det finns behov av en möjlighet att vid förundersökningar om utpressning använda hemlig avlyssning och hemlig övervakning av elektronisk kommunikation. Det bedöms även föreligga ett behov av en möjlighet att använda hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter, kommunikationsövervakningsuppgifter och platsuppgifter samt uppgifter som finns lagrade i ett informationssystem och uppgifter om hur ett informationssystem används. I de fall elektroniska kontakter förekommit mellan den misstänkte och målsäganden kan man därigenom få kunskap om vilka kontakter som förekommit och om innehållet i elektroniska meddelanden. Man kan också få kunskap om var den misstänkte befunnit sig vid olika tidpunkter, vilket t.ex. kan ha betydelse som stöd för målsägandens påstående om att den misstänkte besökt målsägandens företag vid vissa närmare angivna tidpunkter. Eftersom det är vanligt att flera gärningsmän samverkar kan det dock

förväntas vara än vanligare att man genom hemliga tvångsmedel kan få kunskap om brottsligheten via avlyssning, avläsning eller övervakning av kommunikation mellan gärningspersonerna. Under alla förhållanden bedömer vi att en möjlighet att använda de nu aktuella hemliga tvångsmedlen skulle vara effektiv och kunna leda till att fler brott kan utredas och fler gärningspersoner lagföras.

Nästa fråga är om det är proportionerligt att använda hemliga tvångsmedel för utpressning av normalgraden. Vi konstaterar till att börja att utpressning kan vara ett systemhotande brott, vilket i sig är allvarligt. Straffskalan är dock lindrigare än straffskalan för övergrepp i rättssak och mened. Det är därför inte självklart att proportionalitetsbedömningen ska utfalla på samma sätt. Vidare måste man beakta bl.a. det krav som följer av EU-domstolens praxis på att brottsbekämpande myndigheter i princip endast får beviljas tillgång till lagrade uppgifter i syfte att bekämpa allvarlig brottslighet (se bl.a. dom den 2 mars 2021 i mål C-746/18). Någon vedertagen definition av vad som avses med allvarliga brott finns inte och man kan diskutera vad som bör läggas i ett sådant krav. Det finns inte någon generell definition av allvarlig brottslighet inom EU-rätten eller inom svensk rätt. Däremot förekommer i olika sammanhang, både i EU-rätten och i svensk rätt, uppräkningar av brott som – i det sammanhanget uppräkningen förekommer – ska jämställas med grova brott eller som på annat sätt ska särbehandlas. Ett exempel på en sådan uppräkning är bilagan till lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder. I den bilagan finns angivet brott som spänner över en stor del av straffskalan; från mord och våldtäkt till förfalskning, piratkopiering och barnpornografi. Just i denna uppräkning har rådet uppmanat medlemsstaterna att ta ”vederbörlig hänsyn” till vid införandet av det numera upphävda datalagringsdirektivet (prop. 2010/11:46 Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG, s. 21). Utpressning är ett av de brott som räknas upp i bilagan. Det finns dock även exempel på EU-rättsakter där utpressning inte omfattas av en uppräkning av grov brottslighet, se Europaparlamentets och rådets direktiv 2016/681 av den 27 april 2016 (direktivet om PNR-uppgifter).

Vid en sammanvägning av olika faktorer, däribland svårigheten att utreda brotten, den potentiellt systemhotande karaktären och den omständigheten att utpressning kan vara en lukrativ affärsidé för kriminella sammanslutningar som ägnar sig åt organiserad brottslig-

het, gör vi bedömningen att det är fråga om ett allvarligt brott och att det är proportionerligt att införa en möjlighet att använda hemliga tvångsmedel vid förundersökningar om utpressning. Möjligheten att använda hemlig dataavläsning bör begränsas på samma sätt som när det gäller övergrepp i rättssak och mened.

Gängbrottsutredningen har i SOU 2021:68 föreslagit att maximistraffet för utpressning höjs från fängelse i två år till fängelse i tre år. Straffskalan för grov utpressning föreslås höjas från fängelse i lägst ett år och sex månader och högst sex år till fängelse i lägst två och högst åtta år. Om förslaget leder till lagstiftning behöver grov utpressning inte läggas till i brottskatalogen.

Grovt jaktbrott

Vissa uppsåtliga och grovt oaktsamma överträdelser av jaktlagen (1987:259) utgör jaktbrott. Det kan exempelvis röra sig om någon som olovligen jagar på någon annans jaktområde eller som jagar vilt som är fredat (43 § jaktlagen). Straffet för jaktbrott av normalgraden är böter eller fängelse i högst ett år. Om jaktbrottet är grovt döms till fängelse i lägst sex månader och högst fyra år (4 § samma lag). Vid bedömandet av om brottet är grovt ska särskilt beaktas om det avsåg ett särskilt hotat, sällsynt eller annars särskilt skyddsvärt vilt, om det har utförts vanemässigt eller annars i större omfattning, om det har utförts med otillåten hjälp av ett motordrivet fortskaffningsmedel eller någon annan motordriven anordning eller om det har utförts med en särskilt plågsam jaktmetod.

Under 2020 polisanmäldes 67 fall av illegal rovdjursjakt, vilket utgjorde en ökning jämfört med föregående år. Avseende övriga brott mot jaktlagen registrerades drygt 600 anmälningar. Av lagföringsstatistiken framgår att antalet lagförda brott mot jaktlagen under 2020 uppgick till 175.[8]

Straffet bestäms vanligen till böter (Martin Borgeke, Catharina Månsson och Georg Sterzel, Studier rörande påföljdspraxis med mera, femte uppl. s. 1174 och Catharina Månsson, Björn Hansson och Martin Borgeke, Studier rörande påföljdspraxis med mera, elektronisk version 2021 s. 1667). Dock har Högsta domstolen uttalat att jaktbrott

[8] Med lagförda brott avses samtliga brott som enskilda individer lagförts för. Dessa bygger på antal brott i lagföringsbeslut vilket innebär att om samma brott begicks av tre personer tillsammans så räknas de som tre lagförda brott.

är av den arten att det krävs alldeles särskilda skäl för att välja annan påföljd än fängelse, när straffvärdet uppgår till fängelse i sex månader eller mer (NJA 2006 s. 610).

Om brotten begås vanemässigt eller i större omfattning kan det leda till att brotten ska rubriceras som grova (44 § jaktlagen). I ett sådant fall kan hemlig övervakning av elektronisk kommunikation tillgripas, eftersom miministraffet är sex månaders fängelse. Huvudregeln för hemlig avlyssning och hemlig dataavläsning är dock inte tillämplig ens vid grovt brott. De nuvarande straffvärdeventilerna torde i stort sett inte heller vara tillämpliga. Av praxis framgår nämligen att straffvärdet för ett enstaka grovt brott normalt inte bedöms som högre än två års fängelse ens när det föreligger flera kvalificerande omständigheter samtidigt. Som exempel kan man nämna en dom från Hovrätten för övre Norrland (dom 2013-05-30 i mål B 362-12) där straffet bestämdes till två års fängelse. Brottet avsåg då ett särskilt skyddsvärt vilt, nämligen järv. Jakten hade skett med användning av snöskoter och hade dessutom skett på ett sätt som var särskilt plågsamt för järven och som präglades av ett besinningslöst raseri. I ett annat mål dömde Hovrätten för nedre Norrland till två års fängelse för olovlig vargjakt (dom 2014-06-03 i mål B 539-13). I det fallet hade man använt snöskoter, kört på vargen och sedan klubbat ihjäl den. Vargen hade omfattande inre skador och hade dessutom utsatts för maximal ansträngning. Av det anförda drar vi slutsatsen att det med nuvarande regler i princip inte är möjligt att använda hemlig avlyssning och hemlig dataavläsning vid förundersökningar om grovt jaktbrott annat än möjligen i något synnerligen särpräglat fall.

Enligt uppgift från de brottsbekämpande myndigheterna är grova jaktbrott ytterst svåra att utreda. Brotten begås på tider och platser där det sällan finns några utomstående vittnen. Det är som regel inte heller möjligt för polisen att bedriva spaning. I många fall är flera personer inblandade i brottet, men de inblandade och personer i kretsen runt dem är ofta obenägna att medverka i utredningen. Det har till utredningen framförts att det råder en stark tystnadskultur i de kretsar där detta slags brott begås. Denna kan omfatta inte bara gärningspersonerna och deras närmaste omgivning utan hela samhällen. Med hänsyn till det anförda kan i praktiken en hemlig avlyssning av elektronisk kommunikation eller en hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter vara den enda möjligheten att med framgång utreda brottet. Genom sådana tvångsmedel kan man

fånga upp innehållet i meddelanden mellan de inblandade eller mellan inblandade och initierade personer i omgivningen där man utbyter information om tidigare begångna och planerade jaktbrott. Genom en hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning avseende platsuppgifter kan man vidare få fram bevisning om var en misstänkt befunnit sig vid en för utredningen relevant tidpunkt.

Med hänsyn till utredningssvårigheterna gör vi bedömningen att det finns ett behov av en möjlighet att använda hemliga tvångsmedel för att det ska finnas rimliga möjligheter att utreda grovt jaktbrott. Som tidigare sagts kan en sådan möjlighet många gånger vara den enda framkomliga vägen att utreda och få fram bevisning om brottet. Eftersom det är vanligt med flera gärningsmän som måste koordinera sig, är det antagligt att elektroniska kontakter är vanliga och att hemliga tvångsmedel alltså skulle vara en effektiv åtgärd i många fall.

Frågan återstår då om det är proportionerligt att använda hemliga tvångsmedel. Jaktbrott kan inte beskrivas som systemhotande. Dock kan grovt jaktbrott hota den biologiska mångfalden och utrotningshotade rovdjursstammar med litet genetiskt underlag. Det är därför angeläget att särskilt olovlig rovdjursjakt effektivt kan motverkas och att personer inte upplever att det är riskfritt att begå jaktbrott. Utredningssvårigheterna är enligt de brottsbekämpande myndigheterna sådana att brotten många gånger inte kan utredas om man inte kan använda hemlig avlyssning av elektronisk kommunikation eller motsvarande hemlig dataavläsning. När det gäller grovt jaktbrott kan hemlig övervakning av elektronisk kommunikation komma i fråga redan med tillämpning av huvudregeln i 27 kap. 19 § RB, eftersom minimistraffet är sex månader. Detta förutsätter dock att det finns en skäligen misstänkt. Däremot kan det, som anförts ovan, endast i sällsynta fall antas vara möjligt med hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning och då med tillämpning av straffvärdeventilen i respektive bestämmelse. Det grova brottet har samma tak i straffskalan som bl.a. övergrepp i rättssak och mened, men har ett strängare minimistraff. Med hänsyn till detta, till vikten av att allvarliga jaktbrott kan utredas och till de stora utredningssvårigheterna, bedömer vi att det är proportionerligt och även i övrigt förenligt med bestämmelser till skydd för enskildas personliga integritet att införa en möjlighet att använda hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning. Möjligheten att använda hemlig dataavläsning bör begränsas på samma sätt som när

det gäller övergrepp i rättssak, mened och utpressning. Hemlig övervakning av elektronisk kommunikation är möjlig redan enligt gällande rätt. Dock innebär förslaget att åtgärden kan vidtas även när det inte finns någon skäligen misstänkt.

Grovt insiderbrott

Straffbestämmelser för insiderbrott finns i lagen (2016:1307) om straff för marknadsmissbruk på värdepappersmarknaden. För insiderbrott döms personer som på särskilt angivna sätt utnyttjar insiderinformation eller hjälper andra att utnyttja sådan information. Straffet är fängelse i högst två år. Om brottet med hänsyn till gärningsmannens ställning, vinningen av brottet eller övriga omständigheter är grovt, döms för grovt insiderbrott till fängelse i lägst sex månader och högst sex år.

År 2020 anmäldes 151 fall av insiderbrott, inklusive grovt brott. Antalet lagförda insiderbrott uppgick till 4 och grova insiderbrott till 3. En genomgång av de senaste årens domstolspraxis visar att det är förhållandevis vanligt med frikännande domar. Genom den nya marknadsmissbrukslagen höjdes straffmaximum från fyra till sex års fängelse, vilket avsågs skapa utrymme för en mer differentierad straffmätning när det gäller bl.a. insiderbrott som är särskilt allvarliga. Såvitt framgår av rättspraxis och uppgifter från Ekobrottsmyndigheten förekommer det dock ytterst sällan förundersökningar rörande grovt insiderbrott där straffvärdet kan antas överstiga två års fängelse. I dagsläget har hemlig avlyssning förekommit i något enstaka ärende och bedömningen från Ekobrottsmyndigheten är att det är ytterst sällan som det finns förutsättningar för detta. Utrymmet för att med tillämpning av straffvärdeventilerna använda hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning är alltså ytterst begränsat i praktiken. Hemlig övervakning av elektronisk kommunikation kan däremot användas, eftersom minimistraffet för det grova brottet är sex månaders fängelse, förutsatt att någon är skäligen misstänkt.

Insiderbrott är en typ av brottslighet som är svårupptäckt. Den är också förenad med svårigheter från bevissynpunkt bl.a. på grund av att det regelmässigt saknas vittnen, att informationen ofta sprids muntligen i slutna rum och att det inte sker något inflöde av underrättelseinformation. Det är som regel inte heller möjligt för polisen

att bedriva spaning. Till detta kan tilläggas att de misstänkta personerna inte sällan är närstående till varandra, vilket har inneburit ett hinder för utredande myndigheter från att använda bevisning i form av skriftliga meddelanden såsom sms och chattar till följd av beslagsförbudet i närståendefallet (27 kap. 2 § andra stycket RB). Om förslagen i prop. 2021/22:119 genomförs kommer det sistnämnda problemet att försvinna, eftersom det där föreslås att beslagsförbudet i närståendefallet slopas. Även med beaktande av den förbättring av utredningsmöjligheterna som detta förslag innebär gör vi, med hänsyn till det som i övrigt anförts, bedömningen att det i och för sig finns ett behov av en möjlighet att använda hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning i utredningar om grovt insiderbrott.

Insiderbrott sker regelmässigt vid enstaka tillfällen, snarare än systematiskt. Det är normalt inte heller fråga om organiserad brottslighet. Den straffvärdeventil för viss flerfaldig brottslighet som vi föreslår kommer därför normalt inte att vara tillämplig. Som redan konstaterats är det med hänsyn till straffmätningspraxis i praktiken uteslutet att tillämpa de gällande straffvärdeventilerna avseende hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning.

Nästa fråga är om det skulle vara effektivt att lägga till grovt insiderbrott i brottskatalogerna. Det kan då till att börja med konstateras att det regelmässigt är två eller fler personer inblandade i brottligheten. Typfallet är att det är en person som ger information och en eller fler som handlar. Det kan därför antas att det ofta förekommer elektronisk kommunikation mellan de inblandade. Även om brottet oftast är avslutat när förundersökningen börjar hos Ekobrottsmyndigheten kan det antas att en möjlighet att använda hemlig dataavläsning eller hemlig avlyssning av elektronisk kommunikation inte sällan kan ge värdefull information, t.ex. om innehållet i tidigare skickade meddelanden. Ekobrottsmyndigheten har anfört att en möjlighet att använda de angivna hemliga tvångsmedlen skulle vara mycket värdefull med hänsyn till att brotten är så svårutredda. Samtidigt har myndigheten anfört att det endast i ett fåtal ärenden per år kan antas bli aktuellt att tillgripa så ingripande åtgärder som hemlig avlyssning. Även med beaktande av det bedömer vi att hemlig avlyssning och hemlig dataavläsning kan vara effektiva åtgärder i de ärenden där tvångsmedlen kan komma att användas.

Slutligen är frågan om det är proportionerligt med hemliga tvångsmedel för grovt insiderbrott. Grovt insiderbrott har en relativt vid straffskala och ett högt maximistraff. Lagstiftaren har alltså gett uttryck för att det är fråga om allvarlig brottslighet. Regeringen har uttalat att det rör sig om gärningar som påverkar förtroendet för ett system som har betydelse för samhällets funktion (prop. 2016/17:22 Effektiv bekämpning av marknadsmissbruk, s. 294). I skälssatserna till EU-lagstiftningen på området,[9] som kompletteras av bl.a. marknadsmissbrukslagen, betonas att väl fungerande värdepappersmarknader som har allmänhetens förtroende är en förutsättning för ekonomisk tillväxt och välstånd och att marknadsmissbruk skadar finansmarknadernas integritet och allmänhetens förtroende för värdepappersmarknaderna. Det bör också nämnas att en stor del av privatpersoners sparande och även pensionsmedel är placerade på värdepappersmarknaden. Högsta domstolen har i NJA 2008 s. 292 (Tivoxmålet) uttalat att det finns skäl att anse att det bör finnas en viss presumtion för fängelsestraff i allvarligare fall av insiderbrott, även när det gäller brott av normalgraden. Anledningen angavs vara att det är angeläget att motverka insiderbrott som allvarligt äventyrar allmänhetens förtroende för de finansiella marknaderna och som inbringar stora vinster på andras bekostnad. Domstolen konstaterade vidare att brott av det slaget kan vara svåra att upptäcka och att fängelsestraff på detta område kan ha större preventiv betydelse än i många andra sammanhang. Även detta understryker brottens allvar. Om överträdelser och brott på värdepappersmarknaden inte kan bekämpas och lagföras på ett effektivt sätt finns det en risk för att värdepappersmarknaden tappar i förtroende. Kan investerare inte lita på kurser och volymer vågar man inte heller handla. Investerare, större som mindre, går då till andra marknader eller avstår. Då minskar likviditeten (handelsvolymen) på värdepappersmarknaden, vilket medför att värdepappersmarknaden utvecklas sämre.

Sammanfattningsvis är att det är ett tungt vägande samhällsintresse att grova insiderbrott effektivt kan motverkas och att personer inte upplever att det är riskfritt att begå insiderbrott. Sverige är dessutom enligt EU:s regelverk på området skyldigt att ha effektiva

[9] Se skäl 2 till Europaparlamentets och rådets förordning (EU) nr 596/2014 av den 16 april 2014 om marknadsmissbruk (marknadsmissbruksförordning) och om upphävande av Europaparlamentets och rådets direktiv 2003/6/EG och kommissionens direktiv 2003/124/EG, 2003/125/EG och 2004/72/EG och skäl 1 till Europaparlamentets och rådets direktiv 2014/57/EU av den 16 april 2014 om straffrättsliga påföljder för marknadsmissbruk (marknadsmissbruksdirektiv).

och avskräckande sanktioner. Det kan diskuteras om sanktionssystemet i praktiken framstår som effektivt och avskräckande om de brottsbekämpande myndigheternas möjligheter att utreda brotten är små. Vid en sammanvägning anser vi att intresset av att man effektivt kan utreda grova insiderbrott överväger de motstående intressena, inklusive enskildas intresse av skydd för sitt privatliv. Vi bedömer även att en sådan möjlighet är förenlig med Sveriges åtaganden enligt Europakonventionen och EU:s rättighetsstadga. Därför föreslår vi att det ska införas en möjlighet att vid förundersökningar om grovt insiderbrott använda hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning. Möjligheten att utnyttja hemlig dataavläsning bör begränsas på motsvarande sätt som vi föreslagit beträffande övergrepp i rättssak och övriga brott som omfattas av våra förslag i denna del. Hemlig övervakning av elektronisk kommunikation är möjlig redan enligt gällande rätt när det finns en skäligen misstänkt. Ändringarna innebär även att hemlig övervakning kommer att kunna användas i syfte att utreda vem som skäligen kan misstänkas för brottet.

Grovt dataintrång

De brottsbekämpande myndigheterna har framhållit att komplex itbrottslighet är mycket svårutredd. Denna brottslighet utmärker sig på det sättet att det sällan finns någon som skäligen kan misstänkas för brottet, och att de ansvariga döljer sig genom lager av digital infrastruktur. Många gånger har de brottsbekämpande myndigheterna endast kunskap om någon del av den infrastruktur som använts vid brottet. Som kommer att utvecklas närmare i avsnitt 7.5 framstår det som nödvändigt att myndigheterna har en möjlighet att använda hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsövervakningsuppgifter i realtid för att man över huvud taget ska komma vidare i utredningen och identifiera en skäligen misstänkt. Såsom regelverket är uppbyggt är en förutsättning för detta i sin tur att brottet kan leda till hemlig avlyssning av elektronisk kommunikation (27 kap. 19 § fjärde stycket RB och 4 och 5 §§ lagen om hemlig dataavläsning). I avsnitt 9.10.3 kommer vi dessutom fram till att det är nödvändigt med en möjlighet att i vissa fall kunna använda hemlig avlyssning av elektronisk kommunikation

eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas. Något sådant kan knappast komma i fråga om brottet inte bedöms vara på den nivån att hemlig avlyssning av elektronisk kommunikation i allmänhet kan förekomma.

Som vi kommer att utveckla närmare i avsnitt 7.5 och 9.10.3 kan det i vissa fall handla om systemhotande verksamhet. Det är typiskt sett av stort intresse att – även när det saknas en skäligen misstänkt – kunna ta del av uppgifter om meddelanden som överförs eller har överförts (jfr prop. 2002/03:74 s. 35 och 36). Det är i många fall även av avgörande betydelse att man kan del av innehållet i kommunikationen. Grovt dataintrång bör med hänsyn till det anförda läggas till i brottskatalogen i 27 kap. 18 § RB.

För att de nödvändiga förbättringarna att utreda brotten ska uppnås krävs det vidare att hemlig övervakning av elektronisk kommunikation som avser inhämtning av meddelanden samt motsvarande hemlig dataavläsning ska kunna ske i realtid. Vi återkommer till denna fråga i avsnitt 7.5.

Sexuella övergrepp mot barn och barnpornografi

När det gäller internetrelaterad sexualbrottslighet mot barn och internetrelaterade barnpornografibrott finns i allmänhet samma utredningssvårigheter som när det gäller annan komplex it-brottslighet. Dessa utvecklas vidare i avsnitt 7.5 och 9.10.3. Som anges där är det vanligt att dessa ärenden inleds genom att övergreppsmaterial påträffas. Hur brottsmisstanken initialt rubriceras kan bero på ett antal olika omständigheter. Om det finns omständigheter som talar för att den som exempelvis delat övergreppsmaterialet själv är den som förgripit sig på barnet kan misstanken redan från början komma att gälla t.ex. våldtäkt mot barn, sexuellt utnyttjande av barn eller sexuellt övergrepp mot barn. I annat fall kan misstanken gälla barnpornografibrott eller, om det finns något som pekar på att den som delat materialet själv främjat eller utnyttjat att barnet utfört eller medverkat i en sexuell posering, utnyttjande av barn för sexuell posering. Oavsett den initiala rubriceringen kan det många gånger vara så att en möjlighet att identifiera den som t.ex. delat ett övergreppsmaterial

online, kan bidra till att öppna upp hela ärendet, som inte sällan visar sig vara omfattande och röra ett flertal offer.

Med hänsyn till det anförda, och det som sägs i avsnitt 7.5 och 9.10.3, finns det mycket starka behovsskäl som talar för att sexualbrott mot barn läggs till i de nu aktuella brottskatalogerna. Skälen gäller även i fråga om barnpornografibrott av normalgraden och sådana sexualbrott mot barn som, sett till straffskalan, är av mindre allvarligt slag. Mot en sådan lösning kan anföras att straffskalan för vissa av de aktuella brotten är relativt lindrig, och i vissa fall omfattar böter. Det bör dock framhållas att redan den nuvarande brottskatalogen för hemlig avlyssning av elektronisk kommunikation innehåller brott med en motsvarande straffskala, om än med ett annat skyddsintresse. Sexuella övergrepp mot barn är brottslighet av ett slag som framstår som särskilt avskyvärd och angelägen att kraftfullt bekämpa. Det handlar om en viktig aspekt av skyddet för den personliga integriteten. Barnpornografibrott rör i många fall dokumenterade sexuella övergrepp mot barn. Det är känt att den omständigheten att övergreppet dokumenterats medför ett ytterligare trauma för barnet.[10] Vidare talar mycket för att det finns ett samband mellan konsumtion av övergreppsmaterial och egna övergrepp.[11] Utan en möjlighet att använda hemliga tvångsmedel för att utreda barnpornografibrottet kommer man ofta inte vidare i brottsutredningen, och man mister möjligheten att i bästa fall stoppa ytterligare övergrepp mot barn. Efterfrågan på övergreppsmaterial bidrar i sig till övergrepp på barn.

Skyddet av barn, både utanför och på nätet, är en av EU:s prioriteringar. Sexuella övergrepp mot barn och sexuell exploatering av barn utgör allvarliga kränkningar av de mänskliga och grundläggande rättigheterna, i synnerhet barns rätt att skyddas från alla former av våld, övergrepp, vanvård, misshandel och utnyttjande, inbegripet sexuella övergrepp, i enlighet med barnkonventionen och EU:s rättighetsstadga. Denna syn på sexuella övergrepp mot barn och övergreppsmaterial kommer bl.a. till uttryck i Europaparlamentets och rådets förordning (EU) 2021/1232 av den 14 juli 2021 om ett tillfälligt undantag från vissa bestämmelser i direktiv 2002/58/EG vad gäller användning

[10] Se bl.a. Ateret Gewirtz-Meydan, Wendy Walsh, Janis Wolak & David Finkelhor, The complex experience of child pornography survivors. Child Abuse Negl. 2018 Jun;80:238-248. doi: 10.1016/j.chiabu.2018.03.031. Epub 2018 Apr 7. PMID: 29631255.
[11] Se bl.a. Michael C Seto, R. Karl Karl Hanson & Kelly M Babchishin, Contact Sexual Offending by Men With Online Sexual Offenses, artikel i Sexual Abuse A Journal of Research and Treatment, december 2010, DOI: 10.1177/1079063210369013 och NetCleanrapporten 2017.

av teknik hos tillhandahållare av nummeroberoende interpersonella kommunikationstjänster för behandling av personuppgifter och andra uppgifter i syfte att bekämpa sexuella övergrepp mot barn på nätet. Bristande förmåga att utreda sexualbrott mot barn kan också utgöra en kränkning av barnets rättigheter enligt artikel 8 i Europakonventionen (jfr K.U. mot Finland).

Vid en samlad bedömning anser vi att de utomordentligt starka behovsskälen och vikten av att barn skyddas mot sexuella övergrepp gör det proportionerligt att i de nu aktuella brottskatalogerna lägga till alla de sexualbrott mot barn som inte redan på grund av sin straffskala kan föranleda hemlig avlyssning av elektronisk kommunikation. Samma bedömning görs i fråga om barnpornografibrott som inte är ringa och grovt barnpornografibrott.

Ringa brott bör undantas

Straffskalan för ringa övergrepp i rättssak börjar med böter och slutar med fängelse i högst sex månader. Samma straffskala gäller för ringa utpressning och ringa mened. Med hänsyn till straffskalorna anser vi det inte proportionerligt med en möjlighet att använda hemliga tvångsmedel. De ringa varianterna av de angivna brotten bör därför uttryckligen undantas i brottskatalogernas uppräkningar. Som nämnts ovan bör även ringa barnpornografibrott undantas.

Försök, förberedelse och stämpling

Brottskatalogerna omfattar inte bara fullbordade brott utan även försök, förberedelse och stämpling till de uppräknade brotten, om en sådan gärning är belagd med straff. Samma sak gäller enligt de nuvarande straffvärdeventilerna, förutsatt att kravet i fråga om straffvärde är uppfyllt och gärningen är straffbelagd (jfr prop. 2002/03:74 s. 35 och 48). Något skäl till en avvikande bedömning när det gäller de brott som vi föreslår ska läggas till i brottskatalogerna har inte framkommit. Hemliga tvångsmedel bör alltså kunna användas inte bara vid förundersökningar om fullbordat brott utan även vid förundersökningar om försök, förberedelse och stämpling, om en sådan gärning är straffbelagd.

Följdändringar

Bedömningarna i det föregående medför att barnpornografibrott bör tas bort från brottskatalogen i 27 kap. 19 § tredje stycket 3 RB.

7.5 Inhämtningen av uppgifter om meddelanden bör inte begränsas till förfluten tid

Förslag: Det ska vara tillåtet att hämta in uppgifter om meddelanden i realtid vid hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet. Motsvarande ändring ska göras i lagen om hemlig dataavläsning.

Skälen för förslaget

När hemlig övervakning av elektronisk kommunikation används i syfte att utreda vem som kan misstänkas gäller enligt 27 kap. 20 § andra stycket RB att övervakning som innebär att uppgifter hämtas in om meddelanden endast får avse förfluten tid. Någon närmare motivering till denna begränsning finns inte i den proposition som ledde till införandet av bestämmelsen (jfr prop. 2011/12:55 s. 72) och inte heller i Polismetodutredningens förslag, som i huvudsak låg till grund för propositionsförslaget (jfr SOU 2009:1 s. 113–116). I propositionen anges endast att ingen remissinstans hade invänt mot utredningens bedömning, att förslaget motsvarade den inhämtning som enligt dåvarande ordning skedde enligt lagen om elektronisk kommunikation och att regeringen i denna del inte gjorde någon annan bedömning än utredningen.

Motsvarande begränsning gäller vid hemlig dataavläsning enligt 5 § lagen om hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet. Skälen för begränsningen kommenteras inte närmare i förarbetena (jfr prop. 2019/20:64 s. 124 och 125 och SOU 2017:89 s. 259 och 260).

De brottsbekämpande myndigheterna har anfört att det numera finns ett påtagligt behov av en möjlighet att inhämta uppgift om meddelanden i realtid i syfte att utreda vem som skäligen kan misstänkas för brottet. Även om frågan inte uttryckligen omfattas av våra

direktiv har vi valt att ta upp den eftersom vi bedömer att den är viktig och har ett tydligt samband med de frågor vi har att utreda.

Enligt de brottsbekämpande myndigheterna finns behovet av uppgifter om meddelanden i realtid i synnerhet i fråga om komplexa cyberbrott. Det finns vid it-brottsutredningar mycket sällan en misstänkt person att utgå ifrån. Kännetecknande för brott av detta slag är att gärningspersonerna använder en komplex infrastruktur i flera lager. Detta gör det avsevärt svårare att blottlägga infrastrukturen och därmed hitta gärningspersonerna bakom. I normalfallet startar utredningen med att man har identifierat någon del av en infrastruktur som gärningspersonerna har använt vid brottet, såsom en server eller en dator. Dock omfattas dessa i stort sett alltid av kryptering och anonymisering vilket inte sällan gör dessa enheter väldigt svåra att komma in i. Det enda sättet att då nå framåt och om möjligt identifiera nästa steg i attackkedjan eller en gärningsperson är via hemliga tvångsmedel, som hemlig övervakning av elektronisk kommunikation i realtid, hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning. Inhämtning av material från hemlig övervakning i förfluten tid ger sällan något av värde, eftersom datatrafik i stort sett aldrig sparas och enligt uppgift från Polismyndigheten inte heller skulle ge den information som myndigheterna är i behov av för att komma framåt. Enligt uppgift från Polismyndigheten är erfarenheten både från Sverige och andra länder att det ofta är en förutsättning för att man ska kunna komma vidare i utredningen att det kan ske en hemlig övervakning av elektronisk kommunikation i realtid eller en hemlig avlyssning av elektronisk kommunikation. Eftersom det i normalfallet saknas en skäligen misstänkt, är det emellertid enligt svensk rätt inte möjligt med en hemlig avlyssning eller en hemlig övervakning i realtid.

Som ett exempel på den ovanstående problematiken har Polismyndigheten tagit upp attacker med s.k. ransomware, som även kallas gisslanprogram eller utpressningstrojan. Ransomware är en form av skadlig kod som gärningsmännen placerar i offrets informationssystem (t.ex. en dator eller server) och som krypterar och låser informationssystemet och filerna i informationssystemet i syfte att gärningspersonerna ska kunna begära en lösensumma. Gärningen innefattar normalt ett dataintrång och en utpressning. Mycket talar för att gärningarna ofta skulle bedömas som grova, men eftersom det helt saknas praxis är det osäkert hur domstolarnas bedömning skulle utfalla

i rubriceringsfrågan. Ransomwareattacker och annan cyberbrottslighet är gränslös, och det är vanligt förekommande att gärningspersonerna är utspridda i olika länder och samverkar genom lager av servrar som kommunicerar med varandra. Detta gör att det är mycket komplext för rättsväsendet att jobba sig bakåt. Enligt Polismyndigheten finns det oftast inga andra uppslag för att komma vidare i utredningen än de noder i en infrastruktur som gärningspersonerna har agerat ifrån. För att man ska ha en möjlighet att utreda vilka dessa personer är, finns ofta ingen annan möjlighet än en framåtsyftande hemlig övervakning av elektronisk kommunikation, eller en hemlig avlyssning av elektronisk kommunikation. Avsaknaden av möjligheter att använda dessa tvångsmedel när det saknas en skäligen misstänkt gör enligt specialister vid Polismyndigheten att möjligheterna att komma vidare i komplexa cyberbrottsutredningar är små och att svenska myndigheter inte heller kan biträda andra länder med utredningar om allvarlig cyberbrottslighet (se vidare i kapitel 9 angående hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter). Risken är att detta gör det attraktivt för kriminella som ägnar sig åt allvarlig cyberbrottslighet att placera infrastruktur i Sverige i vetskap om att risken att bli avslöjad är liten. Det finns exempel på allvarliga ransomwareattacker i andra länder där spåren har lett till Sverige.[12] Hittills har ingen svensk utredning om ransomware lett till åtal, utan man har i stället förmedlat den insamlade informationen till andra länder varefter den svenska utredningen lagts ner.

Runt om i världen pågår stora satsningar inom just ransomwareområdet. I USA har man exempelvis lagt hotbilden av ransomware på samma nivå som terror och klassat det som brott mot rikets säkerhet. Brotten kan ha en stor samhällspåverkan. Inom flera länder i Europa startas så kallade ”ransomware task-force” för att komma till bukt med denna allvarliga problematik och flera länder omorganiserar sin verksamhet för att på ett effektivare sätt kunna agera. Diskus-

[12] I ett aktuellt exempel blev den irländska sjukvården drabbat av ransomware, vilket slog ut stora delar av dess verksamhet. Man kunde under flertalet dagar inte komma åt några patientjournaler, man blev tvungen att ställa in samtliga operationer utom de som var akuta och samtliga läkarbesök fick ställas in under denna period. Två månader efter händelsen hade man fortfarande inte lyckats återgå till full verksamhet. I den irländska utredningen hittade man spår av de kriminella som ledde mot Sverige. Dessa spår pekade mot att de kriminella använt en server belägen i Sverige för att genomföra sin attack. En begäran om rättslig hjälp skickades därför till Sverige med önskan om att avlyssna denna server för att kunna följa trafiken och förhoppningsvis därmed kunna identifiera gärningspersonerna. Åklagaren gick upp i rätten med detta önskemål men fick avslag med anledning av att skäligen misstänkt saknades i ärendet.

sioner pågår även mellan flera myndigheter om utökade samarbeten kring detta i Sverige. Det handlar alltså om en högaktuell och potentiellt systemhotande brottslighet med en betydande internationell dimension. Det framstår som synnerligen angeläget att brottsligheten kan bekämpas. Detta talar starkt för att det bör vara möjligt att använda hemlig övervakning av elektronisk kommunikation i realtid i syfte att utreda vem som skäligen kan misstänkas för brottet.

Ett annat exempel som de brottsbekämpande myndigheterna tagit upp är internetrelaterade sexuella övergrepp mot barn, inklusive barnpornografibrott. En stor del av kommunikationen (text och fildelning) vid dessa brott sker via olika Darknetforum eller krypterade appar. Initialt uppstår typiskt sett misstanke om brott när en bild- eller videofil föreställande sexuella övergrepp mot barn påträffas och målsäganden på bilden är okänd. Filen kan ha skickats från ett alias till ett annat alias via ett Darknetforum. Vem som döljer sig bakom respektive alias är okänt. Utredningen går i praktiken till på det sättet att utredare samlar in all tillgänglig information avseende det alias som skickat filen. Denna kontroll innefattar bl.a. en avstämning med Europol. Informationsinsamlingen kan leda till att man identifierar ett fåtal intressanta personer runt om i Sverige. Ingen av dessa kan dock i detta skede anses som skäligen misstänkt för brottet. För att komma framåt i utredningen och närmare en identifiering av rätt gärningsperson och även höja misstankegraden är det enligt de brottsbekämpande myndigheterna av mycket stor vikt att de får en möjlighet att utföra en hemlig övervakning av elektronisk kommunikation i realtid. Med hjälp av det tvångsmedlet tillsammans med andra åtgärder kan personer uteslutas och ytterligare bevisning mot rätt gärningsperson erhållas. De brottsbekämpande myndigheterna har anfört att en möjlighet till hemlig övervakning i realtid skulle vara ett mycket effektivt verktyg för att man ska kunna identifiera såväl målsäganden som den misstänkte. Enligt myndigheterna är det i åtskilliga fall den enda framkomliga vägen till att avbryta pågående övergrepp mot den okända målsäganden och kunna lagföra den misstänkte. Även barnpornografibrott är synnerligen angelägna att kunna bekämpa, inte minst eftersom det i många fall är fråga om pågående dokumenterade övergrepp mot barn i Sverige eller andra länder.

När det gäller brott av det anförda slaget utgör den nuvarande regleringen ett hinder i den brottsbekämpande verksamheten dels genom att hemlig övervakning av elektronisk kommunikation i real-

tid endast är möjlig om det finns en skäligen misstänkt – vilket det alltså sällan gör – dels genom att hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas sällan är tillåten. Straffet för barnpornografibrott av normalgraden är fängelse i högst två år, och för grovt brott fängelse i lägst ett och högst sex år. Straffet för dataintrång är böter eller fängelse i högst två år och för grovt brott fängelse i lägst sex månader och högst sex år. Detta innebär att hemlig övervakning av elektronisk kommunikation är möjlig endast om det finns förutsättningar att med tillämpning av straffvärdeventilen utföra hemlig avlyssning av elektronisk kommunikation (jfr 27 kap. 19 § fjärde stycket RB). Vi har i avsnitt 7.4 lämnat förslag som gör det möjligt att använda hemlig avlyssning av elektronisk kommunikation och därmed även hemlig övervakning av elektronisk kommunikation i det nu aktuella syftet.

Med hänsyn till det som de brottsbekämpande myndigheterna anfört bedömer vi att det finns ett påtagligt behov av en möjlighet att kunna inhämta uppgifter om meddelanden i realtid i syfte att utreda vem som skäligen kan misstänkas för brottet.

Förhållandet till den personliga integriteten

En möjlighet till inhämtning i realtid innebär utökade möjligheter att kartlägga den enskildes förhållanden, särskilt om man även hämtar in lokaliseringsuppgifter i realtid (jfr EU-domstolens dom den 6 oktober 2020, i förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl, punkt 187). Ett slopande av begränsningen till meddelanden i förfluten tid skulle därför innebära ett större intrång i den personliga integriteten. Vidare följer det av EU-domstolens praxis att åtgärden på grund av dess ingripande natur inte kan komma i fråga annat än mot personer där det finns något giltigt skäl som talar för att de på ett eller annat sätt är inblandade i den aktuella brottsligheten (jfr det nyss nämnda rättsfallet, punkt 188 och 189). Vi bedömer att den svenska regleringen uppfyller detta krav. Det följer av kravet på synnerlig vikt för utredningen och de övriga principer som gäller vid tvångsmedelsanvändning att en hemlig övervakning inte ska göras mer omfattande än nödvändigt. Vi anser att behoven väger så tungt att integritetsintrånget är försvarligt. Begränsningen till uppgifter om meddelanden som överförts bör därför tas bort.

De anförda skälen gör sig gällande även beträffande hemlig dataavläsning. Begränsningen till historiska uppgifter bör därför tas bort.

7.6 Hemlig kameraövervakning

Bedömning: Möjligheten att använda hemlig kameraövervakning och hemlig dataavläsning som gäller kameraövervakningsuppgifter bör även i fortsättningen omfatta samma brott som hemlig avlyssning av elektronisk kommunikation.

Förslag: Det införs en möjlighet att använda hemlig kameraövervakning och hemlig dataavläsning som gäller kameraövervakningsuppgifter vid förundersökningar om grovt dataintrång, sexuellt utnyttjande av barn, sexuellt övergrepp mot barn, grovt sexuellt övergrepp mot barn, utnyttjande av barn för sexuell posering, grovt utnyttjande av barn för sexuell posering, utnyttjande av barn genom köp av sexuell handling, sexuellt ofredande som gäller barn, kontakt för att träffa ett barn i sexuellt syfte, utpressning som inte är att anse som ringa, grov utpressning, mened som inte är att anse som ringa, övergrepp i rättssak som inte är att anse som ringa, barnpornografibrott som inte är ringa och grovt barnpornografibrott, grovt jaktbrott och grovt insiderbrott.

Skälen för förslaget och bedömningen

Regleringen om hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning hänger ihop på det sättet att tvångsmedlen kan användas vid samma slags brott. Förhållandet kan ses som ett uttryck för att tvångsmedlen anses jämförbara från integritetssynpunkt. Det ingår inte uttryckligen i vårt uppdrag att se över brottskatalogen avseende hemlig kameraövervakning. Samtidigt talar starka skäl för att man upprätthåller den rådande systematiken, dvs. överensstämmelsen när det gäller den brottslighet som kan utredas med hjälp av respektive tvångsmedel. Samma sak kan, som framgått av resonemangen i avsnitt 7.4, anföras i fråga om hemlig dataavläsning som gäller kameraövervakningsuppgifter. Även intresset av att inte i onödan komplicera en redan svårgenomtränglig lagstiftning talar för detta.

Det är inte givet att behovet av hemlig kameraövervakning och kameraövervakningsuppgifter är lika stort när det gäller alla de brott som vi i föregående avsnitt har föreslagit ska läggas till i brottskatalogerna. Detsamma kan dock anföras i fråga om många av de brott som omfattas av den gällande regleringen. Att hemlig kameraövervakning eller hemlig dataavläsning avseende kameraövervakningsuppgifter kan ha ett stort värde i exempelvis en utredning om grovt jaktbrott är dock uppenbart. Detta gäller särskilt med tanke på möjligheten att vid kameraövervakning använda kameror som fästs på drönare (se vidare i kapitel 10). Sammantaget gör vi bedömningen att skälen för att bibehålla överensstämmelsen mellan bestämmelserna påtagligt överväger.

8 Hemlig övervakning av elektronisk kommunikation avseende målsäganden

8.1 Uppdraget

Hemlig övervakning av elektronisk kommunikation får användas i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen (27 kap. 20 § andra stycket rättegångsbalken, förkortad RB). Lagtexten innehåller inga begränsningar i fråga om vem tvångsmedlet får riktas mot och det förekommer att hemlig övervakning av elektronisk kommunikation riktas mot en målsägande. Säkerhets- och integritetsskyddsnämnden har ifrågasatt om det är rimligt att brottsbekämpande myndigheters intresse av övervakningsuppgifter tillåts urholka målsägandens integritetsskydd på detta sätt utan uttryckligt lagstöd (dnr 132-2018). Vi har mot denna bakgrund fått i uppdrag att

- ta ställning till om det bör vara tillåtet med hemlig övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet, och i så fall i vilka situationer detta bör vara tillåtet, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Samma slags uppgifter som kan hämtas in genom hemlig övervakning av elektronisk kommunikation kan erhållas genom hemlig dataavläsning enligt lagen (2020:62) om hemlig dataavläsning. Genom hemlig dataavläsning kan man nämligen i ett avläsningsbart informationssystem läsa av eller ta upp uppgifter om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller någon annan adress (kommunikationsöver-

vakningsuppgifter) och uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits (platsuppgifter). Det finns inte i lagtexten någon begränsning i fråga om vem som åtgärden får riktas mot. Vi bedömer att det, för att regelverket ska ha en välfungerande systematik, är nödvändigt att även överväga om det bör vara möjligt att använda hemlig dataavläsning mot målsäganden avseende kommunikationsövervakningsuppgifter eller platsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet.

8.2 Bakgrund

Bakgrunden till uppdraget i denna del är att Säkerhets- och integritetsskyddsnämnden ifrågasatt om det är rimligt att hemlig övervakning av elektronisk kommunikation utan tydligt lagstöd används mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet (uttalande med beslut 2019-09-11 dnr 132-2018). Nämnden hade uppmärksammat att åklagare i två ärenden hade ansökt om och beviljat tillstånd till hemlig övervakning enligt 27 kap. 19 § första stycket 1 och 3 RB avseende olika telefonnummer som tillhörde målsäganden. Uppgifter fick alltså hämtas in om meddelanden som överförs eller hade överförts till telefonnumret och i vilket geografiskt område kommunikationsutrustningen fanns eller hade funnits. Ansökningarna hade gjorts med stöd av 27 kap. 20 § andra stycket RB, dvs. för att utreda vem som skäligen kan misstänkas för brottet. Det var i båda fallen fråga om allvarliga brott, nämligen synnerligen grov misshandel i det ena fallet och människorov i det andra. I utredningen om synnerligen grov misshandel var det känt att målsäganden tidigare varit i konflikt med personer som tillhörde kriminella grupperingar. Åklagaren gjorde bedömningen att det fanns anledning att tro att målsäganden, trots att han uppgett motsatsen, visste vilka gärningsmännen var och att han hade haft kontakt med dem i anslutning till brottet. Det ansågs därför vara av synnerlig vikt för utredningen att få reda på vilka kontakter som förekommit för att kunna identifiera skäligen misstänkta personer. I utredningen om människorov var teorin att en eller flera misstänkta hade varit i kontakt med målsäganden före gärningen, något som fick visst stöd av bl.a. vittnesuppgifter.

Säkerhets- och integritetsskyddsnämnden anförde följande.

Tillgången till enskildas elektroniska kommunikation utgör ett allvarligt ingrepp i den personliga integriteten. Rätten att utan obehörigt intrång kommunicera på visst sätt och skyddet i övrigt mot intrång som innebär övervakning och kartläggning i hemlighet av den enskildes personliga förhållanden ingår bland de grundlagsskyddade fri- och rättigheter som bara kan begränsas genom lag (2 kap. regeringsformen). Användningen av hemliga tvångsmedel ska alltid följa den s.k. legalitetsprincipen vilken innebär att en myndighet inte utan stöd i lag eller annan författning får ingripa i en enskilds rättsfär. Vid tillämpningen av bestämmelser om hemliga tvångsmedel finns det inte utrymme för extensiva eller analoga tolkningar som urholkar skyddet för enskilda.

– – –

Nämnden har på senare tid noterat att hemlig övervakning används mot målsäganden vid viss typ av brottslighet i syfte att hitta en skäligen misstänkt. Bestämmelsen i 27 kap. 20 § andra stycket RB innehåller enligt ordalydelsen inte någon begränsning när det gäller mot vem tvångsmedlet får riktas. Någon motsvarighet till det krav som finns i första stycket, på att den adress som övervakas måste ha viss koppling till en misstänkt person, är mot bakgrund av syftet med bestämmelsen inte möjlig. Det finns dock enligt nämnden anledning att utifrån ett övergripande integritetsperspektiv invända mot sådan tvångsmedelsanvändning.

En målsägande kan inte tvingas att medverka i en brottsutredning. Han eller hon är visserligen skyldig att låta sig förhöras under förundersökningen men kan inte tvingas att lämna uppgifter under ed. En målsägande är inte heller skyldig att låta sig kroppsbesiktigas. Det gäller även om det skulle medföra att för utredningen avgörande bevisning om ett mycket allvarligt brott, t.ex. en grov våldtäkt, inte kan säkras. I en brottsutredning har målsäganden alltså ett långtgående skydd mot att utsättas för tvångsåtgärder. Det är inte ovanligt vid vissa typer av brott att målsäganden inte vill medverka till att utredningen drivs framåt. Det gäller inte minst vid gängkriminalitet och annan organiserad brottslighet. När så är fallet saknas det i princip förutsättningar att tvinga målsäganden att bidra till utredningen.

Det råder inga tvivel om att uppgifter från hemlig övervakning riktad mot målsäganden i vissa situationer kan öka möjligheten att hitta en skäligen misstänkt. Att målsäganden inom ramen för utredningar om mycket allvarliga brott blir föremål för hemlig övervakning är emellertid enligt nämndens mening oroväckande. Även om målsäganden rör sig i kriminella kretsar, eller av andra anledningar är av intresse för brottsutredande myndigheter, motiverar det knappast att han eller hon utan ett uttryckligt lagstöd i hemlighet utsätts för en så ingående kartläggning som hemlig övervakning kan innebära. I ett av de nu granskade fallen rörde det sig om övervakning under tre månader. Tillämpningen väcker frågan om det är rimligt att målsägandens integritetsskydd urholkas på det sättet.

Dagens reglering innebär att det vid vissa mycket allvarliga brott får användas hemlig övervakning för att hitta en skäligen misstänkt, även om det innebär att tvångsåtgärden riktas mot personer som man med säkerhet vet inte har begått brottet. Ett typiskt exempel är s.k. basstationstömning, som innebär att det samlas in uppgifter om alla som har befunnit sig i närheten av en brottsplats. En systematisk användning av hemlig övervakning riktad mot målsäganden kan emellertid knappast ha varit avsedd. Eftersom det är lagstiftarens uppgift att göra avvägningen mellan behovet och nyttan av tvångsmedlet och integritetsintresset överlämnar nämnden en kopia av detta uttalande till Justitiedepartementet.

8.3 Gällande rätt

8.3.1 Hemlig övervakning av elektronisk kommunikation

En översiktlig redogörelse för gällande rätt finns i kapitel 4. Förutsättningarna för att i en förundersökning använda hemlig övervakning av elektronisk kommunikation framgår av 27 kap. 19 och 20 §§ RB. En grundläggande tanke bakom regleringen om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation är att åtgärderna endast får avse den som är skäligen misstänkt för brott (se prop. 1994/95:227 s. 20). Det framgår dock inte av lagtexten vem åtgärden får riktas mot. Begränsningarna har i stället utformats så att de tar sikte på det telefonnummer eller den adress eller elektroniska kommunikationsutrustning som åtgärden avser. Av 20 § framgår att åtgärden enbart får riktas mot ett telefonnummer eller en adress eller elektronisk kommunikationsutrustning som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte (första stycket 1) eller annars kan antas ha använts eller komma att användas av den misstänkte, eller som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta (första stycket 2). Reglerna om koppling mellan den enskilde och en teknisk utrustning finns till för att skydda integriteten och rättssäkerheten och ska minska risken för att personer som är ovidkommande för utredningen drabbas av åtgärderna (se t.ex. prop. 1988/89:124 om vissa tvångsmedelsfrågor, s. 46). Vid tvångsmedelsanvändning enligt andra punkten anses tvångsmedlet rikta sig mot den misstänkte och inte mot innehavaren av telefonnumret (prop. 2002/03:74 s. 38 f.).

Det krävs alltså som utgångspunkt att ett telefonnummer eller annan adress eller en kommunikationsutrustning kan knytas till en skäligen misstänkt för att en brottsbekämpande myndighet ska erhålla tillstånd till övervakning. Därutöver får dock hemlig övervakning av elektronisk kommunikation ske i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. Då kan det av naturliga skäl inte ställas något krav på en viss koppling mellan den adress eller utrustning som övervakas och någon misstänkt. I det fallet får övervakningen endast innebära att man hämtar in uppgifter om meddelanden från förfluten tid och lokaliseringsuppgifter. Det är alltså inte möjligt att övervaka meddelanden i realtid i dessa fall. Däremot är det möjligt att i realtid hämta in lokaliseringsuppgifter. I dessa fall gäller vidare begränsningen att övervakning endast får ske vid en förundersökning som avser brott som kan leda till hemlig avlyssning av elektronisk kommunikation. Det ställs alltså högre krav i fråga om brottets allvar än vad som gäller för hemlig övervakning av elektronisk kommunikation i allmänhet.

Att syftet med övervakningen ska vara att utreda vem som skäligen kan misstänkas för brottet utesluter inte att åtgärden primärt kan ta sikte på att utröna var t.ex. en brottsplats är belägen, om den upplysningen är av avgörande betydelse för att utreda vem som skäligen kan misstänkas för brottet. Om det finns en skäligen misstänkt person kan inhämtning ske i syfte att identifiera ytterligare personer som skäligen kan misstänkas för brott.

I förarbetena (prop. 2011/12:55 s. 130) anges det att åklagare och domstol vid tillämpning av andra stycket bör begränsa tillståndet så att mängden överskottsinformation minimeras. Övervakningsuppgifter som avser de mobiltelefoner som används eller har använts i anslutning till ett visst brott bör normalt avgränsas till ett geografiskt område som motsvarar brottsplatsen och området däromkring. Bestämmelsen ger även utrymme för att inhämta uppgifter inom områden som polisen befarar att gärningsmannen har använt som flyktväg från brottsplatsen. Vid misstanke om brott som kan pågå en längre tid och där gärningsmannen kan tänkas förflytta sig, t.ex. vid människokorov (4 kap. 1 § brottsbalken), kan övervakningsuppgifter behöva inhämtas avseende mer vidsträckta områden.

8.3.2 Hemlig dataavläsning

Hemlig dataavläsning får som huvudregel endast avse ett avläsningsbart informationssystem som används eller som det finns särskild anledning att anta har använts eller kommer att användas av någon som är skäligen misstänkt för brottet (4 § andra stycket lagen om hemlig dataavläsning). Ett tillstånd som avser kommunikationsavlyssningsuppgifter, kommunikationsövervaknings- eller platsuppgifter får dock även avse ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att den misstänkte under tid som tillståndet av ser har kontaktat eller kommer att kontakta (tredje stycket i samma paragraf). Regeringen uttalade i propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 122 och 123) att ett krav på en koppling mellan den misstänkte och det informationssystem som det ska vidtas åtgärder i utgör ett viktigt skydd för den personliga integriteten, framför allt för andra personer än den misstänkte.

Ett tillstånd till hemlig dataavläsning som avser kommunikationsövervaknings- och platsuppgifter får under vissa förutsättningar beviljas även för att utreda vem som skäligen kan misstänkas för brottet (5 § första stycket). Avläsning eller upptagning av kommunikationsövervakningsuppgifter får då, i likhet med hemlig övervakning av elektronisk kommunikation i motsvarande fall, endast avse förfluten tid. Vidare begränsas möjligheten av att den hemliga dataavläsningen endast får avse ett informationssystem som har använts vid ett brott eller i anslutning till en brottsplats vid brottstidpunkten eller som av någon annan anledning är av synnerlig vikt för utredningen (andra stycket i samma paragraf). Av förarbetena framgår följande om innebörden av dessa krav (prop. 2019/20:64 s. 219). Att det avläsningsbara informationssystemet har använts vid ett brott innebär att det haft avgörande betydelse vid själva genomförandet av brottet eller använts för att understödja brottet. Om polisen inom ramen för en förundersökning om t.ex. grovt narkotikabrott upptäcker en viss ipadress varifrån det har förmedlats stora mängder narkotika kan tillstånd till hemlig dataavläsning beviljas för att utreda vem som är skäligen misstänkt för brottet. Att informationssystemet använts i anslutning till en brottsplats vid brottstidpunkten innebär typiskt sett att det har använts på eller vid en brottsplats när ett brott har begåtts. Det finns dock ingen avgränsning för hur stort område kring brottsplatsen som åtgärden får vidtas inom. Detta måste bedömas från fall

till fall. Att informationssystemet på annat sätt är av synnerlig vikt för utredningen omfattar de fall när det inte står klart att informationssystemet funnits vid eller i närheten av brottsplatsen, men ändå kan ha en avgörande betydelse i utredningen. Ett exempel kan vara att ett informationssystem funnits längs en flyktväg från brottsplatsen eller när det finns skäl att tro att gärningspersonen kan tänkas förflytta sig medan brottet fortfarande pågår, t.ex. vid människorov eller grov narkotikasmuggling.

Som nämnts i tidigare kapitel gäller vidare att hemlig dataavläsning endast får användas för brott av det slag som kan föranleda hemlig avlyssning av elektronisk kommunikation (4 § första stycket). Hemlig övervakning av elektronisk kommunikation kan alltså användas för betydligt fler brott än hemlig dataavläsning. Denna skillnad finns dock inte när det gäller hemlig övervakning av elektronisk kommunikation som sker i syfte att utreda vem som skäligen kan misstänkas för brottet, eftersom hemlig övervakning i det fallet förutsätter att brottet är sådant att det är tillåtet med hemlig avlyssning av elektronisk kommunikation.

8.3.3 Om tvångsåtgärder mot andra än den misstänkte

Målsäganden

I princip alla brott faller under allmänt åtal (20 kap. 3 § RB). I allmänhet krävs inte målsägandens medverkan för att åtal ska få väckas, men det finns ett antal brott där det krävs angivelse av målsäganden. Det förekommer även att det antingen krävs angivelse till åtal av målsäganden eller att åtalet är påkallat ur allmän synpunkt. Exempel på sådana brott är vållande till kroppsskada som inte är grov (3 kap. 12 § brottsbalken, förkortad BrB) och hemfridsbrott (4 kap. 11 § BrB). När det gäller den typ av allvarliga brott där hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet förekommer, ställs dock inte något sådant krav. Något formellt krav på att målsäganden anger brottet till åtal eller medverkar i utredningen ställs alltså inte när det gäller detta slags brott. Däremot kan det givetvis i praktiken vara en förutsättning för att brottet ska komma till myndigheternas kännedom och att utredningen ska komma framåt.

Det kan fordras av en målsägande att han eller hon ska bidra till utredningen så gott det går (se Peter Fitger m.fl. Rättegångsbalken [2021-12-10 JUNO], kommentaren till 37 kap. 1 § RB). Emellertid finns det inget tvångsmedel för att tvinga fram en målsägandeutsaga. En målsägande kan alltså alltid välja att inte uttala sig eller svara på frågor (se Peter Fitger m.fl. Rättegångsbalken [2021-12-10 JUNO], kommentaren till 37 kap. 1 § RB). Målsäganden kan inte heller avlägga ed. Som grund för detta angav Processlagberedningen (se NJA II 1943 s. 492) att de lämnade uppgifterna annars skulle komma att tillmätas ett alltför stort bevisvärde och den tilltalades ställning genom detta obehörigen försvagas. En målsägande kan dock inte hindra att det som han eller hon tidigare berättat används som bevis i rättegången. Om en huvudförhandling hålls trots att målsäganden inte är närvarande, ska rätten i den utsträckning det behövs se till att det som han eller hon tidigare har anfört läggs fram ur handlingarna (46 kap. 6 § RB). Om målsäganden inställer sig men vägrar att svara på frågor eller svaren avviker från vad målsäganden tidigare berättat kan rätten med stöd av 36 kap. 16 § andra stycket jämförd med 37 kap. 3 § RB tillåta att det som målsäganden tidigare berättat för åklagare eller polis läggs fram vid huvudförhandlingen. Med hänsyn till de krav till skydd för den misstänkte som följer av artikel 6 i Europakonventionen finns det dock begränsningar när det gäller möjligheten att lägga en sådan utsaga till grund för en fällande dom (jfr bl.a. hovrättsavgörandet RH 2002:65).

Det finns ett visst utrymme för att använda tvångsåtgärder mot målsäganden. Målsäganden kan t.ex. kallas vid vite att inställa sig till förhör under förundersökningen eller till huvudförhandlingen, och även polishämtning kan förekomma (23 kap. 6 a och 7 §§ respektive 45 kap. 15 § första stycket och 46 kap. 14 § RB). För att rätten ska besluta om hämtning till huvudförhandlingen måste åtgärden bedömas som proportionerlig med hänsyn till bl.a. målsägandens person, vad målet gäller och omständigheterna i övrigt (se Peter Fitger m.fl. Rättegångsbalken [2021-12-10 JUNO], kommentaren till 46 kap. 14 § RB). Målsäganden är vidare skyldig att stanna kvar under en viss tid för förhör under förundersökningen (23 kap. 9 § RB) och är dessutom skyldig att under vissa förutsättningar tillfälligt lämna ifrån sig elektronisk kommunikationsutrustning som han eller hon bär med sig eller har på sig. Om han eller hon vägrar, får en polisman tillfälligt omhänderta utrustningen. Skulle det finnas synnerlig anledning att

anta att utredningen annars kommer att försvåras och det är föreskrivet fängelse för brottet är det tillåtet att kroppsvisitera även en målsägande för att söka efter kommunikationsutrustningen.

Även vissa andra straffprocessuella tvångsmedel kan användas mot målsäganden. Inget hindrar exempelvis att ett beslag görs hos målsäganden, om föremålet eller i handlingen i fråga kan antas ha betydelse för utredning om brottet (27 kap. 1 § RB). Dock torde det ha betydelse vid bedömningen av om åtgärden är proportionerlig att den som utsätts för beslaget är den person som också utsatts för det brott som ska utredas. Av rättssäkerhetsskäl fattas det normalt ett beslut om beslag även i de fall då målsäganden frivilligt lämnat över egendom till polisen.

Det är vidare möjligt att göra en husrannsakan hos andra personer än den som är skäligen misstänkt för brottet (28 kap. 1 § andra stycket RB). I det fallet ställs dock strängare krav för att åtgärden ska få vidtas än om husrannsakan görs hos den skäligen misstänkte. Även här torde det ha betydelse för proportionalitetsbedömningen om åtgärden ska vidtas hos målsäganden.

Av det sagda följer att det – om det finns grund för åtgärden och åtgärden är proportionerlig – är möjligt att göra en husrannsakan hos målsäganden och att ta mobiltelefoner och andra elektroniska informationsbärare i beslag och gå igenom deras innehåll. Genom en sådan åtgärd kan man – förutsatt att uppgifterna finns sparade i informationsbäraren – få tillgång till många av de uppgifter som man även kan få fram genom en hemlig övervakning av elektronisk kommunikation som riktas mot exempelvis målsägandens telefonnummer. Exempel på sådana uppgifter är samtalslistor som visar vilka telefonnummer som varit i kontakt med målsägandens telefon och listor över mottagna sms. Därutöver kan man, om uppgifterna är sparade, få tillgång till en hel del uppgifter av den typ som man kan få tillgång till genom hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning, såsom innehållet i sms, MMS, e-post och snabbmeddelanden som skickats eller mottagits i olika chattfunktioner. Samtidigt är det en viktig skillnad att åtgärden i beslagsfallet inte sker i hemlighet, och att målsäganden har en möjlighet att överklaga beslaget.

Hemliga tvångsmedel som riktas mot den misstänkte, såsom exempelvis en hemlig avlyssning eller hemlig dataavläsning av den misstänktes telefon, eller en hemlig rumsavlyssning i en bostad som delas av den misstänkte och målsäganden, kan givetvis även drabba måls-

äganden på så sätt att kommunikation mellan den misstänkte och målsäganden avlyssnas eller avläses. Detta gäller även om målsäganden är en närstående till den misstänkte. En hemlig avlyssning eller hemlig övervakning kan göras av t.ex. ett telefonnummer som målsäganden innehar, om det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta numret (27 kap. 20 § första stycket 2 RB). I ett sådant fall anses åtgärden rikta sig mot den misstänkte, men målsäganden drabbas givetvis ändå. Enligt uppgift från de brottsbekämpande myndigheterna blir avlyssning som avser nummer som den misstänkte kontaktar allt vanligare. Skälet är att de misstänkta ofta byter telefonnummer, varför det kan vara svårt att rikta en avlyssning mot hans eller hennes telefon (se Ds 2020:12 Registrering av kontantkort, m.m., s. 60). Genom att avlyssna eller övervaka exempelvis en flickväns telefon kan man fånga upp relevanta uppgifter och i vissa fall få tillgång till den misstänktes aktuella telefonnummer så att detta kan avlyssnas.

Av framställningen i detta avsnitt framgår att det finns ett antal situationer där en målsägande kan utsättas för tvångsmedel. När det gäller undersökning av den egna kroppen är skyddet för målsäganden emellertid absolut. Målsägandens kropp kan alltså endast undersökas om han eller hon samtycker till åtgärden. Kroppsbesiktning får endast utföras på den som skäligen kan misstänkas för brottet (28 kap. 12 § RB) och en läkarundersökning i syfte att utfärda ett rättsintyg som avser en målsägande får aldrig utföras utan hans eller hennes samtycke (4 § lagen [2005:225] om rättsintyg). Som huvudregel kräver även utfärdandet av rättsintyget samtycke (5 § samma lag). Skälet till detta krav är främst att vetskapen om att läkaren kan komma att utfärda ett intyg annars skulle kunna avhålla en skadad målsägande från att söka vård (prop. 2004/05:64 s. 31).

Sammanfattningsvis kan man konstatera att en målsägande har ett starkt skydd i samband med utredning och rättsprocess, men att detta inte innebär något absolut hinder mot att vissa tvångsåtgärder kan vidtas mot målsäganden. Det hindrar inte heller att målsäganden drabbas av tvångsåtgärder som riktar sig mot den misstänkte.

Övriga

Tvångsåtgärder kan vidtas inte bara mot skäligen misstänkta personer och målsägande, utan även mot andra personer som är intressanta i utredningen. Ett exempel är personer som är misstänkta men inte skäligen misstänkta. Ett annat exempel är vittnen. Personer som ska höras under förundersökningen kan kallas till förhöret vid påföljd av vite och under vissa förutsättningar hämtas av polis till förhöret (23 kap. 6 a och 7 §§ RB). På tillsägelse av en polisman är den som befinner sig på den plats, där ett brott förövas, skyldig att medfölja till ett förhör som hålls omedelbart därefter (23 kap. 8 § RB). Vägrar personen utan giltig orsak, får polismannen ta med personen till förhöret. Vid vissa mycket allvarliga brott gäller detsamma för den som befinner sig inom ett område i anslutning till den plats där ett brott nyligen förövats. Det finns vidare en skyldighet för förhörspersoner att kvarstanna för förhör under viss tid (23 kap. 9 § RB). Vad som tidigare sagts om omhändertagande av elektronisk kommunikationsutrustning gäller även i fråga om de personkategorier som nu är aktuella. Även förutsättningarna för en husrannsakan är desamma. Här finns det dock skäl att uppmärksamma reglerna om beslagsförbud, som i sin tur anknyter till bl.a. reglerna om vittnesförbud.

Hemliga avlyssning eller övervakning av elektronisk kommunikation kan aktualiseras t.ex. på det sättet att det finns synnerlig anledning att anta att den misstänkte kommer att kontakta personens telefonnummer (27 kap. 20 § första stycket 2 RB). Vidare kan personer som befunnit sig i närheten av en brottsplats komma att omfattas av en basstationstömning (27 kap. 19 § första stycket 2 RB).

8.4 Tidigare överväganden

Buggningsutredningen

Tidigare gällde att de brottsutredande myndigheterna kunde hämta in uppgifter om telemeddelanden från operatörerna med stöd av 6 kap. 22 § första stycket 3 lagen (2003:389) om elektronisk kommunikation (LEK) och dess företrädare telelagen (1993:597). För sådan inhämtning krävdes det endast att brottet hade ett minimistraff på två år eller mer och att det ankom på myndigheten att utreda det. Något krav på att det skulle finnas en skäligen misstänkt

för brottet ställdes inte och bestämmelsen innehöll ingen begränsning i fråga om vems telemeddelanden den kunde avse. Regleringen kritiserades bl.a. mot bakgrund av vissa avgöranden från Europadomstolen. Buggningsutredningen föreslog att den dåvarande regleringen skulle upphävas och att inhämtning av uppgifter om telemeddelanden i stället skulle regleras i 27 kap. RB. Mot bakgrund av detta förslag ansåg utredningen att det i några situationer behövdes undantag från huvudregeln om kravet på brottsmisstanke mot viss person vid hemlig teleövervakning enligt rättegångsbalken.

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

Den första situationen som togs upp är när det i en brottsutredning saknas en skäligen misstänkt person men det finns uppgifter om att någon har ringt eller blivit uppringd i området kring en brottsplats. Som exempel nämndes fallet att ett vittne i samband med ett bankrån har sett en maskerad gärningsman ringa ett mobiltelefonsamtal. De myndigheter som utredningen tillfrågat hade framhållit att teleövervakningsuppgifter, som enligt då gällande rätt kunde inhämtas med stöd av telelagen (sedermera LEK), i ett sådant fall kan vara de enda konkreta uppgifter som utredningspersonalen har att gå efter då de söker en tänkbar gärningsman. Utredningen ansåg att möjligheten till sådan inhämtning dock borde vara begränsad till de teleadresser som använts i anslutning till den plats där brottet har begåtts och förklarade att det i praktiken skulle handla om att uppgifter hämtas in från den eller de basstationer som – vid tidpunkten för brottet – kunde antas har berörts av ett sådant mobiltelefonsamtal.

Den andra situation som Buggningsutredningen tog upp var den att inhämtning av uppgifter om målsägandens teleadress kan ge information som leder till att ett brott klaras upp (s. 404). Utredningen lyfte fram bl.a. mordutredningar där det saknas misstanke mot någon viss person och att det kan vara av avgörande betydelse för förundersökningen att man får reda på vem offret talat med i telefon den närmaste tiden före brottet för att därigenom kunna identifiera tänkbara gärningsmän. De brottsbekämpande myndigheterna hade till utredningen påtalat att ett krav på skälig misstanke mot viss person i dessa fall i praktiken skulle kunna förstöra möjligheterna att

utreda brottet. Buggningsutredningen ansåg följaktligen att inhämtning av uppgifter om målsägandens teleadress borde vara tillåten, men ansåg även att åtgärden som utgångspunkt borde förutsätta att målsäganden har lämnat sitt samtycke. Utredningen menade nämligen att det ur integritetssynpunkt skulle leda allt för långt att införa en regel som innebär att de brottsutredande myndigheterna mot målsägandens vilja kan hämta in uppgifter som rör hans eller hennes teleadresser. Dock ansåg utredningen att åtgärden, för att den skulle vara till praktisk nytta i det polisiära arbetet, borde vara tillåten även i de fall målsägandens samtycke inte kan inhämtas, t.ex. på grund av att målsäganden har avlidit genom brottet, är medvetslös eller försvunnen. Buggningsutredningen ansåg att det i sådana fall får anses ligga i sakens natur att målsäganden vill att brottet utreds och beivras.

Lagrådsremissen Hemlig avlyssning m.m.

I den lagrådsremiss som följde på Buggningsutredningens betänkande tog regeringen upp frågan om hemlig teleövervakning utan känd gärningsman och menade att hemlig teleövervakning borde tillåtas i vissa fall även om det inte finns någon som är skäligen misstänkt för ett begånget brott (s. 78 f.). Regeringen ansåg att undantag från huvudregeln vid fall motsvarande de av utredningen angivna exemplen framstod som angelägna ur såväl effektivitetssynpunkt som av hänsyn till brottsoffret. Regeringen konstaterade också att det i vissa brottsutredningar hade varit av största betydelse att uppgifter av detta slag hade kunnat hämtas in enligt telelagen. Regeringen framhöll att bedömningen inte avsåg situationer där målsäganden kan men inte vill samtycka till att uppgiften lämnas ut. Man tog alltså avstånd från en sådan möjlighet. Regeringen ansåg det möjligt att utforma en bestämmelse som är tillräckligt snäv för att vara acceptabel ur integritetssynpunkt, samtidigt som den medger utlämnande av de uppgifter som polisen kan behöva i de avsedda situationerna. Man föreslog därför att utredningens förslag skulle genomföras.

Lagrådet lämnade synpunkter enbart av lagteknisk karaktär på förslaget. Regeringen gick dock inte vidare med förslaget i propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering (prop. 2002/03:74) och förslaget ledde inte till lagstiftning. I propositionen uttalades att frågan om att avskaffa möjligheten för

brottsutredande myndigheter att inhämta uppgifter om telemeddelanden direkt från operatörerna skulle bli föremål för ytterligare överväganden (anförd prop. s. 12 och 40).

Beredningen för rättsväsendets utveckling

Mot bakgrund av ställningstagandena i prop. 2002/03:74 gav regeringen Beredningen för rättsväsendets utveckling (BRU) i uppdrag att bl.a. göra en översyn av de regelverk som styrde de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation (dir. 2003:15). Frågan om övervakning av elektronisk kommunikation utan en skäligen misstänkt behandlades i beredningens sjunde delbetänkande (SOU 2005:38 s. 193 f.). Beredningen föreslog att man vid förundersökning angående brott som är så allvarliga att de kan ligga till grund för beslut om hemlig avlyssning skulle få använda hemlig övervakning även om det inte finns någon som är skäligen misstänkt för brottet. Utredningen konstaterade att övervakningsuppgifter, däribland uppgifter om positionen hos mobiltelefoner, ofta är den absolut viktigaste nyckeln för att utredningar rörande grövre brott ska kunna föras framåt. Man framhöll att utredningsarbetet, särskilt i det tidiga skedet, kan handla om att polisen lägger pussel med övervakningsuppgifterna och eventuellt vittnesuppgifter och annan information och på så sätt får fram vilka personer som kan misstänkas för brottsligheten samt när, var och hur brottet planerades och genomfördes och vad gärningsmännen gjorde därefter. Utredningen anförde att det genom kontakterna och intensiteten i kontakterna mellan särskilda mobiltelefoner, som senare kanske kan knytas till bestämda individer, kan vara möjligt att klarlägga hur gärningsmännen har agerat och vilka personer som har varit inblandade i brottsligheten.

BRU framhöll även att förslaget skulle täcka in den situation som tagits upp i tidigare förslag, nämligen att myndigheterna behöver få uppgifter om telemeddelanden som har befordrats till eller från en teleadress som innehas av eller av särskild anledning kan antas ha använts av en målsägande som inte kan samtycka till åtgärden.

Polismetodutredningen

Under beredningen av betänkandet SOU 2005:38 bedömdes det nödvändigt att komplettera underlaget i vissa delar. Regeringen tillsatte därför en särskild utredare för att överväga bl.a. vissa frågor om inhämtning av uppgifter om elektronisk kommunikation under förundersökning innan det finns någon skäligen misstänkt person. Utredningen valde namnet Polismetodutredningen. I likhet med Buggningsutredningen och BRU ansåg Polismetodutredningen att en möjlighet till hemlig övervakning i fall där det ännu inte finns en skäligen misstänkt person är nödvändig för att kunna upprätthålla en effektiv brottsbekämpning (SOU 2009:1 s. 114). Polismetodutredningen föreslog dock att syftet med åtgärden, förutom att fastställa vem som skäligen kan misstänkas för brottet, ska kunna vara att utröna annan omständighet av väsentlig betydelse för utredningen. Som exempel på en sådan situation angavs fallet när man genom uppgifterna kan få fram var en målsägande eller ett vittne befinner sig eller har befunnit sig, eller var en brottsplats är belägen (s. 169).

Propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation

Bestämmelserna i lagen om elektronisk kommunikation om de brottsbekämpande myndigheternas tillgång till uppgifter som angår särskilda elektroniska meddelanden upphävdes enligt förslag i propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation (prop. 2011/12:55). Regleringen ansågs vara varken ändamålsenligt utformad eller uppfylla kraven på rättssäkerhet och integritetsskydd (prop. s. 66). Den nuvarande bestämmelsen i 27 kap. 20 § andra stycket RB infördes enligt förslag i denna proposition (prop. s. 70 f.). Regeringen skrev då bl.a. följande.

> Tillgången till uppgifter om elektronisk kommunikation i ett tidigt skede i en brottsutredning är ofta av central betydelse för att effektivt kunna klara upp allvarliga brott. Det är många gånger avgörande att snabbt kunna utröna vem som är skäligen misstänkt för att andra åtgärder ska kunna vidtas mot denne i syfte att föra utredningen framåt. Vid sådan inhämtning är det av naturliga skäl inte möjligt att koppla åtgärden till en skäligen misstänkt person. Regeringen anser därför att de brottsutredande myndigheterna även i framtiden måste kunna få tillgång till uppgifter om elektronisk kommunikation i förundersökningar, även innan det finns en skäligen misstänkt gärningsman.

Regeringen diskuterade vidare hur möjligheten till hemlig övervakning skulle avgränsas (s. 74). Man avfärdade alternativet att avgränsa möjligheten på det sätt som gjorts i fråga om hemlig kameraövervakning i fall där det saknas en skäligen misstänkt person. I de fallen gäller att syftet med åtgärden ska vara att *fastställa* vem som skäligen kan misstänkas för brottet. Enligt förarbetena till den bestämmelsen innebär rekvisitet att övervakningen i allmänhet ska vara avsedd att leda till att gärningsmannen kan påträffas på bar gärning (prop. 2002/03:74 s. 40 f.). Regeringen ansåg att en sådan ordning skulle innebära en alltför omfattande begränsning i fråga om när inhämtning får ske och att åtgärden även bör kunna ta sikte exempelvis på att utröna var en brottsplats är belägen om den omständigheten är av avgörande betydelse för att utreda vem som skäligen kan misstänkas för brottet. Regeringen stannade för den nuvarande avgränsningen av bestämmelsen, dvs. att åtgärden ska ha som syfte att utreda vem som skäligen kan misstänkas för brottet och menade att denna skrivning skulle täcka in även sådana situationer som nyss sagts.

Utredningen om datalagring och EU-rätten

Utredningen om datalagring och EU-rätten hade bl.a. i uppdrag att se över bestämmelserna om skyldighet att lagra uppgifter om elektronisk kommunikation som gäller leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster samt bestämmelserna om de brottsbekämpande myndigheternas tillgång till sådana uppgifter. Till stor del handlar utredningens delbetänkande Datalagring – brottsbekämpning och integritet (SOU 2017:75) om behovet av anpassning av svensk rätt på grund av EU-domstolens avgörande i Tele2-domen. Vi redogör kortfattat för Tele2-domen och viss efterföljande praxis från EU-domstolen i avsnitt 4.2.2. För denna utrednings vidkommande är det i första hand överväganden i SOU 2017:75 om tillgång till lagrade uppgifter som är relevanta. Utredningen gjorde bedömningen att de nuvarande tillgångsreglerna i rättegångsbalken avser grov brottslighet och uppfyller EU-rättens krav. När det gäller utrymmet för att använda hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet gjorde utredningen följande överväganden utifrån Tele2-domen (s. 257–260).

Tillgång till lagrade uppgifter kan enligt domstolen i princip bara beviljas till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. I särskilda fall, som när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism, skulle dock enligt domstolen tillgång kunna ges även till uppgifter om andra personer när det finns objektiva omständigheter som ger skäl att anta att de uppgifterna i ett konkret fall effektivt skulle kunna bidra till att bekämpa terrorism (avsnitt 9.8.3).

Inledningsvis kan noteras att det i sig inte är tillräckligt att det finns en indirekt koppling till bekämpning av allvarlig brottslighet för att myndigheterna ska få tillgång till uppgifterna. Det krävs, som huvudregel, att personen på något sätt är inblandad i den allvarliga brottsligheten. Domstolen beskriver denna personkrets, för vilka uppgifter kan inhämtas, med de exakta orden som används av Europadomstolen i målet Roman Zakharov mot Ryssland, 4 december 2015, som EU-domstolen hänvisar till. Därtill lägger domstolen ”på något sätt inblandad”, vilket alltså innebär att personkretsen är vidare än endast misstänkta gärningsmän och medhjälpare. Detta stöds även av att Europadomstolen i samma dom (§ 245), med hänvisning till tidigare praxis, konstaterade att det kan vara berättigat med en hemlig övervakningsåtgärd även mot en person som kan ha upplysningar om ett brott, utan att vara misstänkt. I begreppet måste t.ex. även en målsägande ingå. Eftersom en hänvisning görs till Europadomstolens praxis torde dock begreppet vara vidare än så. I Greuter mot Nederländerna, 19 mars 2002, som hänvisades till från Roman Zakharov mot Ryssland (§ 245), bedömdes det nämligen befogat att avlyssna en telefon tillhörande partnern till en dödad person, eftersom det fanns misstankar om att gärningsmannen skulle kunna kontakta henne.

I särskilda fall kan det, enligt EU-domstolen, vara befogat att ge myndigheterna tillgång även till andra personers uppgifter. Det bör särskilt noteras att det uppenbarligen inte endast är när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism som tillgång kan beviljas till uppgifter som rör personer som inte är inblandade i ett allvarligt brott. Av domstolens formulering framgår att det endast är fråga om ett exempel.

… Som redogjorts för ovan tillåter EU-rätten i viss utsträckning övervakning även mot andra än misstänkta. Mot denna bakgrund gör utredningen bedömningen att den övervakning som regleras i 27 kap. 20 § första stycket är förenlig med de krav som EU-rätten uppställer. Enligt 27 kap. 20 § andra stycket RB får hemlig övervakning av elektronisk kommunikation även utföras i syfte att utreda vem som skäligen kan misstänkas för ett brott om åtgärden är av synnerlig vikt för utredningen. För att tillstånd till sådan övervakning ska ges krävs att det är fråga om mycket allvarlig brottslighet med ett straffminimum på fängelse två år (27 kap. 19 § fjärde stycket RB).

Exempel på en sådan åtgärd är basstationstömning (masttömning). En sådan utförs t.ex. om polisen hittar en mördad person och vill undersöka vilka som har befunnit sig vid platsen (eller egentligen vilka mobiltelefoner som har funnits där). En sådan åtgärd avser i bästa fall en (eller flera) misstänkta personer men medför samtidigt att uppgifter inhämtas om personer som inte är misstänkta. Sådan basstationstömning har av regeringen bedömts inte innebära ett betydande ingrepp i den enskildes privata sfär och att det inte omfattas av RF:s skydd av den personliga integriteten i 2 kap. 6 §, eftersom det normalt endast är fråga om en positionsbestämning vid ett specifikt tillfälle (prop. 2011/12:55 s. 97). Dessutom är personuppgifter som behandlas hos de brottsbekämpande myndigheterna omgärdade av integritetsskyddande lagstiftning, se polisdatalagen (2010:361), åklagardatalagen (2015:433) och tullbrottsdatalagen (2017:447).

Det ska i detta sammanhang noteras att nu aktuell övervakning endast får utföras om det är av synnerlig vikt för utredningen. Dessutom är inhämtningen begränsad, såvitt avser meddelande, till historisk information.

Utrymmet för att använda hemlig övervakning av elektronisk kommunikation för att utreda vem som är misstänkt är som ovan beskrivits begränsat enligt EU-rätten. EU-domstolen lämnar dock ett utrymme för att få tillgång till lagrade uppgifter även avseende icke misstänkta personer. Mot bakgrund av att inhämtningen är begränsad (sett till de uppgifter som får inhämtas) och till att den brottslighet som berättigar till sådan övervakning måste vara mycket allvarlig, gör utredningen bedömningen att det utrymme som EU-domstolen ger är tillräckligt för att de svenska reglerna i detta hänseende ska lämnas oförändrade.

Utredningen bedömde vidare att reglerna om tillgång genom hemlig övervakning av elektronisk kommunikation är tydliga och precisa och uppfyller de krav som EU-rätten ställer.

Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel

Efter överlämnande av delbetänkandet Datalagring – brottsbekämpning och integritet bytte Utredningen om datalagring och EU-rätten namn till Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel. Utredningen hade bl.a. i uppdrag att se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när hemliga tvångsmedel för särskilt allvarlig brottslighet används. Utredningen övervägde bl.a. regleringen om hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet, och om det borde införas regler om vilken personkrets som kan utsättas för de åtgärder

som kan omfattas av ett beslut om sådan övervakning, när det gäller de brott som avses i 27 kap. 2 § andra stycket 2–7 RB[1]. Dessa överväganden redovisades i utredningens slutbetänkande Rättssäkerhetsgarantier och hemliga tvångsmedel (SOU 2018:61).

Utredningen konstaterade till att börja med att de åtgärder som i praktiken avses är dels basstationstömning, dvs. att man kontrollerar vilka telefoner eller nummer som kopplat upp sig mot en viss mobilmast, dels riktade åtgärder mot t.ex. en målsägandes telefon eller en telefon som man misstänker används av en okänd gärningsman. Enligt vad som framkommit vid utredningens undersökning var basstationstömningar det vanligaste.

Utredningen bedömde att integritetsintrånget för varje enskild vid basstationstömningar oftast är begränsat, eftersom det normalt endast är fråga om en positionsbestämning vid ett enstaka tillfälle. Man konstaterade att regeringen har bedömt att en sådan övervakning därför inte innebär ett betydande ingrepp i den enskildes privata sfär och inte omfattas av regeringsformens skydd av den personliga integriteten, prop. 2011/12:55 s. 97. Utredningen delade denna bedömning, men framhöll samtidigt att integritetsintrånget kan vara betydande även vid sådana åtgärder, beroende på vilket område som masten täcker (t.ex. om masten endast täcker området kring ett behandlingshem eller en ödslig plats där det ska ske en hemlig sammankomst). Även med beaktande av sådana situationer, ansåg utredningen att risken för ett integritetsintrång är så liten att nuvarande ordning kunde accepteras.

Åtgärder som riktar sig mot en enskild persons nummer, adress eller kommunikationsutrustning och som avser mer än någon enstaka kommunikationsuppgift ansågs normalt innebära ett större integritetsintrång än vad en basstationstömning gör. Det kan därför enligt utredningen framstå som en brist att kretsen som tvångsåtgärderna kan riktas mot inte är begränsad till personer som på något sätt kan antas ha upplysningar om brottet. Utredningen konstaterade samtidigt att en bestämmelse av detta slag måste ge utrymme för en viss flexibilitet för att kunna utnyttjas och att det är svårt att förutse alla de sätt på vilka en hemlig övervakning kan leda utredningen framåt.

[1] I prop. 2021/22:119 föreslås att brottskatalogen flyttas till 18 § andra stycket.

Utredningens bedömning var att bristen på begränsning av personkrets inte är oförenlig med kraven i regeringsformen eller Europakonventionen, och då särskilt Europadomstolens dom i målet Roman Zakharov mot Ryssland. Man tog vid bedömningen särskilt fasta på kravet på att åtgärden är av synnerlig vikt för utredningen, som ansågs innebära en indirekt koppling till den brottslighet som utredningen gäller. Utredningen framhöll även att åtgärden avser särskilt allvarliga eller samhällsfarliga brott och att det är rätten som slutligen bedömer om den sökta åtgärden är proportionell i förhållande till motstående intressen, samt möjligheten att förena tillståndet med särskilda villkor till skydd för enskildas personliga integritet.

Propositionen Hemlig dataavläsning

I propositionen Hemlig dataavläsning (prop. 2019/20:64) finns inga uttalanden som specifikt tar sikte på förutsättningarna att avläsa kommunikationsövervaknings- och platsuppgifter som gäller målsägandens informationssystem. Regeringen uttalade att det i likhet med vad som gäller för befintliga hemliga tvångsmedel bör finnas en möjlighet att använda hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för ett visst brott och framhöll att det kan ge viktiga upplysningar när det har begåtts ett allvarligt brott men där det inte går att hitta någon misstänkt. Regeringen angav vidare att det utan en sådan möjlighet finns risk för att brottsbekämpande myndigheter inte kan gå vidare i utredningar om allvarliga brott. Samtidigt kom man fram till att hemlig dataavläsning endast bör få tillgripas mot avläsningsbara informationssystem som funnits på eller i anslutning till en brottsplats eller om uppgifterna av något annat skäl är av synnerlig vikt för utredningen. Det angavs att uttrycket synnerlig vikt för utredningen bör täcka samtliga fall som bedöms vara av synnerlig betydelse för att utreda vem som skäligen kan misstänkas för brottet. I författningskommentaren tog man bl.a. upp exemplen att ett informationssystem funnits längs en flyktväg från brottsplatsen eller när det finns skäl att tro att gärningspersonen kan tänkas förflytta sig medan brottet fortfarande pågår, t.ex. vid människorov eller grov narkotikasmuggling (s. 219).

8.5 Överväganden om hemlig övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet

8.5.1 Dagens reglering

I lagtexten i 27 kap. 20 § andra stycket RB finns det inga begränsningar i fråga om den personkrets som kan omfattas av hemlig övervakning i syfte att utreda vem som skäligen kan misstänkas för brottet. Som framgått av föregående avsnitt ger förarbetena till nuvarande bestämmelse inte något svar på om det övervägts om hemlig övervakning ska kunna ske av målsägandens kommunikation. Frågan har emellertid behandlats i andra lagstiftningsärenden. I betänkandet Rättssäkerhetsgarantier och hemliga tvångsmedel (SOU 2018:61) fann utredaren att målsäganden omfattas av regleringen och att det inte fanns behov av ändring av lagtexten. Remissinstanserna redovisade inte någon annan uppfattning. Det har också framkommit att domstolar gett tillstånd till övervakning i sådana fall och, såvitt vi har kunnat finna, har tillstånd inte nekats på grund av att det är fråga om en målsägande. Vi gör i avsnitt 8.5 och 8.7 bedömningen att regleringen uppfyller de krav som följer av regeringsformen och Sveriges internationella åtaganden. Gällande rätt får därför anses innebära att det är tillåtet att rikta en hemlig övervakning av elektronisk kommunikation mot målsäganden.

8.5.2 Det finns ett behov av åtgärden

Bedömning: Det finns ett påtagligt behov av en möjlighet att rikta en hemlig övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet.

Skälen för bedömningen

Allmänt om behovet

De brottsbekämpande myndigheterna har upplyst att en hemlig övervakning av målsägandens telefon ofta är en av de första åtgärder som vidtas i utredningar om allvarliga brott där det inte finns en skäligen

misstänkt. Ett typexempel kan vara ett spaningsmord, en synnerligen grov misshandel eller ett människorov. En viktig ingång i ärendet kan då många gånger vara att med hjälp av en hemlig övervakning kartlägga hur målsäganden rört sig, vilka andra telefoner som funnits i samma område vid samma tidpunkt och vilka nummer som målsäganden kommunicerat med (jfr även SOU 1998:46 s. 403 f., SOU 2005:38 s. 193 f. och SOU 2009:1 s. 169). Utifrån en sådan kartläggning kan vidare utredningsåtgärder, t.ex. en hemlig övervakning mot något eller några av de intressanta telefonnumren, vidtas. Enligt de brottsbekämpande myndigheterna kan det vara omöjligt att utan en möjlighet till hemlig övervakning riktad mot målsägande komma framåt i utredningen.

Det kan finnas fall där det är okänt vem som innehar eller använder ett visst nummer eller en viss kommunikationsutrustning, som av något skäl är av intresse i en utredning om ett allvarligt brott. Polisen kan ha skäl att tro att numret eller utrustningen tillhör målsäganden eller en tänkbar gärningsperson. Ett exempel kan vara att polisen har påträffat en viss kommunikationsutrustning, typiskt sett en mobiltelefon, på en brottsplats eller längs med en tänkbar flyktväg. En hemlig övervakning kan då ge ledtrådar om vem telefonen tillhör och om denne har koppling till brottet på något sätt. I en sådan situation är det möjligt att telefonen tillhör gärningspersonen, en medhjälpare till denne, målsäganden, någon som bevittnat brottet eller någon helt utomstående person utan relevans för utredningen. Utan en hemlig övervakning eller en motsvarande hemlig dataavläsning kan det vara svårt eller omöjligt att reda ut hur det förhåller sig och komma vidare med detta spår, alternativt avföra telefonens innehavare från utredningen.

Behovet av hemlig övervakning av elektronisk kommunikation mot målsäganden när målsäganden medverkar

Man kan lite förenklat urskilja tre olika situationer som kan aktualiseras när det gäller att få tillgång till uppgifter om målsägandens elektroniska kommunikation. Den första situationen är att målsäganden medverkar i utredningen. I de fallen är det inte sällan möjligt att med hans eller hennes samtycke få tillgång till de uppgifter som kan behövas om t.ex. kontakter med personer som kan vara intressanta i utredningen. Uppgifterna kan exempelvis finnas lagrade i målsägandens telefon, som frivilligt kan lämnas över till de brottsutredande myn-

digheterna för undersökning och s.k. tömning. I normalfallet tas då telefonen i beslag. Det kan också vara möjligt för målsäganden att från operatören få ut uppgifter om telefonnummer som kontaktat målsägandens nummer, dock mot en kostnad. Det förekommer vidare att Polismyndigheten med fullmakt från abonnenten kan få ut vissa uppgifter från operatören.

Under vårt arbete har det framkommit att det finns stora variationer mellan de olika telebolagen vilken typ av uppgifter man kan få tillgång till på frivillig väg och hur långt tillbaka i tiden dessa sträcker sig. Från vissa bolag kan man inte få uppgifter lika långt tillbaka i tiden som man hade kunnat få genom ett beslut om hemlig övervakning av elektronisk kommunikation. Vidare krävs att det handlar om ett registrerat abonnemang. Om målsäganden har ett oregistrerat kontantkort kan man alltså inte få fram några uppgifter, oavsett om det föreligger ett samtycke. Denna olägenhet kan förväntas minska om förslagen i Lagrådsremissen Registrering av kontantkort – förbättrad tillgång till uppgifter för brottsbekämpande myndigheter om krav på registrering av kontantkort genomförs. Vidare kan man inte vid en förfrågan från abonnenten eller med fullmakt från abonnenten få ut uppgifter om geografiska positioner. Sådana uppgifter är enligt de brottsbekämpande myndigheterna ofta avgörande för att man ska komma framåt i en utredning. Möjligheten att med målsägandens samtycke få tillgång till uppgifter kan alltså i ett utredningsperspektiv inte jämställas med ett beslut om hemlig övervakning av elektronisk kommunikation.

Av det sagda följer att möjligheten att i vissa fall få tillgång till trafikuppgifter från operatören på frivillig väg inte är jämförbar med möjligheten att använda hemlig övervakning av elektronisk kommunikation. Det kan därför även i de fall då målsäganden medverkar i utredningen vara nödvändigt att fatta ett beslut om hemlig övervakning av elektronisk kommunikation för att viktiga uppgifter ska kunna tillföras utredningen. Vidare kan det finnas åtskilliga situationer där det är olämpligt med hänsyn till bl.a. förundersökningssekretessen att be målsäganden hämta in uppgifter eller be honom eller henne om en fullmakt att hämta in uppgifter. Om utredningen leder fram till att någon blir skäligen misstänkt kan det från dennes perspektiv ha betydelse att uppgifterna har hämtats in genom ett tvångsmedel och inte genom målsägandens försorg. Till detta kommer att förfarandet där den enskilde lämnar fullmakt till de brottsbekämpande myndig-

heterna är omdiskuterat och ibland har setts som ett kringgående av regleringen om hemliga tvångsmedel. Utredningen anser i och för sig att det är självklart att en målsägande, som av egen fri vilja vill bidra till att det brott som han eller hon utsatts för blir uppklarat, ska ha möjlighet att göra detta genom att lämna en fullmakt och att det inte bör ses som ett kringgående av reglerna. Eftersom uppfattningen finns och med hänsyn till det ovan anförda gör vi bedömningen att det i utredningar som målsäganden medverkar i finns ett behov av en möjlighet att utföra hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet.

Behovet av hemlig övervakning av elektronisk kommunikation mot målsäganden när målsäganden inte kan medverka

En annan situation är att målsäganden inte kan lämna sitt samtycke till att uppgifter hämtas in. Det kan t.ex. handla om att målsäganden har avlidit, är försvunnen, medvetslös eller av andra medicinska skäl inte kan tillfrågas. Det kan många gånger vara fråga om förundersökningar om allvarlig brottslighet, t.ex. ett pågående människorov, mord, mordförsök eller synnerligen grov misshandel. Om målsäganden är försvunnen, medvetslös eller har avlidit kan han eller hon givetvis inte medverka i utredningen. I ett sådant fall kan det finnas uppgifter om att målsäganden varit i kontakt med eller skulle träffa några personer strax före brottet. De brottsbekämpande myndigheterna har, som nämnts tidigare, anfört att hemlig övervakning av elektronisk kommunikation ofta är den första ingången i ett spaningsärende, och många gånger helt avgörande för att man över huvud taget ska komma vidare i utredningen (jfr även SOU 1998:46 s. 403 f., SOU 2005:38 s. 193 f. och SOU 2009:1 s. 169). Utan en uppgift om vilka personer som senast varit i kontakt med målsäganden kan det enligt myndigheterna vara omöjligt att få fram uppslag om vem som kan misstänkas för brottet. I vissa fall, t.ex. när man inte kan lokalisera en mordplats, kan det även vara av stor vikt med en möjlighet att kunna kartlägga målsägandens rörelser i samband med brottet.

En reglering som gör det omöjligt att utföra en hemlig övervakning mot en målsägande som inte kan medverka i utredningen, skulle leda till allvarliga konsekvenser för möjligheterna att utreda, och i vissa fall även avbryta, allvarliga brott. Det finns därför tveklöst ett be-

hov av en möjlighet att kunna utföra en hemlig övervakning av elektronisk kommunikation mot målsäganden i dessa fall.

Behovet av hemlig övervakning av elektronisk kommunikation mot målsäganden när målsäganden inte vill eller vågar medverka

Den tredje situationen är att målsäganden väljer att inte medverka i utredningen. Oviljan kan ha olika orsaker. Målsäganden kan exempelvis vara starkt påverkad av relationen till gärningspersonen eller gärningspersonerna på grund av släktskap eller vänskapsband. Målsäganden kan själv höra till den kriminella miljön och omfattas av dess tystnadskultur. Enligt uppgift från de brottsbekämpande myndigheterna har det blivit allt vanligare, främst när det gäller brott med koppling till gängkriminalitet, att det i utredningen förekommer personer som på goda grunder kan antas ha uppgifter om brottet men som inte lämnar dessa uppgifter till polisen. Inte sällan handlar det om personer som rör sig i den kriminella miljön. Den som ingår i ett kriminellt nätverk förväntas att inte samarbeta med myndigheterna ens i de fall man utsatts för brott av någon i ett annat kriminellt nätverk. Den som bryter mot denna kodex kan utsättas för repressalier. Här kan även vålds- och skrämselkapitalet hos gärningspersonerna eller deras omgivning ha betydelse. I dessa fall kan det vara mycket svårt eller omöjligt att snäva in kretsen av tänkbara gärningsmän utan att målsäganden medverkar om man inte kan använda hemlig övervakning mot målsäganden för att få kännedom om vilka personer som han eller hon varit i kontakt med eller som har befunnit sig på samma plats som målsäganden vid relevanta tidpunkter. Samtidigt är det naturligtvis mycket angeläget att brottslighet inom kriminella nätverk kan utredas även när målsäganden själv rör sig i den kriminella miljön eller har nära koppling till en gärningsperson.

Det kan också vara så att målsäganden egentligen vill att brottet ska utredas men inte vågar medverka. Denna rädsla kan bero på att målsäganden har utsatts för övergrepp i rättssak eller andra påtryckningar för att inte lämna uppgifter till myndigheterna. Rädslan kan också bero på att gärningspersonerna har ett vålds- och skrämselkapital som gör att de inger fruktan även utan att några uttryckliga påtryckningar eller hot behöver framföras. Vetskapen om vad personerna eller personer i deras omgivning är kapabla till kan i det fallet vara tillräckligt avskräckande. I tidigare lagstiftningsärenden har man

inte fäst någon större uppmärksamhet vid frågan om hur rättsväsendet bör förhålla sig till sådana situationer, men det är en viktig fråga eftersom många människor känner rädsla för att lämna uppgifter till rättsväsendet (se bl.a. Brå, Tystnadskulturer. En studie om tystnad mot rättsväsendet, Brå 2019:10).

Av det anförda framgår att den omständigheten att målsäganden inte medverkar i förundersökningen inte nödvändigtvis kan tas till intäkt för att han eller hon inte egentligen vill att brottet ska utredas. Det måste antas vara mer regel än undantag att den som utsatts för ett allvarligt brott mot person, såsom en synnerligen grov misshandel eller ett människorov, känner rädsla för gärningspersonerna och kan uppleva ett starkt obehag inför att medverka i utredningen. Samma sak gäller när målsäganden vet att gärningspersonerna hör till ett kriminellt nätverk och har ett stort våldskapital.

Regeringen tog i lagrådsremissen Hemlig avlyssning m.m., som inte ledde till lagstiftning, avstånd från användning av hemlig övervakning i syfte att utreda vem som skäligen kan misstänkas för brottet i situationer där målsäganden kan men väljer att inte samtycka till att uppgifterna hämtas in. Man problematiserade inte kring situationer där målsägandens egentliga vilja är att medverka men där han eller hon på grund av påtryckningar eller rädsla känner sig förhindrad till det. I den proposition som ledde till införandet av den nuvarande bestämmelsen i 27 kap. 20 § andra stycket RB förs inga resonemang om samtycke över huvud taget, och övervakning riktad mot målsäganden tas inte upp explicit. Däremot tar regeringen som exempel på situationer där åtgärden bör vara möjlig upp i vart fall en situation där övervakningen rimligen måste kunna avse målsäganden i vissa fall, nämligen den att åtgärden vidtas för att man ska kunna utröna var en brottsplats är belägen (prop. 2011/12:55 s. 74). I ett sådant fall torde övervakningen ofta avse i vilket geografiskt område målsägandens elektroniska kommunikationsutrustning finns eller har funnits (27 kap. 19 § första stycket 3).

För vår del anser vi det principiellt tveksamt att i praktiken lägga avgörandet av om ett allvarligt brott ska utredas i målsägandens hand. Som vi utvecklat i avsnitt 8.3.3 disponerar målsäganden inte över denna fråga, även om man i och för sig inte kan tvinga målsäganden att uttala sig. En ordning där hemlig övervakning mot målsäganden inte kan användas för att få fram vem som skäligen kan misstänkas för brottet innebär att en tung börda läggs på målsäganden, som i värsta

fall ställs inför valet att riskera allvarliga repressalier för sin medverkan i förundersökningen, eller att gärningspersonerna ska gå fria. En sådan ordning ger också potentiellt en stor makt åt gärningspersonerna, som genom att hota målsäganden kan förhindra att brottet kan utredas. Sådana konsekvenser framstår som oacceptabla när det är fråga om brottslighet av det allvarliga slag som det nu är fråga om. I praktiken är hemlig övervakning av elektronisk kommunikation mot målsäganden relativt vanligt förekommande när det gäller viss allvarlig brottslighet. Behovet av åtgärden i den brottsutredande verksamheten är alltså stort.

Det finns vidare en inbyggd motsägelse mellan behovet av sekretess i fråga om hemliga tvångsmedel och ett krav på samtycke från målsäganden i enlighet med vad vissa tidigare utredningar förordat. Sekretess gäller för uppgift som hänför sig till förundersökning i brottmål eller till angelägenhet som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs (18 kap. 1 § offentlighets- och sekretesslagen [2009:400]). Sekretessen gäller hos alla myndigheter som tar befattning med tvångsåtgärder, inklusive en domstol som beslutar om hemlig övervakning och den myndighet som verkställer åtgärden (Tansjö, Geijer och Lenberg, Offentlighets- och sekretesslagen [JUNO 2021-11-23], kommentar till 18 kap. 1 §). I de fall som nu diskuteras lär det med hänsyn till sekretessen vara sällsynt att det är möjligt att fråga efter målsägandens samtycke till inhämtning av uppgifter om elektronisk kommunikation. Mot ett krav på samtycke talar också den omständigheten att lagstiftaren hittills inte gjort någon fördjupad analys av om samtycke till tvångsmedel borde lagregleras särskilt och dessutom tagit avstånd från att avgöra frågan beträffande ett enskilt tvångsmedel (prop. 2005/06:29 s. 25 f.).

Med hänsyn till det anförda gör vi bedömningen att det finns situationer där det inte finns någon annan och mindre ingripande möjlighet att utreda vem som skäligen kan misstänkas för brottet än att använda sig av hemlig övervakning av elektronisk kommunikation oavsett målsägandens inställning. Det finns därför ett påtagligt behov av en möjlighet att använda hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet och detta även i de fall där målsäganden inte samtycker

till åtgärden, eller det av hänsyn till utredningen inte är lämpligt att fråga målsäganden om samtycke.

8.5.3 Åtgärden är proportionerlig

Bedömning: Åtgärden är proportionerlig och förenlig med Sveriges internationella åtaganden.

Skälen för bedömningen

Skyddet för den personliga integriteten

Hemlig övervakning av elektronisk kommunikation utgör en inskränkning av den enskildes rätt till skydd för sitt privatliv och sin korrespondens enligt artikel 8 i Europakonventionen. Europadomstolen har uttalat att det kan vara berättigat med en hemlig övervakningsåtgärd inte bara mot misstänkta gärningsmän och medhjälpare, utan även mot en person som kan ha upplysningar om ett brott utan att vara misstänkt, se Roman Zakharov mot Ryssland § 245. I rättsfallet Greuter mot Nederländerna bedömdes det vara befogat att rikta en hemlig avlyssning mot en telefon som tillhörde partnern till en dödad person, eftersom det fanns misstankar om att den okände gärningsmannen skulle kontakta henne. Något förbud mot att rikta åtgärden mot en målsägande kan enligt vår mening alltså inte uttolkas av Europadomstolens praxis. Åtgärden måste dock givetvis vara proportionerlig och uppfylla de övriga krav som följer av artikel 8.

Hemlig övervakning av elektronisk kommunikation utgör även en inskränkning av de rättigheter som följer av artiklarna 7 och 8 i EU:s rättighetsstadga. EU-domstolen har i bl.a. Tele2-domen uttalat att tillgång till trafikuppgifter och lokaliseringsuppgifter i princip bara kan beviljas till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. I likhet med Utredningen om datalagring och EU-rätten anser vi att uttalandet, med hänsyn bl.a. till de hänvisningar som domstolen gör till Europadomstolens praxis, bör förstås på så sätt att den tänkbara personkretsen inte enbart omfattar misstänkta gärningsmän och medhjälpare utan även t.ex. en målsägande (SOU 2017:75 s. 257 och 258). Liknande uttalanden finns i bl.a. EU-domstolens

dom den 6 oktober 2020, i förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl. som i den nu aktuella delen handlade om lagstiftning i terrorbekämpningssyfte. Där uttalade domstolen att inhämtning av lokaliseringsuppgifter i realtid är tillåtet bl.a. i syfte att bekämpa terrorism, men att åtgärden är särskilt ingripande och därför får vidtas endast gentemot personer beträffande vilka det finns ett giltigt skäl att misstänka att de på ett eller annat sätt är inblandade i verksamheten (punkt 187). Uttrycket ”på ett eller annat sätt inblandad” får förstås på samma sätt som motsvarande uttalande i Tele2-domen. Vår bedömning är således att inte heller EU:s rättighetsstadga i och för sig hindrar att hemlig övervakning riktas mot en målsägande, förutsatt att åtgärden är proportionerlig och kraven för inskränkningar i rättigheterna enligt artiklarna 7 och 8 i övrigt är uppfyllda.

Hemlig övervakning av elektronisk kommunikation kan även vara ett sådant betydande intrång i den personliga integriteten, som avses i 2 kap. 6 § andra stycket regeringsformen, om åtgärden innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Det skydd bestämmelsen ger är emellertid generellt utformat, och kan inte i sig anses hindra bestämmelser om hemliga tvångsmedel mot en målsägande. Skyddet får inskränkas genom lag, förutsatt att villkoren i 2 kap. 21 § regeringsformen är uppfyllda. Bekämpning av allvarlig brottslighet är ett godtagbart ändamål. Därutöver måste begränsningen vara proportionerlig i förhållande till sitt ändamål.

Proportionalitet

Vi har i det föregående gjort bedömningen att det finns ett påtagligt behov av en möjlighet att rikta övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet och att varken EU-rätten, Europakonventionen eller regeringsformen innehåller något förbud mot en sådan möjlighet. Denna bedömning omfattar inte bara fallen att målsäganden samtycker eller saknar möjlighet att samtycka, utan också när målsäganden väljer att inte medverka i utredningen, eller där man inte kan fråga målsäganden utan att äventyra utredningen. Nästa fråga är om behovet av åtgärden väger så tungt att det uppväger det intrång i den person-

liga integriteten och rätten till skydd för sina personuppgifter som åtgärden innebär för målsäganden.

Vi konstaterar då till att börja med att hemlig övervakning av elektronisk kommunikation anses vara ett av de minst integritetskänsliga av de hemliga tvångsmedlen. Detta utesluter inte att åtgärden kan utgöra ett allvarligt ingrepp i målsägandens rätt till skydd för sitt privatliv, sin korrespondens och sina personuppgifter, åtminstone i de fall man med hjälp av åtgärden kan dra precisa slutsatser om målsägandens privatliv (jfr artikel 8 i Europakonventionen och artiklarna 7 och 8 i EU:s rättighetsstadga, samt EU-domstolens avgörande i bl.a. dom den 2 mars 2021 i målet C-746/18, Prokuratuur). Detta gäller särskilt när det är fråga om övervakning i realtid (jfr EU-domstolens dom den 6 oktober 2020, i förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., punkt 187). Åtgärden bör därför endast komma ifråga i syfte att utreda allvarlig brottslighet. Detta krav bedömer vi vara uppfyllt genom dagens reglering. Någon anledning att ställa än högre krav finns inte och skulle dessutom leda till att bestämmelsen förlorar alltför mycket i effektivitet.

Vi konstaterar vidare att kraven för att åtgärden ska få vidtas är högt ställda genom att det både krävs att brottet är av det slaget att hemlig avlyssning av elektronisk kommunikation är tillåten och att åtgärden ska vara av synnerlig vikt för utredningen. Det krävs alltså att åtgärden i princip är nödvändig för att utredningen ska föras framåt. I avsnitt 8.8 utvecklar vi varför vi inte heller föreslår någon skärpning i detta avseende. En annan begränsning är att möjligheten att hämta in uppgifter om meddelanden begränsad till förfluten tid. Vi anser dock inte att denna begränsning är lämplig eller nödvändig, vilket har utvecklats närmare i avsnitt 7.5.

Ett argument mot att man tillåter hemlig övervakning mot målsäganden är det särskilda skydd som målsäganden åtnjuter i en förundersökning och rättsprocess. Målsäganden kan inte tvingas att utala sig och kan inte kroppsundersökas utan sitt frivilliga samtycke. Det finns skäl som talar för att man bör respektera målsägandens personliga integritet och önskan att inte medverka i en utredning. Som framgår av framställningen i avsnitt 8.3.3 är det dock möjligt att använda ett visst tvång mot en målsägande inom ramen för en brottsutredning och rättsprocess. Det har även framkommit att målsäganden indirekt kan drabbas av tvångsmedel som riktas mot den misstänkte, t.ex. genom att en hemlig avlyssning av den misstänktes telefon kan

innebära att även telefonsamtal med målsäganden avlyssnas. Som Säkerhets- och integritetsskyddsnämnden anfört kan vidare målsägandens drabbas vid en s.k. basstationstömning, eftersom den visar alla telefonnummer som kopplat upp mot en viss basstation vid en viss tidpunkt. Det är dock en principiell skillnad mellan detta och att ett tvångsmedel medvetet riktas mot målsäganden. I ett sådant fall vet den brottsbekämpande myndigheten att den som utsätts för tvångsmedlet inte är gärningspersonen. Som vi framhållit ovan är det dessutom typiskt mer integritetskränkande att inhämta uppgifter om meddelanden än att göra en basstationstömning. Det handlar vidare, som nyss sagts, om en person som i princip inte kan tvingas att medverka i brottsutredningen. En hemlig övervakning av målsägandens elektroniska kommunikation kan innebära en mer systematisk och omfattande kartläggning av målsägandens kontakter än vad som skulle vara fallet om man övervakar den misstänktes kontakter och vissa av dem är med målsäganden. Samtidigt bör man beakta bestämmelsen i 27 kap. 20 § första stycket 2 RB, som innebär att det är tillåtet inte bara att rikta en övervakning eller avlyssning mot exempelvis en adress eller kommunikationsutrustning som den misstänkte innehar, utan också mot en adress eller kommunikationsutrustning som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta. Inget hindrar att en sådan åtgärd avser exempelvis målsägandens telefonnummer. Det är också viktigt att framhålla att hemlig övervakning som riktar sig mot målsägandens telefonnummer förekommer redan i dag, och har förekommit under lång tid. Det som diskuteras nu är alltså inte någon ny åtgärd. Däremot kan möjligheten att använda den komma att bli mer omfattande till följd av våra förslag i kapitel 6 och 7.

I sammanhanget kan man vidare framhålla att det är möjligt med beslag och genomsökning av telefoner, datorer och andra elektroniska informationsbärare som tillhör målsäganden.

Det har vidare framförts farhågor om att risken för att utsättas för hemliga tvångsmedel kan göra brottsoffer mer obenägna att anmäla brott och medverka i förundersökningen. Som framkommit ovan är det vanligt att målsäganden är rädd för att medverka och för att utsättas för repressalier. Särskilt risken för en minskad anmälningsbenägenhet bör tas på allvar. Däremot är det svårt att se att målsägandena skulle bli mer utsatta i förhållande till gärningspersonerna än de skulle vara om de aktivt medverkar i utredningen och lämnar

uppgifter till de brottsbekämpande myndigheterna. Som nyss sagts är det inte fråga om någon ny möjlighet, även om den kan komma att få ett utvidgat tillämpningsområde. Det är inte känt för utredningen att målsägande hittills skulle ha utsatts för repressalier på grund av att de varit föremål för hemlig övervakning av elektronisk kommunikation.

Sammanfattningsvis konstaterar vi att målsäganden inte har något absolut skydd mot olika former av tvångsåtgärder och integritetsintrång och att den åtgärd som nu diskuteras förekommer redan i dag. I vissa fall, såsom när målsäganden bragts om livet, är medvetslös eller är utsatt för ett pågående människorov, måste det presumeras att målsäganden vill eller hade velat att brottet ska kunna utredas och i förekommande fall avbrytas. Men även när det gäller andra allvarliga brott talar starka skäl för intresset av att brottet kan utredas bör ges företräde och målsäganden att får tåla en hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet. Allvarlig brottslighet kan inte betraktas som en privatsak och lagstiftaren har inte gett målsäganden rätten att disponera över frågan om det ska inledas en förundersökning eller väckas åtal över brott av detta slag. En målsägande som lämnat uppgifter under förundersökningen och sedan tar tillbaka dessa under rättegången kan inte hindra att förundersökningsuppgifterna åberopas som bevis, inte ens om målsäganden och den tilltalade står i ett sådant förhållande till varandra att målsäganden inte hade varit skyldig att vittna i målet. Det ligger i samhällets intresse att allvarliga brott kan utredas även när målsäganden inte vill medverka. Detta gäller inte minst från ett brottsförebyggande perspektiv, eftersom gärningspersonen kan hindras från att begå ytterligare allvarliga brott. Som vi har utvecklat i det föregående är det dessutom så att en målsägande kan vara rädd för att medverka i utredningen fastän han eller hon egentligen mycket gärna vill att brottet ska utredas och de ansvariga ställas till svars. Ett beslut om hemlig övervakning av elektronisk kommunikation kan då lyfta en börda från målsäganden, genom att utredningen inte står och faller med hans eller hennes medverkan. Möjligheten att fatta beslut om tvångsmedlet kan även minska incitamentet för gärningspersonerna att utöva hot eller andra påtryckningar mot målsäganden.

Vår samlade bedömning är att det är proportionerligt med en möjlighet att rikta hemlig övervakning av elektronisk kommunikation mot målsäganden.

8.5.4 Åtgärden bör även fortsättningsvis vara tillåten

Bedömning: Det bör även i fortsättningen vara tillåtet att rikta en hemlig övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet.

Skälen för bedömningen

Som framgått i föregående avsnitt finns det starka skäl som talar för att man även i fortsättningen ska ha en möjlighet att rikta en hemlig övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet, samtidigt som det finns vissa invändningar mot en sådan ordning. Vår bedömning är att de skäl som talar för att en sådan möjlighet ska finnas även i fortsättningen klart överväger invändningarna. En annan ordning skulle innebära ett allvarligt hinder för den brottsutredande verksamheten som, när det handlar om allvarlig brottslighet, inte kan motiveras av hänsynen till målsägandens integritet. Detta gäller inte minst när målsäganden är ett barn, är rädd för att frivilligt medverka i utredningen eller är avliden, försvunnen eller av någon annan anledning förhindrad att medverka. Det är enligt vår mening inte acceptabelt att bördan för att allvarliga brott ska kunna utredas vilar på målsäganden och att kriminella genom att skrämma en målsägande kan hindra att brottet utreds. Vidare bör samhället inte ge vika för de kriminella miljöernas tystnadskultur, vilket blir en av följderna om målsägandens vilja att medverka blir avgörande.

Det bör med hänsyn till det anförda även framöver vara tillåtet att rikta en hemlig övervakning av elektronisk kommunikation mot målsägande i syfte att utreda vem som skäligen kan misstänkas för brott. Besluten ska dock givetvis, som alltid när det gäller hemliga tvångsmedel, utformas på ett sådant sätt att integritetsintrånget minimeras och vara så begränsat som möjligt.

8.6 Överväganden om hemlig dataavläsning mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet

8.6.1 Det finns ett behov av åtgärden

Bedömning: Det finns ett påtagligt behov av en möjlighet att rikta en hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet.

Skälen för bedömningen

Hemlig övervakning av elektronisk kommunikation är ett något mindre ingripande tvångsmedel än hemlig dataavläsning avseende kommunikationsövervaknings- och platsuppgifter, eftersom man med det sistnämnda tvångsmedlet kan få fram fler och mer detaljerade uppgifter om t.ex. var den övervakade har befunnit sig. Kravet på synnerlig vikt betyder enligt förarbetena bl.a. att utredningsläget ska vara sådant att hemlig dataavläsning är nödvändig (propositionen Hemlig dataavläsning, prop. 2019/20:64 s. 216). Åtgärden får inte tillåtas om det som kan vinnas är åtkomligt med andra, mindre ingripande metoder. Synnerlig vikt kan anses föreligga om andra åtgärder inte är tillräckliga, väsentligt svårare att genomföra än hemlig dataavläsning eller förväntas leda till ett större integritetsintrång. Den som ansöker om hemlig dataavläsning måste därför utreda eller tömma ut möjligheterna till andra åtgärder innan ansökan görs.

I de fall det är möjligt att använda hemlig övervakning av elektronisk kommunikation måste man därför förutsätta att det tvångsmedlet väljs. Det följer också av de principer som reglerar all tvångsmedelsanvändning att det mindre ingripande tvångsmedlet ska väljas om det går. I vissa situationer kan det dock vara omöjligt att nå framgång med en hemlig övervakning av elektronisk kommunikation. Ett exempel kan vara att de uppgifter man behöver få tillgång till inte omfattas av operatörernas lagringsskyldighet men kan finnas lagrade i informationssystemet. Operatörer har en lagringsskyldighet för vissa trafik- och lokaliseringsuppgifter. Många uppgifter ingår dock inte i lagringsskyldigheten och om operatören inte lagrar en viss upp-

gift för eget ändamål finns inte uppgifterna kvar. Det kan då ändå vara möjligt att få tillgång till uppgiften genom hemlig dataavläsning som riktas mot informationssystemet. En viktig skillnad mellan hemlig övervakning av elektronisk kommunikation och hemlig dataavläsning är att man genom en hemlig dataavläsning kan få tillgång även till uppgifter om kommunikation som förmedlats i datanätet och via krypterade appar och e-postkonton.

Som nämnts ovan kan man genom en hemlig dataavläsning vidare få tillgång till mer precisa platsuppgifter. En lokaliseringsuppgift som man med stöd av ett beslut om hemlig övervakning av elektronisk kommunikation får ut från en teleoperatör utgår ifrån var en eller flera basstationer är placerade. Det kan då röra sig om ett stort område som täcks av respektive basstation. Med hemlig dataavläsning kan i stället lokaliseringsuppgiften utgå från en gps-positionering från den elektroniska kommunikationsutrustningen (dvs. informationssystemet). Detta ger en betydligt mer precis information om var informationssystemet funnits vid en viss tidpunkt, något som kan vara av stor betydelse i en brottsutredning men som samtidigt innebär ett större integritetsintrång. Beroende på omständigheterna i det enskilda fallet kan man även genom en hemlig dataavläsning få tillgång till fler kommunikationsövervakningsuppgifter bl.a. i form av metadata.

Med hänsyn till det anförda, och till det som tidigare anförts om behovet av platsuppgifter och kommunikationsövervakningsuppgifter bedömer vi att det finns ett påtagligt behov av en möjlighet att använda hemlig dataavläsning mot målsäganden rörande sådana uppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet.

8.6.2 Åtgärden är proportionerlig

Bedömning: Det är proportionerligt med en möjlighet att rikta en hemlig dataavläsning mot målsäganden i syfte att utreda vem som skäligen kan misstänkas.

Skälen för bedömningen

När det gäller proportionalitet gör sig till stora delar samma argument gällande som i fråga om hemlig övervakning av elektronisk kommunikation. Hemlig dataavläsning framstår visserligen som mer ingri-

pande från integritetssynpunkt, men skillnaden är inte särskilt stor när det gäller uppgifter av de aktuella slagen. Det handlar i allt väsentligt om samma slags uppgifter, även om det i vissa fall går att få tillgång till mer detaljerade eller ytterligare uppgifter jämfört med en hemlig övervakning av elektronisk kommunikation. Som redan anförts följer det av allmänna principer för tvångsmedelsanvändning att det minst ingripande tvångsmedel som är möjligt ska väljas. Möjligheten att använda hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet är vidare förenad med betydande begränsningar såväl när det gäller brottets allvar som betydelsen för utredningen och det avlästa informationssystemets koppling till brottet. Vi bedömer med hänsyn till det anförda att det är proportionerligt med en möjlighet att använda tvångsmedlet mot målsäganden.

8.6.3 Åtgärden bör även fortsättningsvis vara tillåten

Bedömning: Det bör vara tillåtet att rikta en hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet.

Skälen för bedömningen

Vi har i föregående avsnitt kommit fram till att det finns ett behov av en möjlighet att rikta en hemlig dataavläsning avseende kommunikationsövervakningsuppgifter och platsuppgifter mot målsäganden. Vi har även kommit fram till att det är en proportionerlig åtgärd. Det bör därför även i fortsättningen vara tillåtet att rikta en hemlig dataavläsning som gäller kommunikationsövervaknings- och platsuppgifter mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet.

8.7 Bestämmelsen bör inte ändras

Bedömningar: Bestämmelsen om hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet är tillräckligt tydlig och avgränsad i fråga om den personkrets som åtgärden får avse. Samma bedömning görs i fråga om hemlig dataavläsning i det angivna syftet.

Skälen för bedömningarna

Kravet på lagstöd och koppling till utredningen om brottet

Som framgått tidigare kan hemlig övervakning av elektronisk kommunikation utgöra en inskränkning av det grundlagsskydd som följer av 2 kap. 6 § andra stycket regeringsformen. Det följer av legalitetsprincipen att en bestämmelse som begränsar en grundlagsskyddad rättighet ska tolkas restriktivt och enligt sin ordalydelse. Ingrepp i rättigheten får inte grundas på en extensiv eller analogisk tolkning (Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas? 4 uppl., s. 21).

Enskildas privatliv och korrespondens åtnjuter även ett skydd enligt artikel 8 i Europakonventionen. Europadomstolen har genom praxis utvecklat en minimistandard för de krav som bör ställas på lagstiftningen om dolda spaningsåtgärder eller hemliga tvångsmedel till undvikande av missbruk (se närmare i framställningen i avsnitt 3.2). Ett av kraven är att den nationella lagstiftningen innehåller en definition av de personkategorier som kan riskera att få hemliga tvångsåtgärder riktade mot sig. Domstolen har i dessa sammanhang uttalat kritik mot lagstiftning som gör det möjligt att, utan närmare klargörande av vilka som kan omfattas av regleringen, rikta sådana åtgärder mot var och en som kan ha information om ett brott eller som har inblandning i ett brott och andra liknande skrivningar (se Roman Zacharov mot Ryssland punkt 245 och 249 och Iordachi mot Moldavien punkt 44). Samtidigt synes domstolen inte kräva att klargörandet finns i skriven lag utan tycks godta att det ges i vedertagen rättspraxis eller en vedertagen juridisk tolkning av begreppen.

Som vi utvecklat i avsnitt 8.5.3 följer det av EU-domstolens praxis att inhämtning av lokaliseringsuppgifter i realtid endast får vidtas gentemot personer beträffande vilka det finns ett giltigt skäl att misstänka att de på ett eller annat sätt är inblandade i brottsligheten (se bl.a. EU-domstolens dom den 6 oktober 2020, i förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl.). Vi har i det nämnda avsnittet gjort bedömningen att uttrycket ”på ett eller annat sätt är inblandade i brottsligheten” måste anses innefatta bl.a. målsäganden.

Frågeställningen

Hemlig övervakning avseende vilka elektroniska kommunikationsutrustningar som funnits inom ett visst geografiskt område, s.k. basstationstömning, (27 kap. 19 § första stycket 2), utgör enligt förarbetena inte ett sådant betydande ingrepp i den enskildes privata sfär som omfattas av skyddet i 2 kap. 6 § andra stycket regeringsformen (prop. 2011/12:55 s. 97). Bestämmelsen kan knappast begränsas genom krav på att åtgärden ska knytas till en viss personkategori. I dessa fall måste det därför anses tillräckligt med de begränsningar som följer av kraven på förundersökning och att åtgärden är av synnerlig vikt för utredningen. Något krav på ett tydligare lagstöd finns alltså inte enligt vår bedömning.

Inhämtning av uppgifter om meddelanden (punkten 1 i samma paragraf) och uppgifter om var en viss utrustning finns eller har funnits (punkten 3 i samma paragraf) kan dock innebära en riktad och systematisk övervakning av en viss person. Om uppgifterna gör det möjligt att dra mycket precisa slutsatser om den övervakade personens privatliv kan det bli fråga om ett betydande ingrepp i den personliga integriteten. Sådan inhämtning kan utgöra en inskränkning av rättigheterna enligt 2 kap. 6 § andra stycket RF som kräver lagstöd och omfattas dessutom av skyddet enligt artikel 8 i Europakonventionen och artiklarna 7 och 8 i EU:s rättighetsstadga. Det krävs därför mer ingående överväganden i frågan om det bör förtydligas vilken personkrets som kan drabbas, och i så fall hur en sådan reglering ska utformas.

Tidigare uttalanden

Frågan har relativt nyligen övervägts av Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel (SOU 2018:61). Utredningen ansåg att åtgärder som riktar sig mot en enskild persons nummer, adress eller kommunikationsutrustning (och som avser mer än någon enstaka kommunikationsuppgift) normalt innebär ett större integritetsintrång än vad en basstationstömning gör. Det kunde därför enligt utredningen framstå som en brist att kretsen som tvångsåtgärderna kan riktas mot inte är begränsad till personer som på något sätt kan antas ha upplysningar om brottet. Utredningen konstaterade samtidigt att en bestämmelse av detta slag måste ge utrymme för en viss flexibilitet för att den ska kunna användas. Vidare anförde utredningen att det är svårt att förutse alla de sätt som en hemlig övervakning kan leda utredningen framåt. Vid en samlad bedömning kom utredningen fram till att bristen på begränsning av personkrets inte är oförenlig med kraven i regeringsformen eller Europakonventionen. Man fäste då särskilt vikt vid att det genom kravet på synnerlig vikt för utredningen finns en indirekt koppling mellan åtgärden och brottsligheten. Vidare lyfte man bl.a. fram att det är rätten som slutligen bedömer om den sökta åtgärden är proportionell i förhållande till motstående intressen och möjligheten att förena tillståndet med särskilda villkor till skydd för enskildas personliga integritet. (SOU 2018:61 s. 122–124.) De remissinstanser som kommenterade frågan ställde sig bekom bedömningen att den nuvarande regleringen är godtagbar.[2]

Utredningen tog även, i delbetänkandet Datalagring – brottsbekämpning och integritet, ställning till bestämmelsens förenlighet med Tele2-domen (SOU 2017:75 s. 257–260). Mot bakgrund av att inhämtningen är begränsad (sett till de uppgifter som får inhämtas) och till att den brottslighet som berättigar till sådan övervakning måste vara mycket allvarlig, gjorde utredningen bedömningen att det utrymme som EU-domstolen ger för att rikta hemlig övervakning mot andra än misstänkta är tillräckligt för att de svenska reglerna i detta hänseende skulle lämnas oförändrade. Reglerna ansågs även vara tillräckligt tydliga och precisa.

[2] Se bl.a. Säkerhets- och integritetsskyddsnämndens yttrande 2018-11-14, där nämnden visserligen inte låter sig övertygas av utredningens argumentation men samtidigt gör bedömningen att det inte framstår som möjligt att på motsvarande sätt som vid hemlig avlyssning införa en begränsning avseende den personkrets som kan komma att träffas av tvångsåtgärden, eftersom syftet med bestämmelsen då skulle motverkas. Nämnden landade i bedömningen att nuvarande reglering kan godtas.

Reglernas praktiska användning

Innan vi går in på frågan om bestämmelsen behöver ändras i fråga om den personkrets som omfattas finns det anledning att något beskriva olika situationer där bestämmelserna tillämpas.

Det bör redan inledningsvis sägas att det i många av de fall som kan aktualiseras är okänt vem som innehar eller använder ett visst nummer eller en viss kommunikationsutrustning, som av något skäl är av intresse i en utredning om ett allvarligt brott. Ett vanligt exempel, inte minst i mordutredningar, är att man genom en hemlig övervakning mot målsägandens telefon har fått uppgift om ett eller flera nummer som målsäganden haft kontakt med. I syfte att utreda om något av dessa nummer används av gärningspersonen kan det vara nödvändigt att rikta en hemlig övervakning mot numren. Åtgärden kan leda till misstankar mot innehavaren av ett visst nummer och till att andra nummer och personer kan avföras från utredningen. Om kontakterna i stället avser exempelvis en molnbaserad e-postadress vars innehavare är okänd, kan en hemlig dataavläsning som riktar sig mot e-postkontot ha motsvarande funktion.

En annan situation kan vara att det i och för sig är känt att brottet begåtts av en person som använder ett visst nummer, men att man inte vet vem som innehar eller använder detta. Det kan också hända att polisen har påträffat en viss kommunikationsutrustning, typiskt sett en mobiltelefon, på en brottsplats eller längs med en tänkbar flyktväg. En hemlig övervakning kan då ge ledtrådar om vem telefonen tillhör och om den har koppling till brottet på något sätt. I en sådan situation är det möjligt att telefonen tillhör gärningspersonen, en medhjälpare till denne, målsäganden, någon som bevittnat brottet eller någon helt utomstående person utan relevans för utredningen. Utan en hemlig övervakning eller en motsvarande hemlig dataavläsning kan det vara svårt eller omöjligt att reda ut hur det förhåller sig och komma vidare med detta spår, alternativt avföra telefonens innehavare från utredningen. Ett liknande exempel kan vara att man genom hemlig övervakning riktad mot den misstänktes telefon har fått kännedom om kontakter som denna haft med andra nummer. Om det finns anledning att tro att det finns ytterligare gärningsmän eller andra medverkande, kan det vara av stort värde att inhämta vissa uppgifter om dessa nummer.

Ytterligare en situation är den att det har genomförts en basstationstömning som visar vilka telefoner som funnits i närheten av brottsplatsen vid brottstidpunkten. En basstationstömning är normalt endast ett första steg, som måste följas av ett omfattande analysarbete som syftar till att man ska identifiera intressanta nummer. När man genom detta arbete identifierat ett eller flera nummer som man har skäl att tro är intressanta i utredningen är det ofta nödvändigt med ett beslut om hemlig övervakning mot numren för att man ska kunna komma vidare och antingen få stöd för hypotesen att numret är relevant, eller avföra det från utredningen. Som ett av många möjliga exempel kan man nämna mordutredningar där ingången i ärendet är de platser där målsäganden befunnit sig precis före mordet och en kartläggning av nummer som funnits på samma platser vid samma tidpunkter. Det kan då vara så att man inte har någon information om det eller de nummer som man får fram mer än att numret kan vara av intresse för att finna en skäligen misstänkt. Inte sällan är det fråga om ett oregistrerat kontantkort som nyligen tagits i bruk. En hemlig övervakning riktad mot det intressanta numret kan då, eventuellt tillsammans med vittnesuppgifter eller annan utredning, leda utredningen framåt och en misstänkt identifieras.

Enligt uppgift från de brottsbekämpande myndigheterna har det blivit allt vanligare, främst när det gäller brott med koppling till gängkriminalitet, att det i utredningen förekommer personer som på goda grunder kan antas ha uppgifter om brottet men som inte lämnar dessa uppgifter till polisen. Inte sällan handlar det om personer som rör sig i den kriminella miljön och det kan vara ovisst vilken roll – om någon – personerna i fråga har i förhållande till brottet.

Ett annat vanligt scenario vid gängskjutningar är att polisen inte har några ingångar i ärendet utöver att det förmodligen rör sig om en hämndaktion. Utredningen inriktas då på en kartläggning av ledarfigurer i gängmiljön och andra personer som skulle kunna ha motiv till gärningen. Det kan då bl.a. vara relevant att hämta in positionsuppgifter avseende tiden före mordet för att se hur personerna har rört sig och om något talar för att man exempelvis har rekognoserat.

Ett annat exempel på när en möjlighet till hemlig övervakning mot en okänd person kan vara avgörande är situationen att någon från ett oregistrerat kontantkort har ringt 112 för att tillkalla ambulans i samband med ett allvarligt våldsbrott. Det kan då vara nödvändigt med

hemlig övervakning i syfte att få reda på vem personen är, så att man kan höra honom eller henne.

Det har blivit allt vanligare att kriminella personer som planerar ett attentat i hemlighet sätter fast en spårningsutrustning på ett fordon eller något annat föremål som används av det tilltänkta offret. Spårningsutrustningen innehåller ett sim-kort som i sin tur är knutet till ett telefonnummer. Genom kommunikation med det nummer som är knutet till sim-kortet kan de kriminella kartlägga det tilltänkta offrets rörelser och planera attentatet. I brottsutredningen kan det därför vara av stort värde att rikta en hemlig övervakning mot detta nummer för att se vilka nummer det har kommunicerat med och därigenom få ledtrådar om vem som skäligen kan misstänkas för attentatet eller det planerade attentatet.

Bedömning

Av framställningen under föregående rubrik framgår att det inte bara finns ett behov en möjlighet att kunna rikta en hemlig övervakning av elektronisk kommunikation, alternativt en motsvarande hemlig dataavläsning, mot en målsägande, utan att det finns många olika scenarion där hemlig övervakning behöver kunna tillgripas, inklusive sådana där det är okänt vem som innehar ett visst intressant nummer eller motsvarande. Som Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel framhöll behöver regleringen vara flexibel för att kunna fungera i praktiken. Vi har övervägt olika möjligheter för att reglera de olika kategorier av personer som kan bli föremål för tvångsmedlet och kommit fram till att det inte låter sig göras utan att den nödvändiga flexibiliteten förloras.

Regleringen är redan i dag utformad på så sätt att det krävs att åtgärden har synnerlig vikt för utredningen om ett specifikt allvarligt brott och att detta ska visas för domstolen som har att pröva tillståndsfrågan. Det krav på en koppling mellan en viss brottsmisstanke och den hemliga tvångsåtgärden som följer av EU-domstolens praxis (se bl.a. La Quadrature du Net) får därför anses uppfyllt.

8.8 Kraven bör inte skärpas

Bedömning: Det bör inte införas strängare krav i fråga om brottets allvar eller åtgärdens vikt för utredningen än vad som gäller för närvarande.

Skälen för bedömningen

Vi har i det föregående kommit fram till att det även i fortsättningen bör vara möjligt att oberoende av målsägandens samtycke rikta en hemlig övervakning av elektronisk kommunikation eller en hemlig dataavläsning mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet. Vi har även konstaterat att kraven för att åtgärden ska få vidtas redan enligt gällande reglering är högt ställda. Med hänsyn till det särskilda skydd som målsäganden åtnjuter i en brottsutredning bör det dock ändå övervägas om det finns anledning till några ytterligare begränsningar utöver de som följer av dagens bestämmelser.

När det gäller syftet med åtgärden gör sig de skäl som anfördes i förarbetena fortfarande gällande. Det bör således inte krävas t.ex. att åtgärden syftar till att man ska kunna fastställa vem som skäligen kan misstänkas för brottet (jfr 27 kap. 20 c § och prop. 2011/12:55 s. 74).

Vi har vidare övervägt om man bör ställa högre krav i fråga om betydelsen för utredningen. Enligt nuvarande bestämmelser ska åtgärden ska vara av synnerlig vikt för utredningen. Kravet innebär bl.a. att åtgärden på grund av utredningsläget är nödvändig och att det som kan åstadkommas genom åtgärden i princip inte är åtkomligt med andra och mindre ingripande metoder (prop. 2013/14:237 s. 94 f.). Det har inte framkommit något som tyder på att hemlig övervakning eller hemlig dataavläsning mot målsäganden används i fall där det hade varit möjligt att föra utredningen framåt med hjälp av andra och mindre ingripande utredningsmetoder. För att inskärpa vikten av att åtgärden inte används annat än när man inte har andra möjligheter kan man ändå tänka sig ett krav på att åtgärden ska vara *nödvändig för utredningen*. Med tanke på hur man i förarbetena har beskrivit innebörden av kravet på synnerlig vikt är det dock tveksamt om det skulle bli någon skillnad i praktiken. Risken är vidare att det blir svårt för den som ska tillämpa bestämmelsen att se någon tydlig gräns

mellan rekvisitet *av synnerlig vikt* och rekvisitet *nödvändig*. Med hänsyn till detta föreslår vi inte någon skärpning i fråga om kravet av åtgärdens vikt för utredningen.

Det kan även övervägas om man bör ställa högre krav på brottets allvar för att hemlig övervakning eller hemlig dataavläsning mot målsäganden ska få användas i de nu aktuella fallen. Man kan då tänka sig att kravet i fråga om minimistraff eller lägsta straffvärde sätts högre än den gräns som gäller i dag, dvs. ett minimistraff på lägst två års fängelse eller ett straffvärde som överstiger två års fängelse (27 kap. 20 § andra stycket RB). Man kan t.ex. tänka sig att sätta den nedre gränsen på så sätt att den överensstämmer med villkoren för hemlig rumsavlyssning. Detta skulle innebära att åtgärden begränsas till de allra allvarligaste brotten såsom mord, människorov och synnerligen grov misshandel. Även de allvarligaste fallen av exempelvis olaga frihetsberövande och grov misshandel skulle omfattas, om man tillämpar en straffvärdeventil och i enlighet med våra förslag i avsnitt 6.9 avskaffar brottskatalogen. Det som talar för en begränsning till de allra allvarligaste brotten är främst hänsynen till målsägandens personliga integritet, med särskilt beaktande av det skydd målsäganden åtnjuter i brottsutredningar och rättegångar. Vi anser dock att övervägande skäl talar emot en sådan begränsning, först och främst det faktum att kraven redan är högt ställda. Det kan knappast motiveras att man ställer högre krav för en hemlig övervakning av elektronisk kommunikation än för en hemlig avlyssning av sådan kommunikation, även om åtgärden riktas mot målsäganden. Som vi redan konstaterat kan det för övrigt förekomma att målsägandens telefon övervakas eller avlyssnas med stöd av 27 kap. 20 § första stycket 2. Det skulle vara inkonsekvent att ställa ännu högre krav enbart för att det inte finns en skäligen misstänkt person. Vidare skulle alltför många angelägna och svårutredda brott sorteras bort med en sådan begränsning. Slutligen skulle regleringen bli spretig och svår att tillämpa. Vi bedömer därför att det bör vara tillräckligt att brottet är sådant att hemlig avlyssning av elektronisk kommunikation är tillåten. Av detta följer att vi inte heller anser att möjligheten bör begränsas genom en brottskatalog. Eftersom vi i kapitel 6 och 7 föreslår utökade möjligheter att använda hemlig avlyssning av elektronisk kommunikation innebär denna bedömning att även möjligheten att använda hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänktas för brottet utvidgas. Det ändrar inte vår be-

dömning. Tvärtom har de argument som vi i kapitel 6 anfört till stöd för ståndpunkten att hemliga tvångsmedel bör vara tillgängliga vid viss organiserad eller systematisk brottslighet även när varje enskilt brott har ett straffvärde som inte når upp till nuvarande trösklar samma relevans också i fråga om hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet.

Vår bedömning är alltså att det inte är påkallat att införa några ytterligare krav eller begränsningar när det gäller brottets allvar eller tvångsmedlets betydelse för utredningen för att hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet även fortsättningsvis ska få vidtas mot en målsägande.

9 Nya möjligheter att utreda vem som skäligen kan misstänkas

9.1 Uppdraget

Det är tillåtet att använda hemlig övervakning men inte hemlig avlyssning av elektronisk kommunikation i vissa fall där det inte finns någon som skäligen kan misstänkas för brottet. Syftet med den hemliga övervakningen ska då vara att utreda vem som skäligen kan misstänkas för brottet. I direktiven anges att det finns skäl ur brottsbekämpningsperspektiv att tillåta även hemlig avlyssning av elektronisk kommunikation i detta syfte. Samtidigt framhålls det att hemlig avlyssning av elektronisk kommunikation är ett ingripande tvångsmedel, varför det finns anledning att se restriktivt på i vilka fall det ska få användas. Vi har därför i uppdrag att

- ta ställning till om hemlig avlyssning av elektronisk kommunikation bör få användas i syfte att utreda vem som skäligen kan misstänkas för brottet och i så fall i vilka situationer tvångsmedlet bör få användas samt vem åtgärden bör få riktas mot, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Det finns redan i dag en möjlighet att använda det nya tvångsmedlet hemlig dataavläsning för att utreda vem som skäligen kan misstänkas för brottet. Möjligheten gäller enbart dataavläsning som avser kommunikationsövervakningsuppgifter och platsuppgifter (5 § lagen [2020:62] om hemlig dataavläsning). Det handlar alltså om samma slags uppgifter som kan omfattas av hemlig övervakning av elektronisk kommunikation enligt 27 kap. 20 § andra stycket rättegångsbalken, RB. Hemlig dataavläsning kan även avse bl.a. kommunikationsavlyssningsuppgifter (2 § första stycket 1 lagen om hemlig dataavläsning). Det är då fråga om samma slags uppgifter som man kan få tillgång

till genom en hemlig avlyssning av elektronisk kommunikation enligt 27 kap. 18 § RB. Syftet med införandet av tvångsmedlet hemlig dataavläsning var bl.a. att kompensera för att hemlig avlyssning av elektronisk kommunikation blivit mindre effektivt på grund av kryptering m.m. Regeringen har uttalat att det är av väsentlig betydelse att hemlig dataavläsning kan användas i motsvarande fall som de befintliga hemliga tvångsmedlen, eftersom det annars finns en risk för att vissa allvarliga brott inte kan utredas när det visar sig vara omöjligt att använda befintliga hemliga tvångsmedel (se prop. 2019/20:64 s. 124). Hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter bör därför omfattas av våra överväganden. Vi anser det även lämpligt att överväga om det bör vara möjligt med hemlig dataavläsning avseende uppgifter som finns lagrade i eller som visar hur ett avläsningsbart informationssystem används, se avsnitt 9.11. Däremot överväger vi inte om möjligheten att använda hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet bör omfatta kameraövervakningsuppgifter eller rumsavlyssningsuppgifter.

9.2 Gällande rätt

9.2.1 De hemliga tvångsmedlen

En redogörelse för gällande rätt finns i avsnitt 4.3 och 4.4. Här redovisas därför endast sådant som är av särskild relevans för överväganden i detta kapitel.

Förutsättningarna för att i en förundersökning använda hemlig avlyssning av elektronisk kommunikation framgår av 27 kap. 18 och 20 §§ RB. Det krävs till att börja med alltid att någon är skäligen misstänkt för brottet. Vidare krävs det att åtgärden är av synnerlig vikt för utredningen. Det framgår inte av lagtexten vem åtgärden får riktas mot. Begränsningarna gäller i stället det telefonnummer eller den adress eller elektroniska kommunikationsutrustning som åtgärden avser. Av 20 § framgår att åtgärden enbart får riktas mot ett telefonnummer eller en adress eller elektronisk kommunikationsutrustning som under den tid som tillståndet avser innehas eller har innehavts av den misstänkte (första stycket 1) eller annars kan antas ha använts eller komma att användas av den misstänkte, eller som det finns synnerlig anledning att anta att den misstänkte har kontaktat eller kommer att kontakta (första stycket 2). Reglerna om koppling mellan den

enskilde och en teknisk utrustning finns till för att skydda integriteten och rättssäkerheten och ska minska risken för att personer som är ovidkommande för utredningen drabbas av åtgärderna (se t.ex. prop. 1988/89:124 s. 46). Vid tvångsmedelsanvändning enligt andra punkten anses tvångsmedlet rikta sig mot den misstänkte och inte mot innehavaren av telefonnumret (prop. 2002/03:74 s. 38 f.).

Av det sagda följer att ett telefonnummer eller en annan adress eller en kommunikationsutrustning måste kunna knytas till en skäligen misstänkt för att en brottsbekämpande myndighet ska få tillstånd att avlyssna numret, adressen eller utrustningen. Något absolut krav på att personen ska vara identifierad med namn torde inte finnas, men enligt JO-uttalanden ska den misstänkte ändå kunna identifieras så att förväxlingsrisk praktiskt tagen är utesluten (JO 2006/07 s. 30). Däremot kan det, med stöd av 27 kap. 20 § första stycket 2, vara möjligt att ge tillstånd till hemlig avlyssning på den grunden att den misstänkte kan antas kontakta en okänd persons telefonnummer, adress eller kommunikationsutrustning.

Det finns inte någon möjlighet att använda hemlig avlyssning av elektronisk kommunikation om det inte finns någon som skäligen kan misstänkas för brottet. En sådan möjlighet finns däremot enligt 27 kap. 20 § andra stycket RB i fråga om hemlig övervakning av elektronisk kommunikation. Det krävs då att brottet är sådant att hemlig avlyssning av elektronisk kommunikation är tillåten, och att åtgärden är av synnerlig vikt för utredningen. Uppgifter om meddelanden får endast avse förfluten tid. En närmare redogörelse för regleringen och de överväganden som gjorts om den finns i avsnitt 8.3 och 8.4.

Även hemlig dataavläsning är tillåten i syfte att utreda vem som skäligen kan misstänkas för brottet. Dock får dataavläsningen då enbart avse kommunikationsövervakningsuppgifter avseende förfluten tid och platsuppgifter, dvs. samma slags uppgifter som man kan få tillgång till genom en hemlig övervakning av elektronisk kommunikation. Vidare gäller vissa ytterligare begränsningar angående kopplingen mellan det avlästa informationssystemet och brottet som vi har redogjort för i avsnitt 8.3.2.

Om det inte finns någon som är skäligen misstänkt för brottet, får hemlig kameraövervakning användas för att övervaka den plats där brottet begåtts eller en nära omgivning till denna plats (27 kap. 20 c § första stycket RB). Syftet med åtgärden får enbart vara att fastställa vem som skäligen kan misstänkas för brottet och åtgärden

måste vara av synnerlig vikt för utredningen (andra stycket i samma paragraf).

Med undantag för de fall som beskrivits här måste det finnas en skäligen misstänkt för att ett hemligt tvångsmedel ska kunna användas under en förundersökning.

9.2.2 Om tvångsåtgärder mot andra än den misstänkte

I avsnitt 8.3.3 finns en redogörelse för möjligheterna att använda tvångsåtgärder i straffprocessuella förfaranden mot andra än den misstänkte. Det som sägs där är relevant även för de frågor som behandlas i detta kapitel och vi hänvisar därför till den framställningen.

9.3 Tidigare överväganden

I regeringens proposition om vissa tvångsmedelsfrågor (prop. 1988/89:124) övervägdes det i enlighet med förslag av Narkotikakommissionen om kravet på misstankens styrka för hemlig telefonavlyssning (numera hemlig avlyssning av elektronisk kommunikation) skulle sänkas och tvångsmedlet kunna tillgripas på ett tidigare utredningsstadium. Det framhålls att det i vissa fall skulle vara till fördel för brottsutredningen, om avlyssning kunde sättas in på ett tidigare stadium. Samtidigt konstaterades att man med en sänkt misstankegrad skulle öka risken för att avlyssning äger rum i fall där brottsmisstanken visar sig obefogad och avlyssningen rikta sig mot en oskyldig. Denna risk kan naturligtvis aldrig elimineras, men det ansågs att den i görligaste mån bör begränsas. I likhet med en stor majoritet av remissinstanserna ansågs det att främst integritetsaspekterna bör ges störst tyngd vid avvägningen och att hemlig teleavlyssning således även i fortsättningen borde få användas endast mot den som är skäligen misstänkt för brottet. Ställningstagandet överensstämde med den uppfattning som redovisades av den parlamentariska nämnden i Wennerströmaffären (SOU 1968:4) och av utredningen om telefonavlyssning (SOU 1975:95).

Bestämmelsen om hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet infördes i enlighet med förslag i propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation (prop. 2011/12:55). Vad som sades där har vi redovisat i avsnitt 8.4.

I propositionen finns det inga överväganden om hemlig avlyssning av elektronisk kommunikation i sådant syfte.

Bestämmelsen om hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet infördes i enlighet med förslag i propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 124 och 125). Regeringen angav då att möjligheten kan ge viktiga upplysningar när det har begåtts ett allvarligt brott men där det inte går att hitta någon misstänkt. I propositionen diskuteras även om det borde införas en möjlighet att hämta in kameraövervakningsuppgifter i syfte att fastställa vem som skäligen kan misstänkas för brottet. Regeringen konstaterade att sådan kameraövervakning som enligt rättegångsbalken får användas för att identifiera en misstänkt endast får avse den plats där brottet har begåtts eller en nära omgivning till denna plats. Sådana fall kan t.ex. vara när ett parti med narkotika hittas på en viss plats. Då kan en kamera monteras på platsen för att iaktta vilka som besöker den. Behovet av hemlig dataavläsning i ett sådant fall, eller andra fall där hemlig kameraövervakning får användas för att identifiera en misstänkt, bedömdes inte som särskilt stort. Regeringen lämnade därför inget förslag om en sådan möjlighet. Regeringen avvisade också ett förslag från Säkerhetspolisen om att de brottsbekämpande myndigheterna skulle få använda hemlig dataavläsning för att ta upp rumsavlyssnings- och kameraövervakningsuppgifter för att kunna identifiera en person. Förslagen ansågs innebära en inte obetydlig utvidgning av vad som är rättsligt möjligt och regeringen såg problem både vad gäller integritetsintrånget och möjligheten att säkerställa att åtgärden uppfyller det platskrav som ställs på rumsavlyssningsuppgifter. Några överväganden om en möjlighet att hämta in kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet redovisades inte.

Även om bestämmelserna om hemlig kameraövervakning inte omfattas av våra direktiv i denna del är det av visst intresse att redogöra för vad som uttalats i förarbetena om möjligheten att använda hemlig kameraövervakning i syfte att fastställa vem som skäligen kan misstänkas för brottet. Denna möjlighet infördes i enlighet med förslag i propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering (prop. 2002/03:74). Åtgärden kan endast avse den plats där brottet begåtts eller en näraliggande plats. Den ska vidare syfta till att man ska kunna *fastställa* vem som skäligen kan misstänkas. Enligt förarbetena till bestämmelsen innebär detta rekvisit

att övervakningen i allmänhet ska vara avsedd att leda till att gärningsmannen kan påträffas på bar gärning (prop. 2002/03:74 s. 40 f.).

9.4 Utgångspunkter

Bedömning: Om det införs en reglering om hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas, bör den innehålla en tydlig avgränsning i fråga om vilka telefonnummer, andra adresser och kommunikationsutrustningar respektive avläsningsbara informationssystem som åtgärden får avse.

Skälen för bedömningen

I kapitel 8 har vi gjort bedömningen att det inte är nödvändigt eller lämpligt att i lagtexten ange vilka personkategorier som en hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas kan avse. Samma bedömning gjordes i fråga om hemlig dataavläsning avseende kommunikationsövervaknings- och platsuppgifter i samma syfte. Hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning av kommunikationsavlyssningsuppgifter utgör typiskt sett ett större intrång i den personliga integriteten. Vi bedömer att det varken är godtagbart eller nödvändigt med en reglering som tillåter motsvarande flexibilitet i fråga om de tvångsmedel som nu är aktuella (jfr bl.a. Europadomstolens avgöranden i Roman Zacharov mot Ryssland och Iordachi mot Moldavien). Regleringen bör därför, om den ska införas, tydligt begränsas till de fall där det framstår som allra mest angeläget och därtill acceptabelt från integritetssynpunkt med en möjlighet att använda tvångsmedlet i syfte att utreda vem som skäligen kan misstänkas. Eftersom åtgärden, som vi utvecklar i det följande, behöver kunna riktas mot en person som man inte har identifierat är det nödvändigt att en möjlighet till hemlig avlyssning, om den ska införas, avser inte en viss person, utan ett visst telefonnummer, en adress eller en kommunikationsutrustning. På motsvarande sätt är det nödvändigt att en eventuell möjlighet till hemlig dataavläsning avser ett avläsningsbart informa-

tionssystem. Detta är även i överensstämmelse med hur regelverket i övrigt är utformat (se t.ex. 27 kap. 20 § första stycket RB och 4 § andra och tredje styckena samt 5 § andra stycket lagen om hemlig dataavläsning).

9.5 Det finns ett behov

Bedömning: Det finns ett påtagligt behov av en möjlighet att utföra hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas.

Skälen för bedömningen

Telefonnummer m.m. som inte kan knytas till en person

En vanlig situation i den brottsutredande verksamheten är att man har kännedom om att en person som förfogar över exempelvis ett visst telefonnummer gör sig skyldig till brott, men att man inte vet vem denna person är. Att situationen är vanlig hänger bl.a. samman med att många kriminella använder sig av oregistrerade kontantkort och dessutom ofta byter telefon och nummer (se prop. 2019/20:145 Ett förenklat förfarande vid vissa beslut om hemlig avlyssning, s. 15 och 16 och Ds 2020:12 s. 59–63). Syftet är många gånger att försvåra för de brottsbekämpande myndigheterna att kunna avlyssna eller övervaka elektronisk kommunikation. Det är inte möjligt att besluta om hemlig avlyssning av elektronisk kommunikation om den skäligen misstänkte inte är identifierad på ett sådant sätt att förväxlingsrisk i princip är utesluten. Som kommer att utvecklas i detta och följande avsnitt är situationen även vanlig när någon annan form av elektronisk kommunikation utnyttjas vid brottsligheten.

Ett exempel på det angivna är bedrägerier eller utpressning som begås över telefon eller genom någon annan form av elektronisk kommunikation. Det kan många gånger vara känt vilket telefonnummer eller vilken elektronisk adress som kontaktat målsäganden eller målsägandena, men utan att numret eller adressen kan kopplas till en viss person. Det kan t.ex. röra sig om ett oregistrerat kontantkort, ett utländskt kontantkort eller ett kort som används av någon annan än

den som registrerat det. En möjlighet att kunna avlyssna numret fastän det inte kan knytas till en skäligen misstänkt person skulle avsevärt kunna förbättra möjligheterna att utreda och få fram bevisning som kan leda fram till identifiering av en skäligen misstänkt. Här kan man t.ex. nämna s.k. vishingbedrägerier[1], som syftar till att få brottsoffret att lämna ut personlig information som gärningspersonerna sedan kan använda för att få tillgång till exempelvis offrets bankkonton. I vissa fall kan gärningspersonerna kontakta en och samma målsägande upprepade gånger under en längre tidsperiod.

Ytterligare sådana exempel är grovt penningtvättsbrott och det näraliggande brottet näringspenningtvätt, grovt brott. Exempel på det senare kan illustreras enligt följande. Näringspenningtvätt, grovt brott förekommer bl.a. i hawalaverksamheter[2] av olika omfattning. I ärendet kan man påträffa en telefon som går att koppla till verksamheten och som i sin tur har haft frekvent kontakt med en annan telefon som de brottsbekämpande myndigheterna inte kan koppla till någon identifierad person. Det kan då vara mycket angeläget att få en identitet knuten till den sistnämnda telefonen för att hitta den verklige huvudmannen. Liknande situationer går att hitta i utredningar mot olika växlingskontor, där det kan finnas en eller flera skäligen misstänkta, men där det är tydligt att det finns andra och kanske viktigare personer som behöver identifieras bakom kända telefonnummer.

Ytterligare ett exempel kan vara att det under en avlyssning mot en skäligen misstänkt framkommer i samtal med en okänd person att denna person är i färd med att hantera en stor mängd narkotika som han eller hon förvarar hos sig. En hemlig avlyssning mot det nummer som den okända personen använder skulle då kunna bidra till att identifiera honom eller henne och därmed till att man kan lokalisera förvaringsplatsen för narkotikan.

Ett annat exempel är att man i samband med s.k. kontrollerad leverans känner till ett telefonnummer som transportören är i kontakt med och som man kan misstänka är inblandat i brottet men där man inte vet identiteten på personen.

[1] Vishing är en förkortning av voice phishing.
[2] Hawala är ett informellt valutaväxelkontor byggt på ett brett nätverk av växelkontor i främst Mellanöstern, Afrika och Asien. Systemet används bl.a. för att föra över pengar till utlandet och transaktionen sker ofta utan någon skriftlig dokumentation av överföringen.

Ytterligare ett exempel kan vara utredningar om pågående människorov där målsägandens anhöriga inte vill medverka i utredningen, men där de brottsbekämpande myndigheterna vet vilket nummer som de okända misstänkta använder i kontakten med de anhöriga.

Regeringen har i lagrådsremissen Registrering av kontantkort och tydligare regler om utlämnande av uppgifter om elektronisk kommunikation föreslagit en registreringsskyldighet för vissa förbetalda tjänster som kan nås via till exempel kontantkort. Den som tillhandahåller en förbetald tjänst ska enligt förslaget registrera uppgifter om abonnenten och kontrollera abonnentens identitet innan tjänsten börjar användas. Om en förbetald tjänst används av någon annan än den registrerade abonnenten ska tjänsten som huvudregel avbrytas. Om förslagen genomförs kan det leda till en minskning av de olägenheter för brottsbekämpningen som följer av användningen av oregistrerade kontantkort. Samtidigt måste man räkna med att kriminella i vissa fall kan hitta vägar runt registreringskravet, t.ex. genom att låta s.k. målvakter registrera abonnemanget eller genom att använda utländska oregistrerade kontantkort (jfr Ds 2020:12 s. 75–77). En möjlighet att avlyssna ett visst telefonnummer fastän det är osäkert om innehavaren av abonnemanget även är den person som använder numret för brottslig verksamhet i syfte att utreda vem som skäligen kan misstänkas skulle därför ändå kunna vara av stort värde.

Internetrelaterade sexualbrott

Ett annat exempel är sexualbrott som begås på distans via en dator eller telefon. Gärningspersonen, som kan vara anonym för målsäganden eller uppträda under en stulen eller uppdiktad identitet, kan i ett sådant fall förmå målsäganden att utsätta sig själv för grova sexuella handlingar. Tvånget kan exempelvis bestå i hotelser om att målsäganden eller målsägandens familj ska skadas eller dödas, att bilder av sexuell karaktär ska läggas upp på pornografiska hemsidor eller att gärningsmannen ska sprida uppgifter om att målsäganden säljer sex. Brottet kan rikta sig mot vuxna, men barn är särskilt sårbara för detta slags övergrepp. Förövare som ägnar sig åt denna sorts brottslighet har ofta många offer som utsätts för likartade övergrepp. Av Högsta domstolens praxis framgår att en handling bestående i att en person förmår någon annan att onanera via webbkamera är att bedöma

som en sexuell handling. Likaså är det klarlagt att det är möjligt att genomföra en sexuell handling med en annan person även på distans, via t.ex. internet. (Se NJA 2015 s. 501). Beroende på omständigheterna kan det vara fråga om bl.a. sexuellt utnyttjande av barn enligt 6 kap. 6 § brottsbalken eller utnyttjande av barn för sexuell posering enligt 6 kap. 8 §. En sexuell handling som går ut på att barnet förmås att göra något med sig själv ska bedömas som våldtäkt mot barn, om handlingen innebär en lika allvarlig kränkning som ett samlag. Så ansågs vara fallet i två avgöranden som HD meddelade den 17 november 2021 (mål nr 4072-21 och 4645-21) som rör fall där gärningspersonen på distans förmått målsäganden att penetrera sig själv med fingrar respektive föremål. Det skulle kunna vara av stor betydelse för möjligheten att utreda vem som skäligen kan misstänkas för brottet och i förlängningen få till stånd en fällande dom mot gärningspersonen om det fanns en möjlighet att avlyssna det nummer eller den andra adress som kontaktat målsäganden, fastän numret eller adressen inledningsvis inte kan knytas till en viss person

I många ärenden om internetrelaterade sexuella övergrepp mot barn uppstår misstanken initialt då det påträffas en fil som innehåller dokumenterade sexuella övergrepp mot barn. Brottsmisstanken kan gälla barnpornografibrott eller, beroende på omständigheterna, något brott enligt 6 kap. brottsbalken, såsom våldtäkt mot barn. En utredning som initialt handlar om barnpornografibrott kan senare visa sig handla om ett sexualbrott mot barn. I många fall är det okänt vem målsäganden är och någon som skäligen kan misstänkas för brottet finns inte. Många gånger är situationen densamma som vid komplexa cyberbrott, dvs. att man har kunskap om exempelvis en server men inte vem som ligger bakom. Det finns därför enligt de brottsbekämpande myndigheterna ett behov av en möjlighet att avlyssna eller rikta en hemlig dataavläsning mot servern trots att den inte kan knytas till en skäligen misstänkt. Utredningssvårigheterna i detta slags ärenden har utvecklats i avsnitt 7.4. och 7.5.

Komplex it-brottslighet

Som framgått i avsnitt 7.4 har de brottsbekämpande myndigheterna lyft fram komplexa cyberbrott som ett område där man i dag brottas med stora utredningssvårigheter. En del av problemet är att det regel-

mässigt saknas en skäligen misstänkt person och att dagens reglering inte tillåter inhämtning i realtid av uppgifter om meddelanden i dessa fall (27 kap. 20 § andra stycket RB) och inte heller hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter. Cyberbrottslighet är gränslös och det är vanligt förekommande att förövare och grupperingar sitter utspridda i olika länder och samverkar genom lager av servrar som kommunicerar med varandra. Det är kännetecknande för detta slags brott att gärningspersonerna använder en komplex infrastruktur som gör det mycket svårt för myndigheterna att jobba sig igenom de olika lagren. Ofta finns ingen annan ingång i ärendet än de noder (t.ex. en server) i en infrastruktur som den bakomliggande grupperingen agerat ifrån. Då är hemlig övervakning av elektronisk kommunikation i realtid eller hemlig avlyssning alternativt hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter ofta en förutsättning för att man ska komma vidare i utredningen. Det är nämligen så man får vidare uppslag för att närma sig en identifiering av gärningspersonerna bakom. Enligt de brottsbekämpande myndigheterna lyckas länder som har dessa möjligheter bättre med att lagföra och avbryta brottslighet av det aktuella slaget. Myndigheterna har anfört att avsaknaden av den möjligheten i Sverige gör att man inte kommer vidare i komplexa cyberbrottsutredningar och inte heller kan biträda andra länder i deras utredningar om allvarlig brottslighet. Detta kan leda till att kriminella väljer att placera den infrastruktur som används vid allvarlig och komplex cyberbrottslighet i Sverige, eftersom det uppfattas som riskfritt.

De komplexa cyberbrotten kan vara av olika slag. Typiska exempel är ransomwareattacker, dataintrång från sofistikerade hotaktörer och brottslighet på darknet. Ransomwareattacker har beskrivits närmare i avsnitt 7.5. Vid utredning av dessa brott försöker man i snabb takt undersöka målsägandens drabbade it-system för att identifiera uppslag att gå vidare med. Det kan exempelvis vara ip-nummer som finns i loggar eller servrar som lämnat avtryck på annat sätt. Lyckas man identifiera angriparens ip-adress så blir det genast aktuellt att begära ut serverkopior från denna. Här skiljer sig våra svenska möjligheter från flera andra länders genom att man här endast kan begära

en kopia av servern medan flera andra länder[3] även kan bedriva avlyssning mot servern för att kunna hitta vägen vidare i de kriminellas infrastruktur eller i bästa fall genom denna kunna identifiera en kriminell aktör som kopplar upp sig mot enheten. De brottsbekämpande myndigheterna har anfört att en möjlighet till hemlig avlyssning mot en sådan server avsevärt skulle förbättra möjligheterna att utreda brotten och även att biträda andra länder i deras utredningar. Ett exempel på behovet av det sistnämnda är en nyligen inträffad situation där den irländska sjukvården blev drabbad av ransomware, vilket slog ut stora delar av dess verksamhet och fick långvariga konsekvenser. De irländska myndigheterna hittade spår som pekade mot att de kriminella använt en server belägen i Sverige för att genomföra sin attack. En begäran om rättslig hjälp skickades därför till Sverige med begäran om att avlyssna denna server för att kunna följa trafiken och förhoppningsvis därmed kunna identifiera gärningspersonerna. Begäran fick avslås eftersom svensk rätt inte tillåter sådan avlyssning om det inte finns en skäligen misstänkt.

Ett annat exempel är synnerligen grova narkotikabrott på darknet, där de brottsbekämpande myndigheterna har identifierat de servrar där narkotikaförsäljningen sker. I dessa fall finns ingen som skäligen kan misstänkas för brott och det enda sättet att på ett effektivt sätt komma vidare i utredningen och identifiera skäligen misstänkta personer är att avlyssna datatrafiken till och från dessa servrar.

De brottsbekämpande myndigheterna har anfört att alla de länder som lyckas bäst med it-brottsutredningar kan använda sig av hemliga tvångsmedel mot enheter för att söka ännu okända personer. I kontrast kan man konstatera att ingen svensk utredning om en ransomware hittills har lett till åtal.

Personer som är försvunna, avlidna eller okontaktbara

Det förekommer fall där målsäganden är försvunnen, medvetslös eller död och hans eller hennes telefon inte har återfunnits eller man inte kan få tillgång till innehållet på grund av lösenord eller av någon

[3] Enligt uppgift från representanter från Joint Cybercrime Action Taskforce (J-CAT) vid Europol finns det i ett flertal europeiska länder möjlighet att avlyssna elektronisk infrastruktur såsom en server fastän det inte finns en skäligen misstänkt i en cyberbrottsutredning. Exempel på sådana länder är Norge, Tyskland, Italien, Frankrike, Nederländerna, Polen och Belgien. Villkoren för att åtgärden ska få vidtas varierar. Av svaren framgår att möjligheten har varit avgörande i många omfattande utredningar av komplex cyberbrottslighet.

annan anledning. Ett exempel kan vara ett pågående människorov, där ett visst nummer vars användare är okänd har varit i kontakt med målsägandens telefon. Förutsatt att man genom t.ex. hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning fått fram uppgifter om vilka telefonnummer eller andra adresser som målsäganden varit i kontakt med, skulle man kunna rikta en hemlig avlyssning mot intressanta nummer eller adresser i syfte att få fram information om vem som använder dem och i bästa fall avbryta brottet. Ett annat exempel kan vara utredningar om mord där det inte finns en skäligen misstänkt. En möjlighet till hemlig avlyssning av elektronisk kommunikation riktad mot nummer som kontaktat målsäganden skulle i ärenden av det angivna slaget kunna avsevärt förbättra möjligheterna att utreda brottet.

Det kan även förekomma att en person har avlidit till följd av ett brott och att det hade varit värdefullt att kunna avlyssna hans eller hennes elektroniska kommunikation. Det kan i vissa fall vara uppenbart att den som avlidit är skäligen misstänkt, eller åtminstone en av flera gärningspersoner. Ett exempel på det kan vara att en terrorist spränger sig själv till döds, eller en skjutning mellan gängkriminella grupperingar där någon som avfyrat skott själv blir skjuten till döds av motståndarsidan. Det kan i sådana fall finnas ett starkt intresse av att man kan avlyssna den dödes telefon i syfte att snabbt utreda om han eller hon haft några medhjälpare som fortfarande är i livet.

I andra fall är det oklart om personen som avlidit är ett brottsoffer eller en gärningsperson, eller båda delar. De brottsbekämpande myndigheterna har som exempel tagit upp ett ärende där en bil sprängdes på grund av sprängmedel som fanns i bilen. Ett antal vuxna och ett litet barn dog i explosionen. Personer som färdades i bilen hade kopplingar till grov kriminalitet, och det var oklart om de transporterade sprängladdningen i syfte att använda den i eget kriminellt syfte eller om de var utsatta för ett attentat. Oavsett om det förhöll sig på det ena eller det andra sättet fanns det stark anledning att anta att det fanns andra personer som var inblandade. Det inleddes en förundersökning om förberedelse till allmänfarlig ödeläggelse. Genom en hemlig övervakning av elektronisk kommunikation mot de avlidnas telefoner som syftade till att utreda vem som skäligen kunde misstänkas för brottet kunde man utreda vilka telefonnummer som de avlidna varit i kontakt med före brottet. De uppgifter man fick fram var dock inte tillräckliga för att grunda skälig misstanke mot någon. En an-

sökan om att utföra hemlig avlyssning av de avlidnas telefoner avslogs av både tingsrätten och hovrätten. Hovrätten angav i sin motivering att det ligger i sakens natur att misstankarna om brott ska riktas mot någon som är i livet och som kan bli lagförd. Högsta domstolen meddelade inte prövningstillstånd. De brottsbekämpande myndigheterna har anfört att en hemlig avlyssning av elektronisk kommunikation, t.ex. genom innehållet i skickade sms, hade kunnat påvisa kopplingar till andra inblandade personer. Det skulle ha kunnat handla om personer som haft inblandning i det dåd som sprängmedlen egentligen varit avsedda för eller som kunde ha placerat sprängmedlen i bilen i avsikt att attackera de personer som färdades i den.

Personer som inte medverkar

Det kan också finnas fall där det finns personer som bevittnat brottet eller annars kan antas ha information om brottet, men som inte berättar vad de vet för polisen. En möjlighet att rikta en avlyssning mot sådana personer i syfte att utreda vem som skäligen kan misstänkas, skulle i vissa fall kunna leda till att en skäligen misstänkt kan identifieras. Ett exempel kan här vara att polisen påträffar flera personer på en mordplats, och det finns skäl att misstänka att åtminstone någon av personerna på platsen i förväg har vetat vad som skulle hända, eller till och med har lurat målsäganden till platsen för att mordet skulle kunna utföras. Ett annat exempel är svårutredda mordfall där det finns anledning att tro att efterlevande vet mer än de delar med sig av till polisen. Efterlevande har inte med automatik ställning som målsägande men om någon har blivit dödad genom brott har vissa efterlevande samma rätt som målsägande att ange brottet eller föra talan om det (20 kap. 13 § första stycket RB). Det finns exempel från verkligheten där det hade varit av värde att exempelvis kunna avlyssna en efterlevandes telefon i syfte att utreda vem som skäligen kan misstänkas för mordet. Ett sådant exempel är ett fall som började med att en person först skottskadades och sedan avrättades av de gärningsmän som skjutit honom. Utredningen i ärendet ledde till att några personer frihetsberövades medan det saknades tillräcklig bevisning mot vissa andra personer, som man därför inte kunde frihetsberöva eller vidta några andra åtgärder mot. Dessa personer valde då att attackera ett vittne vilket ledde till att ytterligare två personer dog. Förundersök-

ningen visade till sist att gärningsmännen hade vuxit upp tillsammans med och var kamrater med det första offret och dennes bror. Enligt polisens bedömning hade man troligen kunnat komma snabbare fram i utredningen och kanske även kunnat förhindra de senare morden om man kunnat avlyssna den efterlevande broderns telefon. Brodern gjorde nämligen egna efterforskningar om gärningsmännens identitet genom sina kontakter och sannolikt berättade han enligt polisen inte om allt när han förhördes.

Det finns ett behov

I de fall som vi tagit upp i det föregående finns det ofta en möjlighet att genom exempelvis hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning få fram ett telefonnummer eller annan adress som man kan misstänka att används av gärningspersonen, exempelvis på grund av att numret varit i kontakt med målsäganden före brottet eller används för att i ett människorovsärende pressa pengar av målsägandens anhöriga. I ett sådant fall bedömer vi att det finns ett påtagligt behov av en möjlighet att rikta en hemlig avlyssning mot detta telefonnummer eller denna adress, även om det är okänt vem innehavaren är eller om flera personer brukar numret eller adressen, och då i syfte att utreda vem som kan skäligen misstänkas för brottet.

Polismyndigheten har uppgett att det i ärenden med våldsinslag, och särskilt sådana som angår särskilt utsatta områden, är vanligt att både målsäganden och anhöriga till målsäganden är ovilliga att berätta om händelsen. Det är alltså enligt polisen vanligt att dessa personer avstår från att berätta om olika detaljer, vilket gör ärendena svåra att utreda. En möjlighet att avlyssna telefoner eller andra adresser eller kommunikationsutrustning som kan kopplas till personer ur denna krets hade därför enligt våra uppgiftslämnare kunnat leda till att fler sådana brott hade kunnat utredas och till att utredningarna gått snabbare. Särskilt i fall där det är fråga om en pågående konflikt kan snabbhet vara avgörande för att man ska kunna förhindra ytterligare grova våldsdåd. Med hänsyn till det anförda bedömer vi att det i och för sig finns ett behov av en möjlighet till hemlig avlysning mot personer ur den nu aktuella kretsen i syfte att utreda vem som skäligen kan misstänkas för brottet. Som framgått under föregående rubriker finns det även andra situationer där det finns starka skäl att miss-

tänka att personer som bevittnat brottet eller annars kan antas ha information om det inte berättar vad de vet eller lämnar felaktiga uppgifter. I vissa fall kan det vara oklart om personerna i fråga är vittnen, målsägande eller i själva verkat har medverkat till brottet. Även i sådana fall kan det vara av stort värde för möjligheten att utreda vem som skäligen kan misstänkas för brottet att kunna avlyssna dessa personers telefoner, eller nummer som varit i kontakt med dem.

Vi bedömer även att det finns ett behov av en möjlighet att kunna rikta en hemlig avlyssning mot exempelvis ett telefonnummer som kan kopplas till en avliden person i syfte att utreda vem som skäligen kan misstänkas för ett visst brott. Det kan handla både om fall där man på goda grunder kan anta att den döde är gärningsperson men att det kan finnas medverkande som fortfarande lever, fall där målsäganden har avlidit till följd av brottet och fall där det är osäkert om den döda personen är misstänkt eller målsägande.

Som tidigare nämnts är det vidare vanligt att kriminella ofta byter nummer och telefoner, just i syfte att försvåra för de brottsbekämpande myndigheterna att övervaka eller avlyssna deras kommunikation (se prop. 2019/20:145 s. 15 och 16). Detta kan göra det mycket svårt att utreda exempelvis grova vishingbedrägerier och pågående grov utpressning, där en målsägande kontaktas upprepade gånger av samma personer men från olika nummer. Om det i ett sådant fall hade varit tillåtet att avlyssna målsägandens telefon skulle man i bästa fall höra om det är samma uppringare varje gång samt få dennes nya nummer för att kunna avlyssna detta. Från bevissynpunkt är det vidare värdefullt med inspelade samtal eftersom de inspelade rösterna kan jämföras med de misstänktas.

I en hel del fall är hemlig avlyssning av elektronisk kommunikation inte en framkomlig väg på grund av exempelvis kryptering. Det kan då t.ex. förhålla sig så att man visserligen får tillgång till den information som överförs, men att innehållet inte är läsligt i klartext. I många sådana fall skulle det vara möjligt att få tillgång till samma information i läsbar form om man i stället använder hemlig dataavläsning som avser kommunikationsavlyssningsuppgifter. De situationer som tagits upp i det föregående är i allt väsentligt relevanta även när det gäller hemlig dataavläsning. Som exempel på fall där just hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter kan vara den enda vägen framåt i utredningen är synnerligen grovt narkotikabrott genom storskalig försäljning av narkotika på Darknet. Någon annan möjlig-

het än hemlig dataavläsning för att identifiera gärningspersonen är i sådana fall svår att föreställa sig. Endast genom den åtgärden kan det vara möjligt att få del av kommunikationen i okrypterad och alltså läsbar form. Vi bedömer med hänsyn till det anförda att det även finns ett behov av en möjlighet att utföra hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet.

9.6 Personkretsen för hemlig avlyssning

9.6.1 Någon som kan misstänkas

Bedömning: En eventuell reglering om hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas bör kunna avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som under tid som tillståndet avser

1. kan antas innehas eller ha innehafts av någon som kan misstänkas ha begått eller annars medverkat till brottet, eller
2. som annars kan antas ha använts eller komma att användas av en sådan person.

Skälen för bedömningen

En av de situationer som lyfts fram under vårt arbete är att utredningen ger vid handen att exempelvis ett visst telefonnummer används för att begå brott, men att man inte vet vem som innehar eller använder numret. Om innehavaren eller användaren, dvs. den misstänkte, inte är identifierad på ett sådant sätt att förväxlingsrisk är utesluten anses det inte tillåtet att fatta ett beslut om hemlig avlyssning (se avsnitt 9.2.1). Enligt de brottsbekämpande myndigheterna är situationer av detta slag vanliga i den brottsutredande verksamheten och det är enligt vår mening ytterst angeläget att regleringen gör det möjligt med hemlig avlyssning av elektronisk kommunikation alternativt en hemlig dataavläsning i syfte att man ska kunna identifiera användaren och därmed den skäligen misstänkte.

Två regleringsalternativ

En lösning skulle kunna vara en bestämmelse som gör det möjligt att avlyssna ett telefonnummer etc. som har använts vid ett brott. Lösningen ligger nära regleringen om hemlig dataavläsning. Vid hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet är det nämligen tillåtet att avläsa bl.a. ett avläsningsbart informationssystem som har använts vid ett brott eller i anslutning till en brottsplats vid brottstidpunkten (5 § andra stycket lagen om hemlig dataavläsning). Av förarbetena (propositionen Hemlig dataavläsning, prop. 2019/20:64 s. 219) framgår att kravet på att informationssystemet har använts vid ett brott innebär att informationssystemet ska ha haft avgörande betydelse vid själva genomförandet av brottet eller ha använts för att understödja brottet. Som exempel på ett fall där tillstånd till hemlig dataavläsning kan ges nämns fallet att polisen inom ramen för en förundersökning om t.ex. grovt narkotikabrott upptäcker en viss ip-adress varifrån det har förmedlats stora mängder narkotika. Man kan tänka sig en liknande reglering när det gäller hemlig avlyssning av elektronisk kommunikation. Lösningen skulle innebära att man frikopplar åtgärden från en viss person och i stället helt riktar in den på ett nummer, en adress eller kommunikationsutrustning som använts för att utföra eller understödja brottet. Med en sådan reglering skulle man kunna använda hemlig avlyssning av elektronisk kommunikation för att utreda vem som skäligen kan misstänkas för brottet i många av de fall som de brottsbekämpande myndigheterna uppmärksammat.

Denna lösning har flera fördelar. Den innebär ett tydligt krav på koppling mellan telefonnumret etc. och brottet. Som nyss sagts kan åtgärden förväntas vara effektiv i många fall. Samtidigt måste det framhållas att den är förknippad med integritetsrisker, som kan variera beroende på vad avlyssningen riktar sig mot. Om det gäller ett mobiltelefonnummer som använts vid ett brott torde risken för att numret används av andra, för utredningen ovidkommande personer, vara relativt begränsad. Om det handlar om en ip-adress eller en server som används av flera är riskerna större. Detta skiljer sig dock inte principiellt från vad som gäller enligt dagens reglering i 27 kap. 20 § första stycket RB. Det följer redan av dagens reglering att det ska göras en noggrann proportionalitetsbedömning i varje enskilt fall, och att tillståndet till åtgärden ska förenas med villkor för att tillgodose intres-

set av att enskildas personliga integritet inte kränks i onödan, när det finns skäl till det.

En annan tänkbar lösning skulle vara att man gör det möjligt att avlyssna ett telefonnummer etc. som har anknytning till någon som kan misstänkas för brottet. Uttrycket ”kan misstänkas” är den lägsta misstankegrad som förekommer i fråga om straffprocessuella tvångsmedel. Uttrycket anses av vissa innebära att beviskravet är uppfyllt om personen i fråga är skyldig i 10 av 100 likadana bevissituationer, och av andra att beviskravet innebär en säkerhet på 10–20 procent (Ekelöf, SvJT 1982 s. 656 respektive Bring & Diesen, s. 160). Beviskravet är så lågt att det innebär att det är fullt möjligt att flera personer kan misstänkas för samma brott (Bring & Diesen, s. 158). Som sagts tidigare bör det inte för tillämpning av bestämmelsen ställas något krav på att personen är identifierad. Däremot bör det – om detta regleringsalternativ väljs – krävas ett samband mellan den som kan misstänkas och det telefonnummer, den adress eller elektroniska kommunikationsutrustning som avlyssningen avser. För att bestämmelsen ska kunna tillämpas i praktiken får kravet på koppling inte ställas alltför högt. Det bör därför enligt vår mening vara tillräckligt att det *kan antas* att någon som kan misstänkas ha begått eller medverkat till brottet innehar, har innehavt, använder eller har använt det som avlyssningen avser. Uttrycket ”kan antas” betyder att det ska föreligga en mindre sannolikhetsövervikt för att antagandet är riktigt (SOU 2017:89 s. 357). Det motsvarar det beviskrav som gäller i fråga om kopplingen mellan den skäligen misstänkte och en telefon som denne använder eller har använt för att det ska vara möjligt med hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation mot den skäligen misstänkte (27 kap. 20 § första stycket 2 RB).

Det senare regleringsalternativet bedöms täcka in de situationer som avses med det första alternativet, men även fånga in ytterligare fall. Avlyssning skulle med det senare alternativet kunna användas även när telefonnumret inte varit ett brottsverktyg men där åtgärden skulle kunna vara av synnerlig vikt för att stärka alternativt avskriva brottsmisstankarna mot någon.

Ett exempel på situationer där en bestämmelse av nu diskuterat slag skulle kunna tillämpas är en mordutredning där man genom basstationstömning har kunnat konstatera att ett visst telefonnummer har kopplat upp på samma mobilmaster som målsägandens nummer i samband med brottet. Man kan tänka sig fall där denna information

räcker för att grunda misstanke, men det kan också finns fall där enbart denna omständighet inte är tillräcklig men där det finns viss annan utredning som stödjer misstanken. En hemlig avlyssning skulle i så fall vara tillåten i syfte att utreda vem personen i fråga är och om han eller hon kan skäligen misstänkas för brottet.

Fördelarna med en möjlighet till hemlig avlyssning även i de fall där föremålet för avlyssningen inte har varit ett brottsverktyg är så stora att vi förordar detta regleringsalternativ. Vi återkommer i avsnitt 9.8 och 9.9 till frågor om effektivitet och proportionalitet.

9.6.2 Kontaktade nummer, adresser och kommunikationsutrustningar

Bedömning: En eventuell reglering om hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas bör även kunna ta sikte på ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att någon som kan misstänkas ha begått eller medverkat till brottet har kontaktat eller kommer att kontakta under den tid som tillståndet avser.

Skälen för bedömningen

Målsäganden

En möjlighet att avlyssna ett nummer, en adress eller kommunikationsutrustning som kan antas ha koppling till någon som kan misstänkas för brottet kan förväntas vara tillräcklig i många fall. Det finns dock fall där det inte finns något sådant nummer etc. men där en hemlig avlyssning riktad mot exempelvis målsägandens telefon skulle vara den enda reella möjligheten att identifiera någon som skäligen kan misstänkas för brottet. Det kan exempelvis handla om en målsägande som är försvunnen eller medvetslös till följd av ett allvarligt våldsbrott eller människorov och där det inte finns någon skäligen misstänkt för dådet. En möjlighet att kunna ta del av innehållet i skickade och mottagna meddelanden skulle då kunna ge nödvändiga uppslag för att komma vidare i utredningen. Ett annat exempel kan vara att den icke identifierade gärningspersonen ideligen byter telefonnummer varför

det, även om det skulle vara tillåtet, inte går att verkställa en hemlig avlyssning riktad mot denne. Som vi har utvecklat i avsnitt 8.3.3 och 8.5 har målsäganden ett särskilt skydd i rättsprocessen och är t.ex. skyddad mot undersökning av den egna kroppen. Skyddet är dock inte absolut. Målsäganden kan bli föremål för ett antal tvångsåtgärder och kan inte heller hindra att tidigare lämnade förhörsuppgifter åberopas i rättegången även om uppgifterna tagits tillbaka. Frågan är då om man bör kunna rikta en hemlig avlyssning även mot målsäganden. Förutom det särskilda skydd som en målsägande har bör man då även beakta att hemlig avlyssning typiskt sett är en klart mer ingripande och integritetskränkande åtgärd än hemlig övervakning av elektronisk kommunikation.

När det gäller hemlig avlyssning mot en målsägande gör sig i övrigt till stor del samma argument gällande här som i fråga om hemlig övervakning mot en målsägande, se avsnitt 8.5. Som vi anfört där menar vi att det inte i praktiken bör överlämnas till målsäganden om ett allvarligt brott kan utredas eller inte. En sådan ordning skulle inte bara framstå som problematisk från principiella utgångspunkter, utan lägger också ett tungt ansvar på målsäganden som kan vara rädd eller på andra sätt utsatt för hård press att inte medverka i utredningen. Här måste man även beakta förekomsten av s.k. tystnadskulturer i vissa miljöer. Vidare finns det, som framkommit tidigare, ärenden där det i inledningsskedet är osäkert om en person är målsägande, vittne eller misstänkt.

Även med beaktande av det anförda kan det starkt ifrågasättas om det är godtagbart att i praktiken framtvinga en målsägandeberättelse genom användning av hemlig avlyssning av elektronisk kommunikation. Vår bedömning är att det inte framstår som proportionerligt att införa en möjlighet att med hjälp av hemlig avlyssning av elektronisk kommunikation ta del av målsägandens elektroniska kommunikation. En mellanväg skulle kunna vara att man tillåter hemlig avlyssning riktad mot målsägandens telefonnummer, elektroniska adress eller kommunikationsutrustning, men endast i syfte att fånga upp kommunikation med gärningspersonen eller någon annan medverkande. Vi tänker då på situationer av det slag som avses i 27 kap. 20 § första stycket 2. RB, dvs. att det finns synnerlig anledning att anta att den som begått brottet har kontaktat eller kommer att kontakta målsägandens telefonnummer, adress eller kommunikationsutrustning. Med en sådan inriktning på regleringen blir det tydligt att avsikten

enbart är att få tillgång till kommunikation med gärningspersonen i syfte att få reda på vem han eller hon är, och inte att i något annat avseende kartlägga eller utreda målsägandens förehavanden. Åtgärden blir därigenom klart mindre ingripande från integritetssynpunkt och enligt vår mening principiellt godtagbar.

Andra personer

Som framgått under föregående rubriker kan det även i vissa särskilda fall finnas ett behov av en hemlig avlyssning mot andra personer som inte kan misstänkas för brottet och inte heller är målsägande.

En kategori är vittnen, dvs. personer som har bevittnat brottet eller av någon annan anledning kan antas ha uppgifter som har betydelse som bevis, men som inte berättar om vad de vet för polisen. I det föregående har vi tagit upp exemplet med personer som bevittnat ett mycket allvarligt brott, t.ex. ett mord, och som det finns skäl att tro vet mer än de säger. Ett liknande, och enligt polisen vanligt exempel i den gängkriminella miljön, är att anhöriga och andra närstående till målsäganden inte berättar vad de vet om ett allvarligt brott. En annan kategori är identifierade eller icke identifierade personer som är intressanta i utredningen men där det är oklart vilken, om någon, roll de har. Ett tidigare nämnt exempel på detta är mordutredningar där en basstationstömning har visat att ett visst nummer kopplat upp mot samma mobilmaster som målsägandens nummer i nära anslutning till mordet, men att utredningen inte ger stöd för en konkret misstanke mot den som innehar eller använder numret.

Vi konstaterar att det i många fall rör sig om personer som hade varit skyldiga att vittna i en rättegång. Ett vittnes skyldighet att medverka i en utredning och rättegång sträcker sig betydligt längre än en målsägandes. Trots detta bedömer vi det som principiellt tveksamt att införa en möjlighet till hemlig avlyssning respektive hemlig dataavläsning enbart på den grunden att exempelvis ett telefonnummer eller en informationsbärare kan kopplas till personen i fråga. I kriminella kretsar kan det finnas ett stort antal personer som skulle kunna ha information om brottet. En alltför långtgående möjlighet till hemlig avlyssning eller hemlig dataavläsning mot sådana personer kan i praktiken bli en sorts underrättelseverksamhet som genererar stora mängder överskottsinformation. Mot denna bakgrund bedömer vi

att det inte är lämpligt med en reglering som grundas på omständigheten att en viss person kan antas ha information av värde för utredningen. Av de skäl som vi anfört i fråga om målsäganden framstår det däremot som principiellt godtagbart att rikta en hemlig avlyssning mot någon på den grunden att det finns synnerlig anledning att anta att någon som kan misstänkas ha begått eller medverkat till brottet har eller kommer att kontakta vederbörande. Det som i föregående avsnitt sagts om uttrycket ”någon som kan misstänkas ha begått eller medverkat till brottet” avses ha samma betydelse i detta sammanhang.

9.6.3 Särskilt om avlidna

Med hänsyn till vad som framkommit om behovet framstår det som nödvändigt att en hemlig avlyssning av elektronisk kommunikation kan riktas även mot ett telefonnummer etc. som kan ha innehafts eller använts av någon som är avliden.

Om det finns någon som kan misstänkas för brottet och det är den personen som har avlidit uppstår först och främst frågan om det finns skäl att driva förundersökningen vidare. Om så inte är fallet ska den läggas ner. En förundersökning gäller dock inte en viss persons roll vid ett brott utan ett visst brott. Om det finns anledning att utreda någon annan än den avlidnes eventuella medverkan i brottet kan förundersökningen därför drivas vidare (Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas? 4 uppl., s. 51). Det bör i den situationen vara tillåtet att använda hemlig avlyssning av elektronisk kommunikation för att hämta in uppgifter som avser tiden fram till dödsfallet, förutsatt att förutsättningarna för tvångsmedlet är uppfyllda (Lindberg a.a. s. 51). Således bör det alltså vara möjligt att hämta in uppgifter om exempelvis innehållet i skickade eller mottagna sms. Om man, i enlighet med diskussionen i avsnitt 9.6.1, inför en möjlighet till hemlig avlyssning avseende ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som på visst sätt kan kopplas till någon som kan misstänkas ha begått eller annars medverkat till brottet, bör möjligheten gälla även om man vet att personen i fråga är avliden.

Om man inför en reglering som tar sikte på telefonnummer etc. som kan antas ha blivit eller komma att bli kontaktade av den okände gärningspersonen bör det inte ha någon betydelse om innehavaren av numret är avliden.

9.7 Personkretsen för hemlig dataavläsning

9.7.1 Någon som kan misstänkas

Bedömning: En eventuell reglering om hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas som gäller kommunikationsavlyssningsuppgifter bör kunna avse ett avläsningsbart informationssystem som under den tid som tillståndet avser kan antas ha använts eller kan komma att användas av någon som kan misstänkas ha begått eller annars medverkat till brottet.

Skälen för bedömningen

Mycket av det som anförts i avsnitt 9.6.1 är relevant även i fråga om hemlig dataavläsning. I fall där utredningen visar att ett visst avläsningsbart informationssystem används för att begå brott, men den brottsliga användarens identitet är okänd, kan det vara nödvändigt med en möjlighet att kunna avläsa kommunikationsavlyssningsuppgifter för att man ska kunna komma framåt med utredningen och identifiera en skäligen misstänkt. Det kan exempelvis handla om situationer där den kommunikation som man behöver få tillgång till är krypterad och därför inte kan avläsas i klartext med hjälp av en hemlig avlyssning av elektronisk kommunikation. I likhet med vad som sagts i avsnitt 9.6.1 sträcker sig behovet dock längre än till informationssystem som använts vid ett brott. Det kan också handla om situationer där det finns skäl att anta att ett visst informationssystem används av gärningspersonen, men att det inte föreligger skälig brottsmisstanke.

Till skillnad från vad som gäller hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas finns det för hemlig dataavläsning som gäller kommunikationsövervakningsuppgifter och platsuppgifter i samma syfte vissa begränsningar i fråga om de informationssystem som kan avses med åtgärden. Sådan hemlig dataavläsning får nämligen avse endast ett informationssystem som antingen har använts vid ett brott eller i anslutning till brottsplatsen eller som av någon annan anledning är av synnerlig vikt för utredningen (5 § andra stycket lagen om hemlig dataavläsning). Av principiella skäl bör som utgångspunkt motsvarande eller strängare

begränsningar gälla vid hemlig dataavläsning i det angivna syftet som gäller kommunikationsavlyssningsuppgifter. Samtidigt talar starka skäl för att regleringen om hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas så långt som möjligt speglar regleringen om hemlig avlyssning av elektronisk kommunikation i samma syfte.

En lösning skulle kunna vara att det införs en möjlighet att avlyssna ett informationssystem som har en viss koppling till någon okänd person som kan misstänkas för brottet. Vi menar att en sådan lösning normalt skulle rymma de fall där informationssystemet använts vid utförandet av brottet. Vi menar vidare att informationssystem med en sådan koppling per definition måste anses vara av synnerlig vikt för utredningen i många fall. En reglering med motsvarande innebörd som den vi föreslagit i fråga om hemlig avlyssning av elektronisk kommunikation skulle därför enligt vår mening principiellt inte gå utanför gränserna för hemlig dataavläsning avseende platsuppgifter och kommunikationsövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas. Med tanke på att bestämmelserna om hemlig dataavläsning generellt bygger på att en viss person använder informationssystemet och alltså inte på innehav av detsamma (se 4 § andra stycket lagen om hemlig dataavläsning), bör den nu aktuella bestämmelsen dock ha samma innebörd.

9.7.2 Kontaktade informationssystem

Bedömning: En eventuell reglering om hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas och som gäller kommunikationsavlyssningsuppgifter bör även kunna ta sikte på ett avläsningsbart informationssystem som det finns synnerlig anledning att anta att någon som kan misstänkas ha begått eller medverkat till brottet har kontaktat eller kommer att kontakta under den tid som tillståndet avser.

Skälen för bedömningen

Vi har i avsnitt 9.6.2 gjort bedömningen att en eventuell reglering om hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas bör kunna avse ett telefon-

nummer, en annan adress eller ett visst kommunikationssystem som det finns synnerlig anledning att anta att någon som kan misstänkas ha begått eller medverkat till brottet har kontaktat eller kommer att kontakta under den tid som tillståndet avser har kontaktat eller kommer att kontakta. De skäl som anförts där gör sig gällande även i fråga om hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter. Vi anser att sådana informationssystem som nu är aktuella typiskt sett är av synnerlig vikt för utredningen. Med kontakta avses här detsamma som i 4 § tredje stycket lagen om hemlig dataavläsning.

9.7.3 Särskilt om avlidna

Det som har anförts i avsnitt 9.6.3 om hemlig avlyssning av elektronisk kommunikation av avlidna personers telefonnummer m.m. är i princip relevant även när det gäller hemlig dataavläsning, som ju avser ett visst informationssystem.

9.8 Åtgärderna förväntas vara effektiva

Bedömning: En möjlighet att utreda vem som skäligen kan misstänkas för brottet med hjälp av hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter förväntas leda till betydligt bättre utredningsmöjligheter i de fall åtgärden kan användas. Respektive åtgärd kommer dock inte att kunna användas i alla de ärenden där det finns behov av den.

Skälen för bedömningen

Av behovsbeskrivningen i avsnitt 9.5 har det framgått att det i vissa fall inte finns någon annan reell möjlighet att komma framåt i utredningen och identifiera en skäligen misstänkt än att använda hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter. Även om man naturligtvis inte kan påstå att en möjlighet att använda endera av de nu aktuella hemliga tvångsmedlen kommer att leda till att man varje gång de används kan identifiera en skäligen misstänkt, menar vi att det

framgår av de brottsbekämpande myndigheternas uppgifter att möjligheten kan innebära en stor förbättring när det gäller möjligheten att utreda vissa sorters brott.

Det finns här anledning att säga några ord om förhållandet mellan hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter. Det bör nämnas att det i praktiken ofta inte är möjligt att få tillgång till den information som behövs genom en hemlig avlyssning. Detta hänger bl.a. samman med förekomsten av kryptering och anonymisering och det faktum att det inte i dagsläget föreligger någon skyldighet för tillhandahållare av internetbaserade tjänster att anpassa sin verksamhet så att hemlig avlyssning kan verkställas. Om det skulle införas en sådan anpassningsskyldighet kan effektiviteten av hemlig avlyssning återigen öka. Förhållandet att man i nuläget kan ha svårt att få tillgång till visst innehåll genom hemlig avlyssning och därför i praktiken behöver besluta om hemlig dataavläsning bör inte tas till intäkt för att hemlig avlyssning inte kan vara effektiv i åtskilliga fall.

En särskild utredare har fått i uppdrag att se över den lagstiftning som medför en skyldighet för tillhandahållare av elektroniska kommunikationstjänster att lagra uppgifter om elektronisk kommunikation för brottsbekämpande syften, samt vissa anknytande frågor om myndigheternas tillgång till sådana uppgifter (dir. 2021:58). Uppdraget syftar till att säkerställa att de brottsbekämpande myndigheternas tillgång till information förbättras och upprätthålls över tid i takt med teknikutvecklingen och förändrade kommunikationsvanor, samtidigt som respekten för mänskliga rättigheter säkerställs. Utredaren ska bl.a. analysera förutsättningarna för att leverantörer av s.k. OTT-tjänster[4] ska kunna omfattas av skyldigheten att lagra och ge tillgång till uppgifter om elektronisk kommunikation samt ta ställning till om en sådan skyldighet bör införas, och analysera och föreslå moderniseringar av regleringen när det gäller tjänsteleverantörers skyldighet att anpassa sin verksamhet så att hemliga tvångsmedel kan verkställas på ett effektivt sätt. Uppdraget ska redovisas senast den 6 februari 2023. Utredningens förslag kan komma att påverka tillämpningsområdena för nu aktuella hemliga tvångsmedlen sinsemellan.

[4] Uttrycket är en akronym för ”over the top” och omfattar tjänster som vanligtvis tillhandahålls av andra än de traditionella teleoperatörerna. Tjänsterna kallas även för nummeroberoende interpersonella kommunikationstjänster. Exempel på OTT-tjänster är Apple Imessage och Facetime, Facebook Messenger, Whatsapp och Signa.

Det bör också sägas något om tillämpningsområdet för att använda de aktuella tvångsmedlen i det nya syfte som nu diskuteras. De krav som vi i avsnitt 9.10 bedömer nödvändiga i fråga om brottet eller brottslighetens allvar innebär en kraftig begränsning av tillämpningsområdet. Även med beaktande av detta bedömer vi att tvångsmedlen kommer att kunna användas i syfte att utreda vem som skäligen kan misstänkas för brottet i tillräckligt många fall för att möjligheten ska anses effektiv från kvantitativ synpunkt. Av särskild betydelse är det att möjligheten kan öka chanserna att utreda mycket allvarlig brottslighet, såsom svårlösta mord, människorov och sexualbrott mot barn.

9.9 Åtgärderna är proportionerliga

Bedömning: Det är proportionerligt att införa en möjlighet att utföra hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas.

Skälen för bedömningen

Skyddet för den personliga integriteten

Var och en är enligt 2 kap. 6 § regeringsformen skyddad mot hemlig avlyssning av telefonsamtal och andra förtroliga försändelser. Varje möjlighet till hemlig avlyssning av elektronisk kommunikation utgör därför en inskränkning av denna rättighet, och måste ske genom lag. Sådana inskränkningar är tillåtna förutsatt att de är godtagbara i ett demokratiskt samhälle, inte går utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett inskränkningen och inte heller sträcker sig så långt att de utgör ett hot mot den fria åsiktsbildningen (2 kap. 21 § regeringsformen).

Hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning utgör också en inskränkning av rätten till privatliv och skydd för korrespondens som slås fast i artikel 8.1 i Europakonventionen. Även dessa rättigheter får inskränkas med lagstöd, och under de förutsättningar som anges i artikel 8.2 (se närmare i avsnitt 3.2. Europadomstolen har i flera avgöranden framhållit att telefonavlyss-

ning utgör ett allvarligt intrång i den enskildes privatliv och förtroliga korrespondens och därför måste vara grundad på lag av särskilt precis natur. Flertalet av de avgöranden som gäller avlyssning inom ramen för en brottsutredning gäller någon som är misstänkt för brottet. Men det framgår av domstolens praxis att hemlig avlyssning även kan vara tillåten i förhållande till personer som inte är misstänkta för ett brott men som kan ha information om en brottslig gärning. I fallet Greuter mot Nederländerna, som gällde hemlig avlyssning mot flickvännen till en man som blivit mördad, fanns inte någon brottsmisstanke mot en viss person. Dock fanns det anledning att tro att den okände gärningsmannen skulle komma att kontakta flickvännen, tillika klaganden i Europadomstolen. Europadomstolen ansåg avlyssningen godtagbar och tog inte upp saken till prövning. Domstolen har dock inte godtagit att den kategori personer som kan utsättas för att få sina telefoner avlyssnade utöver misstänkta och tilltalade även avser ”envar annan person som är inblandad i en brottslig gärning” utan någon närmare förklaring, t.ex. i lag eller praxis eller genom en vedertagen tolkning av begreppets innebörd. (Iordachi och andra mot Moldavien, punkt 44, i vilket klagandena hävdade att de löpte en allvarlig risk för att få sina telefoner avlyssnade för att de var medlemmar i en organisation som specialiserade sig på att företräda sökande inför Europadomstolen, samt även Roman Zakharov mot Ryssland [GC], punkt 245 och Szabó och Vissy mot Ungern, punkt 67 and 73).

En utvidgad möjlighet till hemlig avlyssning av elektronisk kommunikation måste också vara förenlig med artiklarna 7 och 8 i EU:s rättighetsstadga och bestämmelserna i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (se närmare i avsnitt 4.2.2). Däremot torde hemlig dataavläsning inte omfattas av skyddet, såvida åtgärden riktas direkt mot enskilda och inte förutsätter att någon leverantör involveras (jfr EU-domstolens uttalanden i La Quadrature du Net m.fl. punkt 103). EU-domstolen har i bl.a. Tele2-domen uttalat att tillgång till trafikuppgifter och lokaliseringsuppgifter i princip bara kan beviljas till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. Även om uttalandena inte avser innehållsuppgifter måste det enligt vår bedöm-

ning antas att sådana uppgifter, som ju typiskt sett är mer integritetskänsliga, har ett åtminstone lika starkt skydd som trafikuppgifter och lokaliseringsuppgifter. Vår bedömning är emellertid att detta inte innebär att möjligheten till hemlig avlyssning och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i alla situationer måste begränsad till enbart misstänkta. Som angetts tidigare anser vi att uttalandet bör förstås på så sätt att den tänkbara personkretsen inte enbart omfattar misstänkta gärningspersoner och medhjälpare utan även t.ex. en målsägande (jfr SOU 2017:75 s. 257 och 258). Den utformning av bestämmelserna som vi förordar i avsnitt 9.6 och 9.7 bedöms dock innebära att tvångsmedlet riktar sig mot den okände misstänkte. Så har man sett på det när en avlyssning riktas mot ett telefonnummer som det finns synnerlig anledning att anta att den skäligen misstänkte har eller kommer att kontakta, och vi ser inte skäl att anlägga något annat synsätt i de nu aktuella fallen.

Med hänsyn till det anförda gör vi bedömningen att reglerna till skyddet för den personliga integriteten och personuppgifter inte i och för sig utgör ett hinder mot hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet. Bedömningen förutsätter dock att åtgärden är proportionerlig.

Proportionalitet

Behovet av en möjlighet att använda hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet är enligt vår bedömning i avsnitt 9.5 påtagligt. Såväl brottsutvecklingen som de kriminellas riskmedvetenhet och den tekniska utvecklingen har betydelse för denna bedömning. Mot behovet måste man ställa det integritetsintrång som åtgärderna innebär. Det finns vid proportionalitetsbedömningen inte anledning att göra någon större skillnad mellan hemlig avlyssning och hemlig dataavläsning. Hemlig dataavläsning kan nämligen, när det gäller uppgifter av det aktuella slaget, inte anses medföra påtagligt större risker för den personliga integriteten (jfr prop. 2019/20:64 s. 94). Ett nytt tillämpningsområde innebär emellertid att fler personer kan drabbas av två av de hemliga tvångsmedel som typiskt sett innebär

ett stort ingrepp i den personliga integriteten. Det finns vidare en risk för att fler personer som senare visar sig ovidkommande utsätts för hemliga tvångsmedel.

Vid hemlig avlyssning eller hemlig dataavläsning baserad på att en icke misstänkt person kontaktats eller kan antas komma att bli kontaktad av den skyldige kan det komma fram överskottsinformation om personens egen eller någon närståendes brottsliga verksamhet. Sannolikheten för att sådan information kan komma fram är särskilt stor vid konflikter i kriminella miljöer, där det inte är ovanligt att både gärningsman och målsägande rör sig i miljön och ägnar sig åt brottslig verksamhet. Det är dock inte någon nyhet i sig att hemliga tvångsmedel kan ge information om t.ex. målsägandens egen brottslighet. Sådan information kan ju komma fram på flera andra sätt, t.ex. vid en avlyssning med stöd av 27 kap. 20 § första stycket 2 som avser målsägandens telefon. Möjligheten kan vidare inbjuda till missbruk av tvångsmedlet. Med hänsyn till de omfattande rättssäkerhetsgarantier som finns i fråga om hemlig avlyssning respektive hemlig dataavläsning, och risken för att en åklagare som överskrider gränserna döms för tjänstefel, bedömer vi dock att risken för missbruk är liten. Vidare finns det numera bestämmelser om hur överskottsinformation får användas (se 27 kap. 23 a § RB och 28 § lagen om hemlig dataavläsning). Information som har hämtats in i enlighet med ett interimistiskt åklagarbeslut som upphävs av rätten får inte användas i en brottsutredning till nackdel vare sig för den avlyssnade eller någon annan som uppgifterna avser (27 kap. 21 a § RB).

Hemlig avlyssning eller hemlig dataavläsning på grund av att personen kan antas ha kontaktats eller bli kontaktad av den okände gärningspersonen kan komma att riktas mot någon som är närstående till den person som senare blir skäligen misstänkt och sedermera tilltalad. Det finns därför skäl att uppmärksamma reglerna i 36 kap. 6 § RB, som innebär att personer som på visst angivet sätt är närstående till den tilltalade är befriade från vittnesplikten. Om en sådan person väljer att vittna får han eller hon inte avlägga vittnesed (36 kap. 13 § andra stycket). Telefonsamtal eller andra meddelanden mellan närstående omfattas dock inte av avlyssningsförbudet i 27 kap. 22 RB. Det är alltså redan i dag tillåtet att avlyssna detta slags kommunikation. Vi bedömer därför att detta förhållande i sig inte innebär något starkt skäl mot ett införande av en möjlighet till hemlig avlyssning i de nu diskuterade fallen.

Det bör avslutningsvis sägas att det kan visa sig att en person man avlyssnat hör till den krets som omfattas av avlyssningsförbud på grund att personen inte kunnat höras som vittne. I ett sådant fall ska en pågående avlyssning omedelbart avbrytas och alla upptagningar och uppteckningar omedelbart förstöras i de delar de omfattas av avlyssningsförbud (27 kap. 22 § RB). Uppgifter som fångats upp fastän de omfattas av avlyssningsförbud får alltså inte användas som bevis.

Utöver det påtagliga behovet måste det vidare beaktas att vi föreslår att möjligheten begränsas till brott och brottslighet av allvarligt slag där det finns ett särskilt stort behov (se våra överväganden i avsnitt 9.10 om strafftrösklar m.m.). När det gäller integritetsintrånget finns det även skäl att uppmärksamma skyldigheten att, när det finns skäl till detta, ange särskilda villkor i beslutet för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan (27 kap. 21 § sjätte stycket RB). Man kan genom sådana åtgärder begränsa integritetsintrånget för den som utsätts för tvångsmedlet. Vidare måste man beakta de starka rättssäkerhetsgarantier som omgärdar användningen av hemliga tvångsmedel. Av betydelse är även att en möjlighet att använda tvångsmedlen i fråga inte bara kan leda till att man kan utreda vem som skäligen kan misstänkas, utan även att man kan få klart för sig att en person är oskyldig och kanske helt ovidkommande för utredningen. Det bör också beaktas att åtgärden, så långt det är möjligt, bör begränsas till syftet att identifiera en skäligen misstänkt. Så snart en skäligen misstänkt identifierats, eller det av något annat skäl inte finns anledning att fortsätta avlyssningen, måste den avbrytas eftersom ändamålet med den inte längre föreligger.

Vid en samlad avvägning gör vi bedömningen att det är proportionerligt med en möjlighet att använda hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet. Bedömningen förutsätter att möjligheten begränsas på det sätt som vi förordar i avsnitt 9.6 respektive 9.7 och 9.10.

9.10 Användning av tvångsmedlen i ett nytt syfte bör tillåtas

9.10.1 En ny möjlighet införs

Förslag: Det införs en möjlighet att, om det är av synnerlig vikt för utredningen, utföra hemlig avlyssning och hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet. Avlyssning och dataavläsning ska få ske i realtid.

Hemlig avlyssning ska endast få avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning

1. som under tid som tillståndet avser kan antas innehas eller ha innehafts av någon som kan misstänkas ha begått eller annars medverkat till brottet eller som annars kan antas ha använts eller komma att användas av en sådan person, eller
2. som det finns synnerlig anledning att anta att någon som kan misstänkas ha begått eller medverkat till brottet har kontaktat eller kommer att kontakta under den tid som tillståndet avser.

Hemlig dataavläsning ska endast få avse ett avläsningsbart informationssystem

1. som under den tid som tillståndet avser kan antas ha använts eller kan komma att användas av någon som kan misstänkas ha begått eller annars medverkat till brottet, eller
2. som det finns synnerlig anledning att anta att någon som kan misstänkas ha begått eller medverkat till brottet har kontaktat eller kommer att kontakta under den tid som tillståndet avser.

Skälen för förslagen

Mot bakgrund av de överväganden som gjorts i avsnitt 9.5–9.9 föreslår vi att det ska införas en möjlighet att använda hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter i syfte att utreda vem som skä-

ligen kan misstänkas bör brottet. Personkretsen bör avgränsas på det sätt som vi kommit fram till i avsnitt 9.6 och 9.7.

Avlyssning och dataavläsning bör få göras i realtid

Hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet får avse inhämtning av både historiska lokaliseringsuppgifter och övervakning i realtid av var en viss kommunikationsutrustning finns. Inhämtning av uppgifter om meddelanden, s.k. HÖK-listor, får däremot endast avse förfluten tid, dvs. meddelanden som redan har överförts. Motsvarande begränsning gäller för hemlig dataavläsning avseende kommunikationsövervakningsuppgifter i syfte att utreda vem som skäligen kan misstänkas. Vi har i avsnitt 7.5 föreslagit att denna begränsning ska tas bort och att det alltså ska bli möjligt att hämta in uppgifter om meddelanden i realtid såväl vid hemlig övervakning av elektronisk kommunikation som vid hemlig dataavläsning.

När det gäller hemlig avlyssning av elektronisk kommunikation konstaterar vi att avlyssning av telefonsamtal endast kan ske i realtid. En begränsning till historiska meddelanden skulle därför innebära att ändamålet med en möjlighet till hemlig avlyssning i syfte att utreda vem som skäligen kan misstänkas för brottet till stor del skulle gå förlorad. Redan detta innebär att begränsningen inte bör införas. Det bör vidare framhållas våra förslag innebär att tvångsmedlet enbart får tillgripas i allvarliga och mycket angelägna fall, och att villkoren för dess tillämplighet i allmänhet är strängare än vad som gäller i fråga om hemlig övervakning av elektronisk kommunikation. Hemlig avlyssning i de nu aktuella fallet bör alltså få avse även avlyssning i realtid. Motsvarande skäl gör sig gällande i fråga om hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter.

Det bör gälla ett krav på synnerlig vikt för utredningen

För att ett hemligt tvångsmedel ska få användas under en förundersökning krävs att åtgärden är av synnerlig vikt för utredningen. Det framstår som självklart att detta krav måste gälla också i de nu aktuella fallen. Om samma resultat kan uppnås på något annat och mindre ingripande sätt, bör åtgärden alltså inte vara tillåten.

9.10.2 Huvudregeln bör vara gränsen för hemlig rumsavlyssning

Förslag: Tvångsmedlen ska kunna användas i syfte att utreda vem som skäligen kan misstänkas vid utredning om brott eller brottslighet som kan föranleda ett beslut om hemlig rumsavlyssning.

Skälen för förslaget

En första fråga är vad som bör krävas i fråga om brottets eller brottslighetens allvar för att respektive tvångsmedel ska få användas i det nya syftet, om en sådan möjlighet införs.

Av de exempel som lämnats till oss framgår att behovet av hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter kan vara särskilt stort i utredningar om synnerligen allvarliga brott, såsom mord och människorov. Vissa av de exempel som lämnats och där vi anser att det föreligger ett behov avser dock brott som, även om de är allvarliga, inte har en lika sträng straffskala. Flera av dessa brott kan föranleda en hemlig avlyssning av elektronisk kommunikation, antingen på grund av sin straffskala eller med stöd av en straffvärdeventil, men sällan eller aldrig hemlig rumsavlyssning. Som exempel kan nämnas allmänfarlig ödeläggelse, som straffas med fängelse i lägst två och högst åtta år. Exempel på andra brott som kan föranleda en hemlig avlyssning av elektronisk kommunikation men sällan eller aldrig en hemlig rumsavlyssning är grova bedrägerier, internetrelaterade sexualbrott mot barn, grova penningtvättsbrott och många fall av grov narkotikabrottslighet.

Av det anförda framgår att flera av de fall där det finns ett behov av en möjlighet till hemlig avlyssning eller hemlig dataavläsning skulle falla bort om man sätter en högre gräns än ett krav på att brottet kan leda till hemlig avlyssning av elektronisk kommunikation. Det kan tala för att man borde sätta samma gräns för tvångsmedlen som när det finns en skäligen misstänkt. Detta skulle dock samtidigt innebära att man sätter samma gräns för den nya regleringen som för hemlig övervakning av elektronisk kommunikation eller hemlig dataavläsning av kommunikationsövervakning- och platsuppgifter som sker i syfte att utreda vem som skäligen kan misstänkas för brottet. Eftersom hemlig avlyssning och hemlig dataavläsning som gäller kom-

munikationsavlyssningsuppgifter typiskt sett är betydligt mer ingripande, även om personkretsen begränsas i enlighet med vad vi föreslår, kan en sådan gräns knappast motiveras om man inte samtidigt gör bedömningen att man bör sänka de befintliga gränserna. Det ingår inte i vårt uppdrag att överväga en sådan förändring och det är långtifrån givet att det skulle vara en lämplig ändring. Goda skäl kan nämligen anföras till stöd för ståndpunkten att det bör ställas högre krav när det inte finns någon skäligen misstänkt, särskilt som risken torde öka för att ovidkommande personer drabbas. En sådan ändring skulle dessutom rubba förhållande till bestämmelserna om hemlig dataavläsning. För hemlig dataavläsning (förutom sådan avläsning som gäller rumsavlyssningsuppgifter) gäller ju ett generellt krav på att brottet är sådant att det kan föranleda hemlig avlyssning av elektronisk kommunikation. Vi lägger alltså inte fram några sådana förslag eller några närmare överväganden än de som nyss redovisats.

En lägre gräns än den som gäller för hemlig avlyssning av elektronisk kommunikation generellt kan självfallet inte komma i fråga. Det som återstår är alltså att överväga olika varianter av strängare gränser än den som gäller för hemlig avlyssning av elektronisk kommunikation i allmänhet.

Ett alternativ skulle kunna vara att man sätter gränsen vid ett minimistraff på tre års fängelse jämte en straffvärdeventil för fall där straffvärdet kan antas överstiga tre års fängelse. Det bör då framhållas att det är fråga om en ytterst komplicerad reglering som ställer höga krav på den som ska tillämpa den. Våra förslag i kapitel 6 och 7 kommer, om de genomförs, att komplicera regleringen ytterligare. Redan med hänsyn till detta anser vi det inte lämpligt att föreslå en särskild gräns för de nu aktuella fallen. Starka skäl talar i stället för att man knyter an till de gränser i fråga om straffsats och straffvärde som i övrigt gäller. Det bör också framhållas att hemlig avlyssning och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter typiskt sett är mycket integritetskränkande tvångsmedel, och att våra förslag innebär en ökad risk för den personliga integriteten genom att tvångsmedlet kommer att kunna användas i fler fall än i dag. Risken för att personer som är ovidkommande för utredningen avlyssnas bedöms öka om våra förslag genomförs, inte minst genom att vi föreslår att åtgärden ska kunna riktas mot ett nummer eller någon annan adress, kommunikationsutrustning eller informationssystem vars användare inte är identifierad.

Med hänsyn till det anförda bedömer vi att gränsen för en eventuell möjlighet att använda hemlig avlyssning av elektronisk kommunikation respektive hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet måste sättas högre. Det framstår då som naturligast att som huvudregel kräva att brottet eller brottsligheten kan leda till hemlig rumsavlyssning. Bedömningen innebär (förutsatt att våra förslag i kapitel 6 genomförs) att hemlig avlyssning av elektronisk kommunikation respektive hemlig dataavläsning i nu aktuellt syfte skulle kunna användas vid en förundersökning om

1. brott med ett minimistraff om lägst fyra års fängelse,
2. spioneri enligt 19 kap. 5 § brottsbalken,
3. brott som avses i 26 § lagen (2018:558) om 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, eller
5. flerfaldig brottslighet som kan antas ha utövats i organiserad form eller systematiskt och som kan antas ha ett samlat straffvärde överstigande fängelse i fyra år och där varje enskilt brott som ingår i sammanläggningen har ett minimistraff om sex månaders fängelse eller mer.

De särskilda begränsningarna för hemlig rumsavlyssning som följer av 27 kap. 20 e § bör däremot inte gälla.

9.10.3 Huvudregeln bör kompletteras med en brottskatalog

Förslag: Tvångsmedlen ska kunna användas i syfte att utreda vem som skäligen kan misstänkas även vid utredning om vissa andra brott eller flerfaldig brottslighet där det föreligger ett särskilt påtagligt behov av en möjlighet att använda hemlig avlyssning eller hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas. Dessa andra brott ska räknas upp i en särskild brottskatalog.

Skälen för förslaget

Det behövs en brottskatalog

Den gräns som vi angett i avsnitt 9.10.2 utgör en kraftig begränsning av möjligheten att använda de nu aktuella tvångsmedlen i syfte att utreda vem som skäligen kan misstänkas. Frågan är därför om man bör lägga till ytterligare, särskilt utpekade brott, som framstår som speciellt angelägna att kunna utreda med hjälp av hemlig avlyssning eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter även innan det finns en skäligen misstänkt. Mot en sådan lösning talar bl.a. de inbyggda problem som finns med brottskataloger. En brottskatalog speglar alltid den tid då den infördes och det är otympligt och kan ta relativt lång tid att ändra den. Samtidigt kan man konstatera att det är en viss skillnad mellan en katalog av den typ som används i fråga om straffvärdeventilen avseende hemlig rumsavlyssning och den typ av katalog som används i bestämmelsen om hemlig övervakning av elektronisk kommunikation. Den förstnämnda katalogen begränsar ventilens tillämplighet till endast vissa uppräknade brott, medan den senare utvidgar möjligheten att använda tvångsmedlet även till vissa brott som har en lindrigare straffskala än vad som gäller enligt huvudregeln. Den katalog som vi nu överväger hör till den senare kategorin. Vi gör bedömningen att fördelarna med en särskild brottskatalog som utvidgar tillämpningsområdet överväger nackdelarna och att tillämpningsområdet skulle bli alltför snävt utan en sådan katalog. Flera av de brottstyper där det finns ett särskilt påtagligt behov skulle sällan eller aldrig bli aktuella. Om det ska införas en möjlighet att använda de nu aktuella tvångsmedlen i syfte att utreda vem som skäligen kan misstänkas anser vi alltså att det, utöver de brott och sådan flerfaldig brottslighet som kan leda till hemlig rumsavlyssning enligt våra förslag i kapitel 6, bör vara möjligt att använda tvångsmedlen i syfte att utreda vem som skäligen kan misstänkas för brottet vid utredning om viss allvarlig brottslighet där det finns ett särskilt påtagligt behov av detta.

Grundförutsättningar för att ett brott ska tas med i katalogen

Nästa fråga är vilka brott som bör ingå i en särskild brottskatalog, om det införs en möjlighet att använda de aktuella tvångsmedlen i syfte att utreda vem som skäligen kan misstänkas. Avgörande bör då

vara att brottet eller brottsligheten är så allvarlig att åtgärden är försvarlig, att det föreligger ett särskilt behov av åtgärden och att den kan förväntas vara effektiv. En annan grundläggande förutsättning bör vara att brottet, eller den samlade brottsligheten, är sådan att hemlig avlyssning av elektronisk kommunikation hade varit möjlig om det funnits en skäligen misstänkt. Det kan alltså inte komma i fråga att tillåta tvångsmedlet i utredningar om brott eller brottslighet som inte ens hade kunnat föranleda hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter mot en skäligen misstänkt.

Grovt bedrägeri som begås med hjälp av elektronisk kommunikation

En kategori brott som är svårutredda men som sällan når upp till ett sådant straffvärde respektive samlat straffvärde att den befintliga eller av oss föreslagna av straffvärdeventilen för hemlig rumsavlyssning blir tillämpliga, är grova bedrägerier som begås med hjälp av elektronisk kommunikation. Straffet för grovt bedrägeri är fängelse i lägst sex månader och högst sex år. Vår bedömning är att det behövs mer kraftfulla verktyg för att kunna utreda grova bedrägerier som begås med hjälp av elektronisk kommunikation, även när de inte har ett straffvärde eller samlat straffvärde överstigande fyra års fängelse. Brottet bör därför tas med i brottskatalogen. Med tanke på straffskalan bör det krävas att någon av straffvärdeventilerna för hemlig avlyssning av elektronisk kommunikation är tillämplig för att de aktuella tvångsmedlen ska få användas i de nu aktuella fallen.

Utpressning

Som vi har utvecklat i avsnitt 7.4 är utpressning ett annat brott som kan vara mycket svårt att utreda, bl.a. med hänsyn till att målsäganden ofta kan vara rädd för att medverka i brottsutredningen. En form av utpressning som är förenad med särskilda utredningssvårigheter är ransomwareattacker. Som vi framhållit i avsnitt 7.5 är attacker med ransomware en typ av brottslighet där det finns ett starkt behov av en möjlighet att kunna använda hemlig avlyssning och hemlig dataavläsning för att ha en chans att identifiera någon eller några skäligen misstänkta. Eftersom ransomwareattacker kan vara systemhotande är

det angeläget att de kan utredas effektivt. Det är allvarligt om Sverige framstår som en fristad för den som vill begå denna typ av brottslighet och om det svenska regelverket förhindrar nödvändigt internationellt samarbete.

Ransomwareattacker innefattar dels utpressning eller försök till utpressning, dels någon form av dataintrång. En konsekvens av att de brottsbekämpande myndigheterna inte når fram med utredningar om ransomwareattacker är att det saknas rättspraxis. Det är därför svårt att uttala sig om hur domstolarna skulle se på frågan om vad som krävs för att det ska vara fråga om grovt brott och på straffvärdet.

Vi har i avsnitt 7.4 föreslagit att utpressning och grov utpressning läggs till i katalogen över brott som kan leda till hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter. Starka behovsskäl talar för att det även ska vara möjligt att använda nu aktuella hemliga tvångsmedel i syfte att utreda vem som skäligen kan misstänkas för brottet. Behovet föreligger i synnerhet när det gäller ransomwareattacker, men kan även finnas i andra fall av utpressning. Som vi framhållit i avsnitt 7.4 kan utpressning bidra till otrygghet i samhället och även vara systemhotande. Med hänsyn till detta anser vi att utpressning – även av normalgraden – bör kunna leda till hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas. Med tanke på att brottet föreslås ingå i brottskatalogen i 27 kap. 18 § RB finns det inte anledning att kräva att någon av straffvärdeventilerna är tillämplig.

Grovt dataintrång

Som framgått i det föregående innefattar en typisk ransomwareattack både ett dataintrång och en utpressning. I de fall skadlig kod används i utpressningssyfte bedömer vi att behovet av hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning i allt väsentligt tas om hand av våra förslag i fråga om utpressning i det föregående. Dock kan det finnas andra situationer som inte omfattas och där behovet är påtagligt. Ett exempel kan vara att individer eller sammanslutningar begår dataintrång i syfte att straffa myndigheter eller makthavare. Även detta slags brott kan vara systemhotande och mycket

svåra att utreda. Det finns samtidigt åtskilliga fall av dataintrång som inte är av den digniteten att hemlig avlyssning och andra hemliga tvångsmedel på motsvarande nivå bör kunna förekomma. Med hänsyn till det anförda bedömer vi att hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning som gäller kommunikationsavlyssningsuppgifter bör kunna användas vid misstanke om grovt dataintrång i syfte att utreda vem som skäligen kan misstänkas för brottet.

Straffskalan för grovt dataintrång är fängelse i lägst sex månader och högst sex år. Vid bedömande av om brottet är grovt ska det särskilt beaktas om gärningen har orsakat allvarlig skada eller avsett ett stort antal uppgifter eller annars varit av särskilt farlig art. Rättspraxis är knapp men ger vid handen att straffvärdet för grovt dataintrång sällan eller aldrig överstiger fyra års fängelse. Vår bedömning är därför att brottet bör läggas till i den nu aktuella brottskatalogen.

Allmänfarlig ödeläggelse

Allmänfarlig ödeläggelse begås sällan med digitala hjälpmedel även om exempelvis mobiltelefoner givetvis kan användas som ett verktyg, t.ex. för att flera gärningspersoner ska kunna planera brottet och koordinera sig. Straffskalan är fängelse i lägst två och högst åtta år. Som framgått tidigare kan det förekomma fall där det saknas möjlighet att utreda brottet utan en möjlighet till hemlig avlyssning. Det rör sig om en mycket allvarlig typ av brottslighet med en sträng straffskala. Med tanke på straffskalan finns det inte anledning att kräva att någon av straffvärdeventilerna är tillämpliga.

Penningtvätt

Möjligheten att tjäna pengar är den huvudsakliga drivkraften bakom organiserad brottslighet. För att kriminella ska kunna använda brottsvinster i den lagliga ekonomin tvättas svarta pengar rena. Syftet med penningtvätten är att dölja var pengarna kommer ifrån. Genom olika transaktioner kan personer som ägnar sig åt organiserad brottslighet omvandla pengar från t.ex. narkotikahandel eller bankrån till skenbart lagliga inkomster och tillgångar. Enligt rapporten ”Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2019” tvättas cirka 130 miljarder kronor varje år i det svenska finan-

siella systemet. Det innebär alltså att kriminella lyckas tvätta enorma summor som ofta används till konsumtion och investeringar, men som också kan gå till att finansiera terrorism. Det är mot denna bakgrund ytterst angeläget att dessa brott kan utredas effektivt och de bör därför tas med i brottskatalogen.

Straffskalan för grov penningtvätt och näringspenningtvätt, grovt brott, är fängelse i lägst sex månader och högst sex år. Hemlig avlyssning av elektronisk kommunikation mot en skäligen misstänkt kan alltså bara äga rum med stöd av någon av straffvärdeventilerna. Av en genomgång av penningtvättsdomar åren 2016–2020 som sammanställts av Ekobrottsmyndigheten i april 2020 (Aktuella rättsfrågor ARF 2020:1) framgår att straffvärdet för näringspenningtvätt, grovt brott, varierar relativt mycket. I en dom bedömdes en gärning avseende 1,6 miljoner kronor ha ett straffvärde som motsvarade fängelse i sex månader, medan en gärning avseende cirka 2 miljoner kronor i en annan dom bedömdes ha ett straffvärde på fängelse ett år och sex månader. Det är svårt att säga vilken beloppsnivå som skulle öppna en möjlig straffvärdeventil på fyraårsnivå, och majoriteten av ärendena kommer inte upp till en sådan nivå.

Med hänsyn till det anförda gör vi bedömningen att även grov penningtvätt och näringspenningtvätt, grovt brott, bör ingå i brottskatalogen. Med tanke på straffskalan bör det krävas att någon av straffvärdeventilerna för hemlig avlyssning av elektronisk kommunikation är tillämplig.

Grovt narkotikabrott och grov narkotikasmuggling

Handel med narkotika är den viktigaste inkomstkällan för kriminella nätverk och bidrar, bl.a. genom sin koppling till våldsutövning, till otrygghet i bl.a. utsatta områden (se bl.a. SOU 2021:68 s. 159 och 160). Det är därför av stor vikt att man kan strypa tillgången på narkotika genom att man effektivt kan utreda grova narkotikabrott och grov narkotikasmuggling. Som har framgått i behovsbeskrivningen finns det situationer där man har små eller obefintliga möjligheter att komma framåt i utredningen och identifiera gärningsmännen utan en möjlighet till hemlig avlyssning eller hemlig dataavläsning gällande kommunikationsavlyssningsuppgifter. Brotten har ett minimistraff på fängelse i två år. Med hänsyn till det anförda bör grovt narkotikabrott och grov narkotikasmuggling läggas till en eventuell brottskatalog.

Grova brott avseende vapen och explosiva varor

Under senare år har skjutvapenvåldet och införseln av illegala vapen ökat. En allt högre andel av det dödliga skjutvapenvåldet förekommer i konflikter i kriminella miljöer (se bl.a. promemorian En strängare syn på vapenbrott och smuggling av vapen och explosiva varor, Ds 2019:14 s. 84–86). Även användningen och införseln av explosiva varor, främst handgranater, har ökat (Ds 2019:14 s. 87 och 88). I propositionen Explosiva varor – Tullverkets befogenheter vid inre gräns (prop. 2016/17:169 s. 13) anförde regeringen bl.a. följande. Det finns tydliga tecken på att personer som tillhör kriminella grupperingar har tillgång till explosiva varor i större utsträckning än tidigare och också har en större benägenhet att använda dessa. När hanteringen av explosiva varor har koppling till kriminella grupperingar finns en påtaglig risk för att den explosiva varan ska komma till användning i samband med brott. Enligt regeringens uppfattning är det angeläget att förhindra att dessa varor olovligen förs in i landet. Vidare konstaterades att förebyggande av olaglig hantering av explosiva varor är en prioriterad fråga inom EU.

Vi bedömer att det är ytterst angeläget med goda möjligheter att kunna utreda brotten och att identifiera en skäligen misstänkt. Straffskalan för grov vapensmuggling respektive grov smuggling av explosiva varor är fängelse i lägst två och högst fem år. Vi anser att brotten bör läggas till i brottskatalogen. Av motsvarande skäl bör grovt vapenbrott och grovt brott mot lagen (2011:1011) om brandfarliga och explosiva varor, som har samma straffskala som de nyss nämnda smugglingsbrotten, också läggas till i katalogen.

Sexualbrott

Som angetts i avsnitt 9.5 kan det finnas ett behov i ärenden om allvarliga sexualbrott mot vuxna. Både våldtäkt och grovt sexuellt övergrepp ingår i den nuvarande brottskatalogen för hemlig rumsavlyssning. Om det är av synnerlig vikt för att man ska kunna hitta en skäligen misstänkt är det enligt vår mening motiverat att man kan använda hemlig avlyssning eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter. Samma sak gäller i fråga om grovt sexuellt övergrepp under förutsättningen att straffvärdet är sådant

att hemlig avlyssning av elektronisk kommunikation är tillåten enligt någon av straffvärdeventilerna.

Sexualbrott mot barn och barnpornografi

Vi bedömer att sexualbrott mot barn är en sådan brottskategori som det är särskilt angeläget att beivra och som även i övrigt uppfyller de kriterier som vi nyss ställt upp. De grova sexualbrotten mot barn ingår i den nuvarande brottskatalogen för hemlig rumsavlyssning (våldtäkt mot barn, grovt sexuellt övergrepp mot barn, grovt utnyttjande av barn för sexuell posering). Även grovt barnpornografibrott ingår i den nämnda brottskatalogen.

Det är fråga om särskilt avskyvärd brottslighet och om gärningspersoner som ofta har ett stort antal offer. Inte minst sexualbrott mot barn via nätet är ofta massbrottslighet som kan begås mot många barn, på olika fysiska platser och snabbt. Det är därför av yttersta vikt att man kan identifiera gärningspersonen så snabbt som möjligt och ingripa så att inte fler barn utsätts. Det är inte ovanligt med ett stort antal brott i ett och samma ärende. En av dessa händelser kan generera information som blir den nyckel som öppnar upp hela ärendet. Ärenden om sexualbrott mot barn börjar ofta med att övergreppsmaterial (dvs. barnpornografiskt material) påträffas. Det kan vara bilder eller filmer som visar allvarliga sexuella övergrepp mot barn. I många fall är barnets identitet okänd och barnet kan finnas var som helst i världen. Det är av synnerlig vikt att få stopp på denna typ av gärningar med hänsyn till risken för att fler barn utsätts. Det finns ofta en förslagenhet och en systematik i dessa ärenden genom det specifika modus som den enskilde gärningspersonen arbetar utifrån. I fall av sexuella övergrepp i digital miljö sker kommunikation mellan den misstänkte och barnet, eller en vuxen person i barnets närhet som möjliggör övergreppet, i regel digitalt. I dessa fall kan hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning ge information som är nödvändig för att man ska kunna identifiera gärningsmannen. När övergreppsmaterial påträffas är situationen ofta motsvarande den som gäller vid andra komplexa cyberbrott (se bl.a. avsnitt 7.5). Behovet av en möjlighet att kunna använda såväl hemlig övervakning som hemlig avlyssning av elektronisk kommunikation som motsvarande former av hemlig dataavläsning är alltså stort. Detta

gäller även barnpornografibrott av normalgraden, som dock har en straffskala – fängelse i högst två år – som innebär att det i dagsläget i princip är uteslutet med en hemlig avlyssning av elektronisk kommunikation och därmed även med en hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas.

De stora utredningssvårigheter som föreligger vid särskilt internetrelaterad sexualbrottslighet mot barn och barnpornografibrott talar enligt vår mening starkt för att hemliga tvångsmedel ska kunna användas i syfte att utreda vem som ligger bakom. Här har barns särskilda skyddslöshet och vikten av att sexuella övergrepp mot barn kraftfullt motverkas en stor betydelse. Vi menar att även barnpornografibrott typiskt sett är att anse som allvarlig brottslighet, trots den relativt lindriga straffskalan. I många fall handlar det om dokumenterade sexuella övergrepp mot barn – övergrepp som dessutom många gånger upplevs som värre för att de dokumenterats. Efterfrågan efter övergreppsmaterial medför i sig att barn utsätts för sexuella övergrepp.

Vi har i avsnitt 7.4 föreslagit att sexualbrotten mot barn och barnpornografibrott läggs till i brottskatalogen för hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning förutom sådan som gäller rumsavlyssningsuppgifter. Med hänsyn till vikten av att dessa brott kan utredas effektivt och till det stora behovet av en möjlighet till hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att utreda vem som skäligen kan misstänkas, talar starka skäl för att brotten läggs till även i den brottskatalog som vi diskuterar i detta avsnitt. Detta skulle innebära att det blir möjligt att använda både hemlig övervakning och hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet. Motsvarande ändring skulle då få göras i lagen om hemlig dataavläsning. Fördelarna från ett utredningsperspektiv med en sådan lösning är betydande. Vi anser även att den skulle vara såväl effektiv som proportionerlig. Vi föreslår därför att de angivna brotten läggs till i brottskatalogen.

Brotten i den nuvarande brottskatalogen

Hemlig avlyssning av elektronisk kommunikation kan i dag förekomma för ett antal särskilt uppräknade brott (i skrivande stund i 27 kap. 2 § andra stycket 2–7 och enligt förslag i prop. 2021/22:119

i 18 § andra stycket 2–7). Katalogen innehåller vissa brott mot rikets säkerhet, allmänfarliga brott, högmålsbrott och terroristbrott. Det framstår som uppenbart behövligt och även proportionerligt att även dessa brott ska ingå i brottskatalogen.

9.10.4 Osjälvständiga brottsformer

Förslag: Tvångsmedlen ska kunna användas i det nya syftet även vid misstanke om försök, förberedelse och stämpling.

Skälen för förslaget

I likhet med vad som gäller i övrigt bör försök, förberedelse eller stämpling till ett brott som kan läggas till grund för ett tillstånd till hemlig avlyssning av elektronisk kommunikation eller hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter också kunna föranleda respektive tvångsmedel. Detta bör anges uttryckligen.

9.11 Hemlig dataavläsning avseende lagrade uppgifter och användningsuppgifter

Bedömning: Det bör inte införas någon möjlighet till hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet gällande sådana uppgifter som avses i 2 § första stycket 6 och 7 lagen om hemlig dataavläsning.

Skälen för bedömningen

I kapitel 6 har vi gjort bedömningen att den nya straffvärdeventilen för viss flerfaldig brottslighet bör omfatta sådana uppgifter som avses i 2 § första stycket 6 och 7 lagen om hemlig dataavläsning, dvs. uppgifter som finns lagrade i informationssystemet och uppgifter som visar hur informationssystemet används, förutsatt att det inte är fråga om uppgifter som avses i de övriga punkterna i första stycket. Motsvarande bedömning har gjorts i kapitel 7 i fråga om de utökade brotts-

kataloger som föreslås där. Utöver effektivitetsskäl vilar förslagen vilar på en principiell bedömning att möjligheten att använda hemlig dataavläsning i syfte att få tillgång till olika uppgiftstyper bör vara densamma även när nya brott läggs till.

Effektivitetsskäl talar för att även hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet bör kunna omfatta uppgifter som avses i 2 § första stycket 6 och 7. Det finns dock även tungt vägande skäl som talar för att de uppgifter som avses i punkterna 6 och 7 inte bör inkluderas.

Dataavläsning enligt 2 § första stycket 6 och 7 ger tillgång till en stor mängd nya uppgifter, inte minst när det gäller uppgifter som finns lagrade i det avlästa informationssystemet. Uppgifterna kan vara av ytterst integritetskänsligt slag och kan t.ex. omfatta privata bild- och filmfiler som inte har delats med någon men som finns lagrade i informationssystemet. Det kan till att börja med ifrågasättas om behovet av detta slags uppgifter gör sig gällande på samma sätt i det initiala skede för vilket tvångsmedlet är avsett i det syfte som diskuteras i detta kapitel. Meningen med en möjlighet att använda hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet är inte att samla in bevisning som kan läggas till grund för ett åtal, utan endast att få fram en skäligen misstänkt. Så snart utredningen kommit så långt, kan en hemlig dataavläsning i stället ske enligt bestämmelserna i 4 § lagen om hemlig dataavläsning och riktas mot den skäligen misstänkte. I det läget kan det fattas beslut om avläsning av sådana uppgifter som avses i punkterna 6 och 7. Vidare har det betydelse att redan möjligheten att inhämta kommunikationsavlyssningsuppgifter innan det finns en skäligen misstänkt utgör en nyhet och ett betydande principiellt steg i förhållande till vad som gäller i dag. Den medför en ökad risk för att personer som visar sig vara ovidkommande drabbas av tvångsmedlet. Den omständigheten att det är fråga om en tidsbegränsad försökslagstiftning som ska utvärderas innebär att det är motiverat med särskild försiktighet. Sammantaget bedömer vi att övervägande skäl för närvarande talar emot en möjlighet till avläsning av uppgifter som avses i 2 § första stycket 6 och 7 lagen om hemlig dataavläsning. Vi är därför i nuläget inte beredda att lägga fram något sådant förslag, men konstaterar att det kan vara motiverat att återigen överväga frågan i samband med att lagen utvärderas.

10 Hemlig rumsavlyssning och hemlig kameraövervakning kan knytas till en person

10.1 Uppdraget

Tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning måste enligt dagens regler alltid knytas till en viss plats. Åklagarmyndigheten har väckt frågan om tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning ska få knytas till en person (Ju2019/03572/Å s. 7–13).

Frågan om anknytning mellan person och tvångsmedel har varit föremål för överväganden i flera tidigare lagstiftningsarbeten (se t.ex. prop. 1994/95:227 s. 20–22, prop. 1995/96:85 s. 30–32 och prop. 2013/14:237 s. 96 och 97). I det lagstiftningsärende som föregick lagen (1995:1506) om hemlig kameraövervakning övervägde regeringen om tillståndet skulle knytas till en plats eller en person. Regeringen bedömde då att det skulle medföra svårigheter att tillämpa ändamåls-, behovs- och proportionalitetsprinciperna om tillståndet skulle knytas till en person (prop. 1995/96:85 s. 30). I propositionen Hemlig dataavläsning har regeringen återigen gjort samma principiella bedömning om hemlig dataavläsning och föreslagit att en verkställighet genom hemlig dataavläsning också ska vara underkastad ett platskrav (prop. 2019/20:64 s. 118–120). Detta ställningstagande ligger även i linje med den slutsats som dras i propositionen Ett förenklat förfarande vid vissa beslut om hemlig avlyssning, nämligen att det inte finns tillräckliga skäl att knyta tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation till en person. Skälen till detta är bl.a. att det är viktigt att domstolen i sin proportionalitetsprövning kan ta ställning till

den konkreta avlyssnings- eller övervakningsåtgärd som ska utföras (prop. 2019/20:145 s. 14).

Åklagarmyndigheten uppger att grovt kriminella personer är ytterst säkerhetsmedvetna. Det har gjort att det blivit vanligt att misstänkta personer träffas på allmänna platser där de känner sig säkra på att kunna tala utan risk för att bli avlyssnade. Den tekniska utvecklingen har gjort att utrustningen för att verkställa hemlig rumsavlyssning och hemlig kameraövervakning kan anpassas efter de misstänkta personerna snabbare än tidigare med minskade risker för att utomstående personer drabbas av tvångsmedlet (Ju2019/03572/Å s. 7, 8 och 12).

Det anges i direktiven att det alltjämt finns starka betänkligheter mot att knyta ett tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning till en person i stället för en viss plats. Mot bakgrund av förändringen av de brottsaktiva personernas beteende och den ovan beskrivna tekniska utvecklingen finns det dock enligt direktiven tillräckliga skäl att i detta sammanhang återigen analysera frågan.

Vi ska därför

- ta ställning till om tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning bör kunna knytas till en person, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Eftersom hemlig dataavläsning kan vara en metod för att få tillgång till rumsavlyssningsuppgifter och kameraövervakningsuppgifter omfattar våra överväganden även hemlig dataavläsning avseende dessa uppgiftstyper inom ramen för en förundersökning.

Bestämmelser om krav på koppling till en viss plats vid preventiv hemlig kameraövervakning finns i 3 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Ett motsvarande krav finns avseende preventiv hemlig dataavläsning avseende kameraövervakningsuppgifter, 7 § tredje stycket lagen om hemlig dataavläsning. Vi bedömer att en översyn av dessa bestämmelser sträcker sig längre än vad som följer av vårt uppdrag att föreslå följdändringar. Vi har inte heller möjlighet att ta upp frågan utan att det skulle leda till fördröjningar. Några överväganden om dessa bestämmelser redovisas alltså inte (se även avsnitt 15.6). Vi vill dock framhålla att det kan finnas anledning att se över bestämmelserna i något annat sammanhang.

Det framgår av Åklagarmyndighetens framställan att det som efterfrågas är en alternativ möjlighet när det finns ett behov, och alltså inte ett slopande av huvudregeln om ett krav på att tvångsmedlet knyts till en plats. Våra överväganden bygger på denna premiss. Vi överväger alltså inte ett fullständigt slopande av kravet på att en hemlig rumsavlyssning och en hemlig kameraövervakning som huvudregel ska vara knuten till en viss plats, utan enbart om huvudregeln kan förses med några modifieringar eller undantag. Samma begränsning gäller våra överväganden om hemlig dataavläsning.

10.2 Gällande rätt

Hemlig kameraövervakning och hemlig dataavläsning avseende kameraövervakningsuppgifter

Hemlig kameraövervakning innebär att man i hemlighet använder fjärrstyrda tv-kameror, andra optisk-elektroniska instrument eller därmed jämförbara utrustningar för optisk personövervakning vid förundersökning i brottmål (27 kap. 20 a § första stycket RB). Bestämmelserna om hemlig kameraövervakning omfattar endast kameror som används för personövervakning och som inte manövreras på platsen (jfr prop. 1989/90:119 s. 14 f. och 39 ff.) I rättstillämpningen har åtgärden ansetts omfatta övervakning med fjärrstyrda drönare.

Åtgärden får, förutom i ett visst fall, endast avse en plats där den skäligen misstänkte kan antas komma att uppehålla sig (27 kap. 20 b § andra stycket RB). Undantaget är om man använder åtgärden i syfte att fastställa vem som skäligen kan misstänkas. I ett sådant fall kan åtgärden avse den plats där brottet har begåtts eller en nära omgivning till denna plats (27 kap. 20 c § RB).

Kameraövervakningsuppgifter kan även inhämtas med hjälp av hemlig dataavläsning (1 § lagen om hemlig dataavläsning). Det kan då t.ex. gå till så att man på distans aktiverar en webbkamera i den misstänktes dator. När det gäller platsen för åtgärden gäller i princip samma begränsningar som vid hemlig kameraövervakning. Dock finns det inte någon möjlighet att använda hemlig dataavläsning som gäller kameraövervakningsuppgifter i syfte att utreda eller fastställa vem som skäligen kan misstänkas för brottet (5 § första stycket samma lag). Åtgärden får aldrig avse någons stadigvarande bostad.

Hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter

Hemlig rumsavlyssning avser en avlyssning eller upptagning som görs i hemlighet 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 (27 kap. 20 d § första stycket RB). Åtgärden får bara avse en plats där det finns särskild anledning att anta att den skäligen misstänkte kommer att uppehålla sig. Kravet på särskild anledning innebär ett starkare krav än det som gäller för hemlig kameraövervakning. Det krävs att det finns någon faktisk omständighet som med viss styrka talar för att den misstänkte kommer att uppehålla sig på platsen (prop. 2005/06:178 s. 101). Om åtgärden avser någon annan stadigvarande bostad än den misstänktes, får hemlig rumsavlyssning användas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där (27 kap. 20 e § andra stycket RB). Kravet på synnerlig anledning innebär att det med fog ska kunna förvänta att den misstänkte kommer att uppehålla sig där (anförd prop. s. 101).

Vissa platser är skyddade från hemlig rumsavlyssning. Det gäller bl.a. platser som används för verksamhet som omfattas av tystnadsplikt enligt 3 kap. 3 § tryckfrihetsförordningen och läkarmottagningar (27 kap. 20 e § tredje stycket RB).

De brottsbekämpande myndigheterna kan även få tillgång till rumsavlyssningsuppgifter med hjälp av hemlig dataavläsning (1 § lagen om hemlig dataavläsning). Detta kan t.ex. ske genom att mikrofonen på den misstänktes telefon aktiveras. Hemlig dataavläsning avseende rumsavlyssningsuppgifter får bara användas vid förundersökningar om brott som hade kunnat föranleda hemlig rumsavlyssning (6 § första stycket lagen om hemlig dataavläsning). När det gäller platsen för åtgärden gäller samma begränsningar som vid hemlig rumsavlyssning (6 § andra och tredje styckena samt 13 § samma lag).

10.3 Tidigare överväganden

Propositionen Hemlig teleavlyssning och hemlig teleövervakning

Som nämnts har frågan om kopplingen mellan person och tvångsmedel varit föremål för överväganden i flera lagstiftningsarbeten. År 1995 infördes ändringar i rättegångsbalken som syftade till att göra bestämmelserna om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation mer teknikneutrala för att underlätta verkställigheten av tvångsmedlen. Ändringarna byggde på förslag i propositionen Hemlig teleavlyssning och hemlig teleövervakning (prop. 1994/95:227 s. 20 f.) Regeringen övervägde där frågan om det skulle vara möjligt att reglera tillämpningsområdet för hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation genom att endast låta åtgärden avse telemeddelanden med viss anknytning till den misstänkte. Regeringen konstaterade i propositionen att det är nödvändigt, inte minst från integritetssynpunkt, att en bestämmelse om vad som får avlyssnas och övervakas är så utformad att domstolen kan ta ställning till den konkreta åtgärd som avses vid tillståndsgivningen. Men framför allt är det från tillämpningssynpunkt ett oeftergivligt krav att ett beslut om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation kan konkretiseras. I annat fall blir beslutet inte praktiskt verkställbart. I propositionen behandlades Datastraffrättsutredningens överväganden i betänkandet Information och den nya informationsteknologin – straff och processrättsliga frågor m.m. (SOU 1992:110).

Propositionen Hemlig kameraövervakning

Frågan om kopplingen mellan person och tvångsmedel var också aktuell i det lagstiftningsärende som föregick lagen (1995:1506) om hemlig kameraövervakning. Den aktuella frågan var då om tillståndet till det nya tvångsmedlet skulle avse en person eller plats. Regeringen konstaterade i propositionen Hemlig kameraövervakning att frågan huruvida ett tillstånd till hemlig kameraövervakning ska avse en viss person eller plats hänger samman med ändamåls-, behovs- och proportionalitetsprinciperna. Om ett tillstånd till hemlig kameraövervakning skulle avse en viss person blir principerna enligt regeringen

svåra att tillämpa. Det skulle t.ex. i den situationen inte gå att tillämpa proportionalitetsprincipen eftersom det på förhand inte skulle vara känt vilka eller hur många platser som skulle komma att övervakas (prop. 1995/96:85 s. 29 f.) Även andra, rent praktiska, skäl ansågs tala mot att knyta övervakningen till en viss person. Regeringen anförde då följande.

> Om det inte på förhand kan anges vilka platser som kan bli aktuella för övervakning torde det ändå inte gå att undvara spaningspersonal på platsen. Den misstänkte måste ju hela tiden bevakas och kameror skulle behöva sättas upp och monteras ned beroende på den misstänktes rörelsemönster. Det torde vara förenat med betydande svårigheter och opraktiskt att organisera en övervakning på det sättet.
>
> Det finns även en risk för att antalet kameror skulle bli mycket stort.

Regeringen tog avstånd ifrån att regleringen skulle förses med en begränsning av de platser som får övervakas med dolda övervakningskameror utöver de begränsningar som följer av att åtgärden endast får avse en sådan plats där den misstänkte kan antas komma att uppehålla sig och av de allmänna principer som gäller för all tvångsmedelsanvändning. Det ansågs därmed att det inte skulle vara lämpligt med en begränsning till övervakning av allmänna platser, eller ett förbud mot övervakning som består i att övervakningskameran riktas mot fönstret i en bostad.

I propositionen behandlades överväganden i betänkandet Polisens användning av övervakningskameror vid förundersökning (SOU 1995:66). I den nu aktuella delen överensstämde utredningens förslag med regeringens.

Beredningen för rättsväsendets utveckling

Beredningen för rättsväsendets utveckling (BRU) tog i samband med förslag om en möjlighet till hemlig övervakning av elektronisk kommunikation utan att det fanns en misstänkt gärningsman, upp frågan om att knyta tillståndet till en person i betänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38). Utredningen föreslog att det i sådana fall inte skulle ställas något krav på att det i beslutet anges vilken teleadress tillståndet till hemlig övervakning gäller. Utredningen ansåg att den snabba tekniska utvecklingen och de metoder som de kriminella personerna använder för

att undgå tvångsmedlen hade gjort att regeringens tidigare uttalanden om integritet och verkställighet behövde omprövas (s. 199 f.). BRU:s förslag i denna del ledde inte till lagstiftning.

Propositionen Hemliga tvångsmedel mot allvarliga brott

I propositionen Hemliga tvångsmedel mot allvarliga brott (prop. 2013/14:237) lämnade regeringen förslag till en reglering om hemliga tvångsmedel som bl.a. innebar att de tidsbegränsade lagarna om hemliga tvångsmedel skulle göras permanenta med vissa justeringar. Inom ramen för överväganden om rekvisiten för tvångsmedelsanvändningen övervägde regeringen kravet på kopplingen mellan åtgärden och en viss adress, utrustning eller plats. De brottsbekämpande myndigheterna hade anfört att kravet på att en viss adress, utrustning eller plats ska anges i beslutet utgjorde ett betydande effektivitetshinder i myndigheternas verksamhet. Regeringen ansåg att det fanns faktorer som talade för en ändrad reglering, så som svårigheten att inhämta ett beslut om tvångsmedel i tid när kriminella med kort varsel beslutar om t.ex. platsen för ett viktigt möte samt att många tillstånd till hemlig avlyssning och hemlig övervakning är identiska med redan löpande tillstånd förutom i fråga om teleadressen. Trots det ansåg regeringen att integritets- och rättssäkerhetsskäl alltjämt talade för att lagstiftningen borde vara utformad på ett sådant sätt att beslutsfattaren kan ta ställning till den konkreta åtgärd som avses vid tillståndsgivningen. Förutsättningarna för delar av den initiala prövningen, bl.a. tillämpningen av proportionalitetsprincipen, skulle enligt regeringen försämras om åtgärden inte var bestämd till en viss adress, plats eller liknande. Dessutom ansågs det att beslutsfattarens möjligheter sannolikt också skulle minska när det gäller att bedöma i vilken mån ett tillstånd behöver förenas med villkor för att tillgodose intresset av att enskildas integritet inte kränks i onödan (anförd prop. s. 97). För att möta behovet av ett snabbt beslutsfattande utökades åklagarnas möjligheter att fatta interimistiska beslut till att även omfatta hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och kvarhållande av försändelse (anförd prop. s. 136 f.). I propositionen behandlades överväganden i betänkandet Hemliga tvångsmedel mot allvarliga brott (SOU 2012:44). I frågan om kravet på att tillståndet

skulle knytas till en viss plats m.m. överensstämde utredningens förslag med regeringens.

Propositionen Hemlig dataavläsning

Regeringen tog i propositionen Hemlig dataavläsning ställning mot att knyta hemlig dataavläsning till en person på grund av de skäl som anförts ovan (prop. 2019/20:64 s. 118 f., i vilken behandlas överväganden i SOU 2017:89). Regeringen anförde även följande (s. 86).

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

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

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

Med denna begränsning ansåg regeringen att hemlig dataavläsning för att ta del av kameraövervakningsuppgifter och rumsavlyssningsuppgifter inte skulle innebära någon beaktansvärd ökad risk för den personliga integriteten.

Propositionen
Ett förenklat förfarande vid vissa beslut om hemlig avlyssning

Motsvarande bedömning gjordes i propositionen Ett förenklat förfarande vid vissa beslut om hemlig avlyssning (prop. 2019/20:145). Några överväganden om hemlig rumsavlyssning görs inte i propositionen men uttalandena om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation är ändå av visst principiellt intresse. Regeringen anförde då bl.a. följande (s. 12–14). Om tillståndet till avlyssning eller övervakning knyts till en person skulle bedömningen av kopplingen mellan nummer, adress eller utrustning och den person som ska avlyssnas inte längre kunna göras av rätten. Den bedömningen skulle i stället förskjutas till åklagare eller den verkställande myndigheten. Rättens prövning skulle då inskränkas till att bedöma om personen är skäligen misstänkt för ett brott som kan motivera åtgärden och om åtgärden är av synnerlig vikt för utredningen. Även prövningen av om åtgärden är proportionerlig skulle alltjämt vara en fråga för rätten, men regeringen ansåg att det på goda grunder kan ifrågasättas hur reell denna prövning skulle bli. Det skulle exempelvis inte vara möjligt för rätten att bedöma om det är proportionerligt att tillåta hemlig övervakning eller avlyssning av en utrustning som brukas av flera personer utöver den misstänkte, t.ex. en dator på ett bibliotek eller en telefon som används på den misstänktes arbetsplats. Regeringen framhöll att integritetsskyddsintressen är särskilt viktiga när det gäller avlyssning eller övervakning av ett telefonnummer som inte tillhör den misstänkte men som denne kan förväntas kontakta (27 kap. 20 § första stycket 2 RB och 2 § första stycket 2 preventivlagen). De möjligheter som rätten i dag har att föreskriva villkor i tillståndet om att avlyssning eller övervakning endast får ske vid vissa givna förutsättningar, skulle enligt regeringen inte längre finnas. I de angivna fallen skulle proportionalitetsbedömningen och möjligheten att föreskriva integritetsskyddande villkor lämnas över till åklagaren eller den verkställande myndigheten.

Även möjligheten för rätten och de offentliga ombuden att bevaka integritetsskyddsintressen skulle enligt regeringen försämras. Regeringen landade i att den effektivitetsvinst som skulle kunna bli följden av en ordning där tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation knyts till en person i stället för till ett telefonnummer eller annan adress eller till en viss elektronisk kommunikationsutrustning inte stod i proportion till de rättssäkerhets- och integritetsskyddsförluster som skulle uppstå.

I propositionen behandlades övervägandena i betänkandet Förenklat förfarande vid vissa beslut om hemlig avlyssning (SOU 2018:30). Utredningens bedömning i frågan om koppling till en viss adress m.m. överensstämde med regeringens.

Platsbegreppet

Förarbetena ger endast indirekt ledning för vad som avses med en plats. I prop. 2005/06:178 Hemlig rumsavlyssning (s. 59, 62, 100 och 104) anges att tal som får tas upp genom tvångsmedlet avser tal i rummet. Hemlig rumsavlyssning kommer därför att förutsätta att ett dolt tekniskt hjälpmedel placeras ut på en viss plats eller i ett visst utrymme, t.ex. i ett rum eller i en bil. Ett beslut om hemlig rumsavlyssning bör mot den bakgrunden avse en viss plats, anges det. Vidare framgår av förarbetena att rumsavlyssningen kan avse en lokal som inte disponeras av den misstänkte, t.ex. ett garage som tillhör en bekant, och att avlyssningen kan ske utomhus, t.ex. i en park, eller inomhus, t.ex. i en galleria eller i en bostad. Det framhålls även att proportionalitetsprincipen får särskild betydelse vid rättens prövning i fråga om den plats som begärs avlyssnad och vilket slags intrång som är nödvändigt för att genomföra åtgärden. Av prop. 1995/96:85 Hemlig kameraövervakning framgår att hemlig kameraövervakning kan avse både allmänna och enskilda platser och att det ska vara fråga om en ”särskilt angiven” plats (s. 30–32 och 39).

Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel uppmärksammade att definitionen av plats tolkas olika av domstolarna i ärenden om tillstånd till hemlig rumsavlyssning (SOU 2018:61 s. 126–128). Enligt uppgift från Polismyndigheten och Säkerhetspolisen ställer vissa domare hårda krav på att platsen ska anges mycket specifikt medan andra godtar betydligt mer diffusa

definitioner, t.ex. den plats längs en viss väg där den misstänkte uppehåller sig. Utredningen hade gjort en genomgång av samtliga domstolsbeslut om hemlig rumsavlyssning som meddelats under 2017. Denna visade att platserna i tillstånden för det mesta hade varit avgränsade till t.ex. ett fordon eller en lägenhet. Men det hade också förekommit att platsen angetts diffust. Som ett exempel angavs att tillstånd getts till hemlig rumsövervakning på ”offentlig plats i Stockholm där ett möte kan förväntas äga rum”. I det specifika fall där tillståndets formulerats på detta sätt var tillståndet inte förenat med några särskilda villkor till skydd för enskildas personliga integritet. Utredningen anförde följande.

> Enligt vår mening är det uppenbart att den plats som anges i tillståndet som huvudregel ska avse en tydligt begränsad yta. I annat fall skulle det vara omöjligt att vid tillståndsprövningen kunna överblicka risken för onödiga integritetsintrång. Om den brottsbekämpande myndigheten t.ex. skulle få möjlighet att avlyssna den plats i en viss stad där den misstänkte befinner sig, skulle det innebära att proportionalitetsbedömningen helt skulle ligga i de brottsbekämpande myndigheternas händer och därmed falla utanför domstolens förhandsprövning, vilket inte tycks ha varit lagstiftarens avsikt. (Jämför även prop. 1995/96:85 s. 29 angående kameraövervakning.) Bedömningen av hur stor en plats kan vara kan emellertid inte göras fristående utan måste prövas utifrån flera aspekter, såsom typ av plats, risk för integritetsintrång och om tillståndet kan förenas med särskilda villkor. Det ska även beaktas att det är fråga om användning av ett särskilt ingripande tvångsmedel och att bestämmelsen därför ska tolkas restriktivt, jämför prop. 2005/06:178 s. 99 och NJA 1996 s. 577. För det fall det är nödvändigt att ha en relativt vid plats, t.ex. ett torg, är det enligt vår mening viktigt att förena tillståndet med särskilda villkor. Sådana villkor kan vara att endast samtal som den misstänkte deltar i får avlyssnas, att avlyssningen endast får ske när den misstänkte befinner sig på platsen och under vissa tider eller att avlyssning bara får vara aktiv när man genom fysisk spaning har bekräftat att den misstänkte är närvarande. En så vid och diffus plats som en hel stad är emellertid svår att avgränsa tillräckligt ens med särskilda villkor.

Utredningen konstaterade att det är ofrånkomligt att det kan uppstå vissa skillnader i domstolarnas bedömningar och menade att det fanns ett behov av mer vägledande överrättspraxis och andra åtgärder för att göra tillämpningen mer enhetlig. Bestämmelsen om plats ansågs oaktat det inte så oklar att den inte uppfyller kraven i regeringsformen och Europakonventionen.

SIN har i ett uttalande den 28 mars 2018, dnr 111-2017, uttalat att en ansökan om hemlig kameraövervakning ska föregås av en ingå-

ende prövning av hur tvångsmedlet ska verkställas. Uppgifter om antalet kameror och var de ska placeras bör enligt nämnden normalt anges i ansökan, eftersom de uppgifterna är av central betydelse vid rättens proportionalitetsprövning och av vikt för prövningen av om tillståndet ska förenas med särskilda villkor.

I RH 2015:32 avslog Svea Hovrätt en begäran om tillstånd till hemlig rumsavlyssning avseende ”avlyssning av den misstänkte på offentlig plats i Sverige med den begränsning som anges i 27:20e RB vid övervakande samtal mellan den misstänkte och andra personer av särskilt intresse”. Beslutet motiverades med att åklagaren inte hade angett någon plats.

10.4 Behovet av en möjlighet att knyta vissa hemliga tvångsmedel till en person

Bedömning: Det finns ett påtagligt behov av en möjlighet att knyta ett tillstånd till hemlig rumsavlyssning, hemlig kameraövervakning och hemlig dataavläsning som gäller rumsavlyssnings- eller kameraövervakningsuppgifter till den skäligen misstänkte.

Skälen för bedömningen

Hemlig rumsavlyssning

I dag är många grovt kriminella personer ytterst säkerhetsmedvetna. Det gör det svårt för de brottsbekämpande myndigheterna att oupptäckta bereda sig tillträde till deras bostäder. Personerna är också väl medvetna om möjligheten att de kan bli avlyssnade i sina fordon men även på avgränsade platser såsom caféer och liknande. Detta gör dem försiktiga när det gäller att prata om brott i fordonen eller på sådana platser. Samtidigt inser de risken för att deras telefonsamtal kan bli föremål för hemlig avlyssning av elektronisk kommunikation. Därför använder de ofta krypterade telefoner och olika applikationer för att kommunicera. Det har också blivit vanligt att personerna träffas för att prata på sådana allmänna platser där de känner sig säkra på att kunna tala utan risk för avlyssning, t.ex. när de är på väg till eller från sitt fordon, under promenader eller vid andra möten i stadsmiljö eller

på andra platser som är tillgängliga för allmänheten. Det enda hemliga tvångsmedel som med nuvarande lagstiftning står till buds för att uppfatta sådana personers kommunikation är hemlig rumsavlyssning (eller hemlig dataavläsning avseende rumsavlyssningsuppgifter). Samtidigt är det ofta svårt att på förhand veta exakt var misstänkta personers möten och samtal kan komma att äga rum.

Enligt uppgift från de brottsbekämpande myndigheterna har utvecklingen lett till att det är relativt vanligt att man avstår från att ansöka om tillstånd till hemlig rumsavlyssning, eftersom det inte är möjligt att ange en specifik plats där åtgärden ska ske. I ett exempel som lämnats av Åklagarmyndigheten var det känt att de misstänkta kontinuerligt träffades på olika platser. Genom hemlig avlyssning av elektronisk kommunikation fick de brottsbekämpande myndigheterna kännedom om att de misstänkta skulle träffas, men själva mötesplatserna bestämdes vid krypterad kommunikation som man inte kunde ta del av i klartext. Åklagaren i ärendet övervägde att begära hemlig rumsavlyssning på alla de platser där möten ägt rum men avstod från detta efter diskussion med polisen, som ansåg att åtgärden skulle kräva en stor arbetsinsats samtidigt som utgången skulle vara osäker eftersom mötet lika gärna skulle kunna komma att äga rum på en ny plats.

Utvecklingen har även lett till att åklagare i vissa fall begärt och ibland även fått domstolens tillstånd till hemlig rumsavlyssning på större bestämda platser, såsom den plats längs en viss väg där den misstänkte kan förväntas uppehålla sig eller på offentlig plats i en viss angiven stad där ett möte kan förväntas äga rum (jfr SOU 2018:61 s. 127 och 127). Ofta men inte alltid har besluten förenats med villkor i syfte att minimera integritetsintrånget för tredje man. De brottsbekämpande myndigheterna har för oss beskrivit flera sådana exempel som vi återger i det följande.

I ett ärende som beskrivits av åklagare stod det klart att ett möte skulle äga rum mellan de två huvudmännen, men det var oklart var. Åklagaren ansökte om och beviljades tillstånd till hemlig rumsavlyssning på allmän plats och i skog och mark i en viss angiven stad. Tillståndet förenades med villkor att avlyssning fick ske i samband med möten mellan de två misstänkta och under spaning. Det enda som avlyssnades var samtalen mellan de två misstänkte när de diskuterade kommande brott. Enligt åklagaren gav denna hemliga rumsavlyssning mer än all utredning som fram till dess skett i ärendet som pågått en längre tid. I samma utredning avslogs dock vid ett senare

tillfälle en likadant formulerad begäran inför ett annat möte som planerades mellan de två misstänkta. Tid och plats var inte heller denna gång kända mer än att det handlade om en viss stad och under en relativt begränsad tidsperiod.

I ett tillstånd till hemlig rumsavlyssning i en mordutredning angavs platsen som ”i anslutning till väg E6 mellan Skåne och Stockholm samt på annan plats i Sverige där den misstänkte befinner sig och där detta kan bekräftas med fysisk spaning”. Avlyssningen skulle verkställas genom att polis med portabel avlyssningsutrustning skulle närma sig den misstänkte.

I ett ärende gällande förberedelse till mord beviljade tingsrätten hemlig rumsavlyssning i det hotellrum där den misstänkte skulle checka in. Vid tidpunkten för beslutet var det inte känt vilket hotell samt vilken bil som de misstänkta skulle komma att hyra. Rumsavlyssningen var kopplad till att det genom spaning eller avlyssning kunde konstateras att en för brottet skäligen misstänkt person uppehåller sig på platsen eller agerar inom brottsplanen.

Utvecklingen att domstolarna ibland anger platsen väldigt brett eller diffust kan ses som en uppluckring av platsbegreppet. Regeringen har vid flera tillfällen uttalat att en bestämmelse om vad som får avlyssnas och övervakas måste vara så utformad att domstolen kan ta ställning till den konkreta åtgärd som avses vid tillståndsgivningen (se bl.a. prop. 1994/95:227 s. 20 f.). Detta måste rimligen förstås på så sätt att lagstiftaren tänkt sig att en ansökan som huvudregel ska innehålla en tämligen precis uppgift om var en avlyssningsanordning ska vara placerad, så att domstolen kan ta ställning till risken för att avlyssningen leder till integritetsintrång för tredje man och till behovet av särskilda villkor för att minska detta integritetsintrång.[1] Man kan ifrågasätta värdet av en platsangivelse som är så allmänt formulerad att det inte med hjälp av den fullt ut går att bedöma integritetsriskerna för tredje man, i vart fall om den inte förenas med tydliga begränsande villkor. Samtidigt kan lagstiftaren knappast heller ha föreställt sig att det praktiska tillämpningsområdet för tvångsmedlet skulle krympa på det sätt som skett på grund av de kriminellas beteende.

Enligt uppgift från de brottsbekämpande myndigheterna har det under de senaste åren blivit mer regel än undantag att kriminella väljer att ha sina fysiska samtal på platser där de känner sig trygga från risken för avlyssning, såsom utomhus på promenad, på en park-

[1] Jfr SIN den 28 mars 2018, dnr 111-2017.

bänk eller liknande. Det är alltså alltmer sällan som hemlig rumsavlyssning kan verkställas i ett avgränsat utrymme. Tendensen till uppluckring av platsbegreppet kan knappast förstås på något annat sätt än som en anpassning av rättstillämpningen till denna utveckling. Som angetts har det har samtidigt framkommit att domstolarnas praxis varierar när det gäller hur preciserat en plats måste anges för att tillstånd ska ges, och att vissa domstolar ställer höga krav på precisering. Som nämnts tidigare är det relativt vanligt att de brottsbekämpande myndigheterna avstår från att ansöka om tillstånd eftersom en specifik plats inte kan anges. Med hänsyn till det anförda är det enligt vår bedömning uppenbart att den gällande regleringen om hemlig rumsavlyssning inte möter den brottsbekämpande verksamhetens behov av en möjlighet att kunna anpassa en hemlig avlyssning till den misstänktes agerande.

Vi lämnar i kapitel 11 förslag om att åklagare ska få möjlighet att fatta interimistiska beslut om hemlig rumsavlyssning och tillträdestillstånd för installation av utrustning för sådan avlyssning. Dessa förslag bedöms i första hand minska de olägenheter som följer av att behov av tillstånd till hemlig rumsavlyssning kan behöva fattas under tider då domstolarna inte är tillgängliga. I viss mån bedöms de även kunna göra det möjligt att få till stånd beslut när möten blir kända med kort varsel eller en mötesplats ändras och det inte går att få till en domstolsprövning. Regeringen har i tidigare lagstiftningsärenden angående hemliga tvångsmedel tagit upp möjligheten till interimistiska beslut som ett argument mot att man tar bort kravet på att en viss adress, utrustning eller plats ska anges i beslutet (prop. 2013/14:237 s. 136 f.). De brottsbekämpande myndigheterna har anfört att det visserligen är nödvändigt att införa en möjlighet till interimistiskt beslutsfattande, men att en sådan möjlighet inte fullt ut tillgodoser dagens behov. I de fall då de misstänkta stämmer träff eller ändrar mötesplats med kort varsel kan visserligen en åklagare i vissa fall fatta ett interimistiskt beslut, men man bör enligt de brottsbekämpande myndigheterna inte överskatta denna möjlighet. Åklagaren måste nämligen ha ett tillräckligt underlag som grund för sitt beslut, som huvudregel en skriftlig promemoria, och även ha tillräckligt rådrum för att överväga om åtgärden bör tillåtas och i så fall om den behöver förenas med några villkor. Enligt de brottsbekämpande myndigheterna är förhållandena många gånger sådana att dessa förutsättningar inte är uppfyllda. Även om det rättsligt finns en möjlighet för

åklagaren att fatta ett interimistiskt beslut kan det alltså vara så att tiden inte medger att han eller hon får ett tillräckligt underlag och tillräcklig tid för de överväganden som måste göras. I den minutoperativa verksamheten kan det exempelvis handla om att spanare observerar att ett intressant möte påbörjas och att ett beslut skulle behöva fattas i princip omedelbart. En möjlighet till interimistiska beslut löser inte heller de svårigheter som följer av att de personer som ska avlyssnas är i rörelse utomhus, och att platsen därför inte kan anges med någon precision.

Det anförda leder oss till bedömningen att det nuvarande platskravet kan leda till oacceptabla hinder i den brottsbekämpande verksamheten och att dessa problem endast i viss utsträckning kan motverkas genom att man skapar en möjlighet för åklagare att fatta interimistiska beslut om hemlig rumsavlyssning. Den fråga som ställs i direktiven är om man bör kunna knyta en hemlig rumsavlyssning till den person som ska avlyssnas i stället för till en viss plats. Ett alternativ till en sådan lösning hade kunnat vara att man ändrar regleringen på ett sådant sätt att det uttryckligen blir tillåtet med vidare platsangivelser i fall då man inte på förhand vet var och när olika intressanta möten ska äga rum. Det är dock svårt att se hur en sådan bestämmelse skulle utformas. Som vi angett tidigare kan man vidare ifrågasätta värdet vid en proportionalitetsbedömning av diffusa och vida platsangivelser som t.ex. tar sikte på en hel stad eller ett större område. Platsangivelsen i sig säger i ett sådant fall ganska lite om vad åtgärden innebär i integritetshänseende och risken för integritetsintrång för tredje man. Avgörande blir då snarare om avlyssningen kombineras med särskilda villkor som minskar risken för onödiga integritetsintrång och hur dessa villkor i så fall utformas. Vi anser därför att det inte är någon bra lösning att i lagtexten fokusera på lägre ställda krav i fråga angivande av plats. Vi gör i stället bedömningen att det finns ett påtagligt behov av en möjlighet att knyta ett tillstånd till hemlig rumsavlyssning till den person som ska avlyssnas, och att fokusera på andra sätt att minska risken för onödiga integritetsintrång.

Enligt den nuvarande regleringen får hemlig rumsavlyssning endast avse plats där det finns särskild anledning att anta att den skäligen misstänkte kommer att uppehålla sig (27 kap. 20 e § andra stycket RB). Redan av detta skäl kan det inte komma ifråga att knyta tillståndet till någon annan person än den skäligen misstänkte utan att påtagligt utvidga tillämpningsområdet för tvångsmedlet. Något så-

dant har inte efterfrågats av de brottsbekämpande myndigheterna. Frågan är alltså om det bör finnas en kompletterande möjlighet att i vissa fall knyta ett tillstånd till den skäligen misstänkte i stället för en viss plats och i så fall i vilka fall och på vilka förutsättningar detta bör vara möjligt. Avgörande för bedömningen är då om regleringen kan utformas på ett sådant sätt att beslutsfattaren även utan angivande av en specifik plats får ett tillräckligt bra underlag för sin prövning av om åtgärden bör tillåtas i det konkreta fallet.

Hemlig kameraövervakning

De brottsbekämpande myndigheterna har för oss beskrivit att de kriminellas riskmedvetenhet och anpassade beteende medför svårigheter även när det gäller hemlig kameraövervakning på i första hand allmänna platser. Många gånger kan det enligt myndigheterna vara nödvändigt att kunna spana på den skäligen misstänkte när denne rör sig på allmänna platser, samtidigt som det kan vara omöjligt att genomföra en fysisk spaning utan upptäckt. Ett exempel på detta kan vara att de brottsbekämpande myndigheterna misstänker att det finns en narkotika- eller vapengömma på någon avsides plats, och att man vill kunna följa den misstänkte för att i bästa fall kunna lokalisera gömman och knyta vederbörande till denna. I sådana fall är fysisk spaning ofta utesluten på grund av risken för upptäckt. Samtidigt finns det ingen plats som kan pekas ut i ett tillstånd till hemlig kameraövervakning och ingen möjlighet att placera ut kameror, eftersom man inte på förhand vet var de behövs. Det kan däremot vara möjligt att med exempelvis en kamerautrustad drönare följa och filma den misstänktes väg utan upptäckt. Ett annat exempel är att kriminella väljer avsides mötesplatser och att det finns ett behov av att, utan fysisk polisiär närvaro, kunna få kännedom om och dokumentera vilka som träffats. Vidare finns det vissa områden där kriminella grupperingar utövar sådan övervakning att polisen överhuvudtaget inte kan vistas inom området utan upptäckt. I vissa fall har det handlat om att grupperingen satt upp fysiska vägspärrar, men det förekommer också att personer med koppling till grupperingarna har till uppgift att övervaka vilka som kommer in i området och försäkra sig om att de inte är poliser. En möjlighet till hemlig kameraövervakning kan i sådana områden vara den enda framkomliga vägen för att kunna spana

på den skäligen misstänkte när denne rör sig i området. Med hjälp av drönare kan övervakning utomhus genomföras utan någon föregående installation och utan att man behöver få tillträde till intrångsskyddade utrymmen. Åtgärden kan alltså i vissa fall vidtas snabbt och med relativt begränsade förberedelser. Kameror kan även i vissa andra fall placeras ut relativt snabbt.

Däremot krävs det ofta förberedelser inför en hemlig kameraövervakning i ett utrymme som inte är tillgängligt för allmänheten. En eventuell möjlighet att besluta om tillträdestillstånd även när det inte samtidigt ska ske en hemlig rumsavlyssning – som vi lämnar förslag om i kapitel 12 – kan inte förväntas leda till någon ändring i detta avseende. Det är självklart inte möjligt att vidta förberedande åtgärder på en okänd plats eller inhämta tillstånd till tillträde till en plats som man inte känner till. Det krävs alltså ofta att platsen är känd i förväg för att kameraövervakning ska kunna ske på platser som allmänheten inte har tillträde till. Något behov av en möjlighet att knyta ett tillstånd till hemlig kameraövervakning till en person i stället för en plats finns därför oftast inte med anledning av kameraövervakning som ska verkställas på platser dit allmänheten inte har tillträde. Man kan dock tänka sig att den misstänkte beger sig till en plats, t.ex. en inhägnad tomt som inte är allmän, i syfte att undgå risken för kameraövervakning och att övervakning kan ske utan att man behöver tillträda platsen, t.ex. med hjälp av drönare. Det är också i vissa fall möjligt – och enligt gällande rätt tillåtet – att kameraövervaka exempelvis en bostad genom ett fönster förutsatt att kameran är placerad utanför (se prop. 1995/96:85 s. 30 och 31).

Vi har i tidigare avsnitt beskrivit att utvecklingen har lett till att det ibland fattas beslut om hemlig rumsavlyssning där platsen för avlyssningen anges brett. Sådana exempel finns även när det gäller hemlig kameraövervakning. I ett ärende som vi tagit del av hade tingsrätten i en utredning om förberedelse till mord meddelat tillstånd till hemlig kameraövervakning från luften med hjälp av drönare inom ett område som omfattar tre kommuner. Det offentliga ombudet överklagade och anförde bl.a. att tillståndet ska vara knutet till viss plats och inte till person. Ombudet ansåg att omfattningen av tillståndet inte överensstämde med lagens krav på precision av den plats som ska övervakas. Åklagaren bestred ändring och anförde följande.

> Begreppet plats är inte närmare avgränsat i lagtexten eller i förarbetena. Det har inte närmare angetts hur stor eller liten platsen ska vara. I förarbetena har kopplingen till den misstänkte betonats. Genom polisens spaning i det aktuella ärendet har man kunnat se att den misstänkte har rört sig på flera platser i … . Det har även iakttagits att den misstänkte är försiktig i sin kommunikation och andra tvångsmedel som använts har varit resultatlösa. Den rörliga övervakningen verkställs genom att en pilot, som är en fysisk person, fjärrstyr en drönare med monterad kamera först när polisen, genom fysisk spaning eller på annat sätt, identifierat att misstänkt finns i visst område. Platsen är därigenom tillräckligt avgränsad eftersom den är kopplad till just det ställe där den misstänkte befinner sig inom dessa tre angivna kommuner. Övervakning sker alltså inte generellt överallt i tre kommuner samtidigt. Integritetsintrånget är mindre vid denna typ av övervakning än vid hemlig kameraövervakning med en fastsatt kamera där övervakning sker över tid. Övervakningen med drönaren sker på sådan höjd att det är svårt att identifiera allmänheten. Den misstänkte kan identifieras utifrån uppgifter som kommer från en kombination av den fysiska spaningen och den hemliga övervakningen.

Hovrätten avslog det offentliga ombudets yrkande om inhibition och fastställde tingsrättens beslut samt förenade det med följande villkor.

- Hemlig kameraövervakning får genomföras först när det genom spaning eller på annat sätt kan misstänkas att den för brottet misstänkta personen agerar i enlighet med brottsplanen inom det geografiska område som beslutet gäller.
- Kameran får endast vara aktiv när UAS (drönaren) är i luften.
- Okända personer och allmänhet som inte agerar med den misstänkta personen ska inte kunna identifieras med ansiktsbild med hjälp av drönarens kamera.

Som skäl för beslutet anförde hovrätten följande bl.a. följande i fråga om platskravet.

> Övervakning får ske på plats som den misstänkte kan antas komma att uppehålla sig. Av förarbetena framgår att tillstånd till hemlig kameraövervakning bör knytas till en viss plats. Det kan röra sig om flera olika platser och antalet platser bör kunna utvidgas genom nya beslut. Det är av avgörande betydelse att det finns en koppling till den misstänkte (Se prop. 1995/96:85 s. 30 ff.) …
>
> I det här fallet har åklagaren begärt tillstånd till hemlig kameraövervakning i tre kommuner med en kamera som sitter på en drönare. Det är ett stort upptagningsområde och det skulle inte vara ändamålsenligt eller proportionerligt att besluta om hemlig kameraövervakning över hela området. Dock har åklagaren begärt tillstånd till hemlig kamera-

övervakning förenat med villkor som innebär att kameraövervakningen enbart får ske när polisen genom fysisk spaning eller på annat sätt kopplat den misstänkte till en viss plats inom angivna kommunerna. Det är enbart då åklagaren har begärt att kameraövervakning får ske.

Med anledning av de villkor som åklagaren uppställt för den hemliga kameraövervakningen bedömer hovrätten att platsen är tillräckligt avgränsad och åtgärden därmed är proportionerlig. Hovrätten fastställer därför tingsrättens beslut och förtydligar de av åklagaren angivna villkoren för kameraövervakningen.

Ärendet illustrerar såväl svårigheterna att i tillståndet ange en precis plats när den misstänkte är riskmedveten som vikten av begränsande villkor när platsen inte kan anges med precision. I detta ärende har domstolen förhållit sig till problematiken genom att godta en bred platsangivelse och fokusera på specifika villkor för verkställigheten.

Från åklagare har vi även fått flera andra exempel på att domstolar lämnat tillstånd till hemlig kameraövervakning, ofta med drönare, omfattande ett stort område. Det har förekommit att ett sådant beslut kombineras med ett beslut om hemlig rumsavlyssning och att kameraövervakningen används för att fastställa när den misstänkte är på den plats som ska avlyssnas.

– I ett ärende beviljades hemlig kameraövervakning med drönare i en utredning angående grovt narkotikabrott. Platsen var i beslutet markerad på en satellitbild över en svensk stad med tre större områden markerade som vart och ett innehåller en eller flera stadsdelar. Beslutet gällde de markerade områdena och var förenat med följande villkor. ”Övervakning får endast ske när det kan konstateras att misstänkt befinner sig inom respektive område och ska då vara riktat endast mot honom”.

– I ett ärende lämnades tillstånd till hemlig kameraövervakning avseende en hel kilometerlång gata. Tvångsmedlet syftade till övervakning av ett fordon som användes som narkotikagömma och som med jämna mellanrum flyttades längs med gatan i syfte att undgå parkeringsböter.

– I ett ärende tilläts hemlig kameraövervakning avseende ett helt bostadsområde, verkställd med drönare, med villkor att misstänkt kommer till bostadsområdet och bildupptagningen avser den misstänkte.

- Ett beslut om hemlig kameraövervakning gällande grovt narkotikabrott avseende platsen ”utomhus inom Stockholms län”. Beslutet var förenat med villkor att åtgärden fick påbörjas först då det kan konstateras att den misstänkte uppehåller sig på den aktuella platsen, att övervakningen kommer att genomföras med bruk av fjärrstyrd kamera på ett sådant sätt att risken för övervakning av utomstående minimeras genom att den övervakade platsen begränsas genom s.k. zoomning samt att övervakning får genomföras endast under tid då kameran manövreras av polisen eller bildupptagningen kontinuerligt övervakas av polisman.
- I ett ärende angående grovt narkotikabrott beviljade tingsrätten hemlig kameraövervakning med hjälp av drönare avseende en hel stadsdel. Följande villkor beskrevs i polisens PM men skrevs inte in som villkor i tingsrättens beslut. ”Beslutet omfattar hemlig kameraövervakning i hela området och kommer att påbörjas då det genom spaning alternativt avlyssning kan konstateras att en för brottet skäligen misstänkt person uppehåller sig på platsen och agerar inom brottsplanen. Kameraövervakningen kommer att genomföras med fjärrstyrd kamera från hög höjd på sådant sätt att risken för övervakning av utomstående person minimeras. Kameran manövreras av en för ändamålet utbildad polisman och bildupptagningen följs kontinuerligt under tiden för övervakningen”.
- I ett ärende angående grovt narkotikabrott beviljade tingsrätten hemlig kameraövervakning genom drönare avseende en hel polisregion. Följande villkor beskrevs i polisens PM men skrevs inte in som villkor i tingsrättens beslut. ”Beslutet omfattar hemlig kameraövervakning i hela området mot misstänkt på tänkt brottsplats, genom en på platsen lämpligt dold kamerainstallation. Kameran manövreras av en för ändamålet utbildad polisman och bildupptagningen följs kontinuerligt under tiden för övervakningen. Kamerabevakningen sker på sådant sätt att risken för övervakning av utomstående person minimeras genom zoomning. Då övervakningen enbart sker mot misstänkt under kortare tidsperioder minimeras risken för påverkan av någon utomstående”.
- I ett ärende rörande synnerligen grovt narkotikabrott gavs tillstånd till hemlig kameraövervakning avsedd att verkställas med drönare över hela Norra Botkyrka. Beslutet villkorades med ”att polisen fått information om pågående eller förestående möte där någon av de utpekade personerna medverkar”.

De angivna exemplen visar på tendensen att domstolar i vissa fall beviljar tillstånd avseende stora områden. Det har dock även framkommit att domstolarnas praxis varierar när det gäller hur preciserat en plats måste anges för att tillstånd ska ges, och att vissa domare ställer höga krav på precisering. Som ett exempel har åklagare tagit upp en situation där domstolen beträffande drönarövervakning avseende en viss lokal i ett fall begränsat tillståndet så snävt att det inte kunde verkställas och i ett annat fall gett tillstånd utan begränsning till övervakning av samma lokal. Enligt uppgift är det, liksom i fråga om hemlig rumsavlyssning, relativt vanligt att de brottsbekämpande myndigheterna avstår från att ansöka om tillstånd eftersom en specifik plats inte kan anges.

Med hänsyn till det anförda är det enligt vår bedömning uppenbart att inte heller den gällande regleringen om hemlig kameraövervakning längre möter den brottsbekämpande verksamhetens behov.

Åklagare har redan i dag en möjlighet att fatta interimistiska beslut om hemlig kameraövervakning. Vi föreslår i kapitel 12 att det ska bli möjligt att besluta om tillträdestillstånd för installation av kamerautrustning även utan samband med hemlig rumsavlyssning, och att sådana beslut ska kunna fattas interimistiskt. En sådan möjlighet kan, om den införs, förväntas förbättra förutsättningarna för hemlig kameraövervakning på platser som är skyddade mot intrång, i de fall det finns tid och möjlighet att installera en kamera i rätt tid.[2] Förslaget medför dock ingen förbättring när det gäller möjligheterna till kameraövervakning på allmänna platser. Som vi utvecklat närmare i övervägandena om hemlig rumsavlyssning löser möjligheten till interimistiska åklagarbeslut om hemlig kameraövervakning inte heller de problem som beskrivits i detta avsnitt. Som anförts i fråga om hemlig rumsavlyssning anser vi att det inte är en lämplig väg att i lagtext vidga platsbegreppet. Med hänsyn till det anförda bedömer vi att det finns ett påtagligt behov av en möjlighet att knyta ett beslut om hemlig kameraövervakning till den skäligen misstänkte.

[2] Tillträdestillstånd för hemlig kameraövervakning får inte avse någons stadigvarande bostad (27 kap. 25 a § andra stycket). Däremot finns det som tidigare sagts inget som hindrar att man filmar in i någons bostad från en kamera placerad på annan plats.

Hemlig dataavläsning

Sådana uppgifter som man kan få fram genom en hemlig kameraövervakning eller en hemlig rumsavlyssning kan man även få tillgång till med hjälp av hemlig dataavläsning (1 och 2 §§ lagen om hemlig dataavläsning). Skillnaden är att man vid hemlig dataavläsning inte monterar en avlyssnings- eller kamerautrustning, utan i stället utnyttjar ett informationssystem som har en viss koppling till den skäligen misstänkte (4 § samma lag). Ett sådant informationssystem kan t.ex. vara en dator, mobiltelefon eller läsplatta. Konkret kan det t.ex. handla om att man aktiverar den misstänktes webbkamera eller mikrofonen på den misstänktes mobiltelefon.

Eftersom bestämmelserna om hemlig dataavläsning har utformats med rättegångsbalkens regler som förebild och då det är fråga om en metod att få tillgång till samma slags uppgifter, gäller den problem- och behovsbeskrivning vi i föregående avsnitt gett även i fråga om hemlig dataavläsning. Vi gör alltså bedömningen att det även föreligger ett påtagligt behov av en möjlighet knyta hemlig dataavläsning avseende rumsavlyssnings- och kameraövervakningsuppgifter till den skäligen misstänkte.

10.5 Det införs en möjlighet att knyta tillståndet till den skäligen misstänkte

Förslag: Det införs en möjlighet knyta ett tillstånd till hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssnings- och kameraövervakningsuppgifter till den skäligen misstänkte i stället för till en viss plats.

Skälen för förslagen

Vi har i avsnitt 10.4 gjort bedömningen att det finns ett påtagligt behov av en möjlighet att i vissa fall knyta ett tillstånd till hemlig rumsavlyssning, hemlig kameraövervakning och hemlig dataavläsning avseende rumsavlyssnings- och kameraövervakningsuppgifter till den person som ska avlyssnas. Det rör sig om fall där det inte finns någon annan möjlighet att skaffa motsvarande information,

eller där det inte är möjligt utan att beslutet avfattas på ett sådant sätt att platsen anges mycket brett. I det följande redovisas våra övriga bedömningar och avvägningar.

Förhållandena har ändrats

Vid bedömningen av om det finns förutsättningar för att i vissa fall släppa kravet på att tillståndet ska avse en viss plats har bl.a. den tekniska utvecklingen betydelse.

När det gäller hemlig rumsavlyssning har utvecklingen inneburit att utrustningen för att avlyssna brottsmisstänkta personer kan anpassas snabbare än tidigare och kan riktas så att man kan avlyssna misstänkta som förflyttar sig utan att det innebär stora risker för att samtal mellan andra personer fångas upp. Spanare kan utan särskilt mycket planering placera ut avlyssningsutrustning i offentliga miljöer där de misstänkta förväntas komma att röra sig och tala med varandra. Spanarna följer efter dem som avlyssnas, just eftersom det är okänt i förväg hur dessa kommer att förflytta sig. Räckvidden för att fånga upp ljud är relativt begränsad, även om det varierar beroende på övriga ljud i omgivningen. Spanarna kan efter avlyssningen snabbt och enkelt ta bort avlyssningsutrustningen. Risken för att tredje man drabbas av avlyssningen kan därmed minimeras. Under senare tid har det också kommit utrustning som ger möjlighet att på visst avstånd avlyssna kommunikation utan föregående teknisk installation. Av det sagda framgår att avlyssning på allmänna platser numera i vissa fall kan genomföras på ett sätt som innebär lägre risker för intrång i utomståendes personliga integritet än vad som tidigare varit möjligt. En sådan möjlighet kan finnas även i vissa fall när den misstänkte befinner sig på en intrångsskyddad plats, såsom en inhägnad tomt. Beroende på omständigheterna och den teknik som används kan det även i vissa fall vara möjligt att rikta in avlyssningen mot en viss person när det gäller på förhand monterad utrustning i exempelvis en bostad. Detta kan vara möjligt om det genom spaning eller på annat sätt finns uppgift om var i bostaden personen befinner sig och man använder avlyssningsutrustning som kan aktiveras och avaktiveras på distans. I praktiken används dock inte denna möjlighet i dagsläget.

När det gäller hemlig kameraövervakning har den nya drönartekniken inneburit att det är möjligt att från luften kameraövervaka brottsmisstänkta som är i rörelse eller som befinner sig på avsides platser eller utomhus på privata fastigheter. Drönarna kan flygas på sådant avstånd att risken för att de övervakade personerna upptäcker dem är mycket liten. Kamerorna kan riktas och zoomas in mot de övervakade personerna, varför risken för integritetsintrång förutomstående är begränsat. I den mån utomstående fångas upp på bild, t.ex. när den misstänkte rör sig i stadsmiljö, torde det ofta handla om att någon kortvarigt syns på bild. Med dagens teknik är det normalt inte möjligt att på filmer och bilder som tagits med drönarkamera urskilja ansikten eller registreringsnummer på fordon. Vid behov kan bildmaterialet i efterhand bearbetas på ett sådant sätt utomstående personer inte kan identifieras. Övervakning med drönare sker utan föregående installation och utan att någon utrustning behöver tas bort i efterhand. Övervakningen kan alltså begränsas i tid, vilket även det innebär minskad risk för integritetsintrång för utomstående. Möjligheten att snabbt anbringa och zooma in kameran på de personer som är intressanta i utredningen är inte begränsad till drönarkameror. Det kan alltså finnas möjlighet att använda andra kameror än sådana som är monterade på drönare och att rikta in dessa på ett sådant sätt att man minskar risken för integritetsintrång för utomstående.

De brottsbekämpande myndigheterna har framhållit att man vid verkställigheten av en hemlig kameraövervakning eller hemlig rumsavlyssning alltid strävar efter att undvika att fånga upp sådant som saknar intresse för utredningen, såsom samtal mellan utomstående personer. Det finns inget intresse av att dokumentera sådan information som närmast kan betraktas som en störning i förhållande till tvångsmedlet.

De uttalanden som gjorts i tidigare lagstiftningsärenden om vikten av att beslutsfattaren kan pröva den konkreta åtgärd som planeras har fortfarande giltighet. Emellertid anser vi att den tekniska utvecklingen har förändrat spelplanen, särskilt när det gäller rumsavlyssning och kameraövervakning på allmänna platser och andra platser utomhus. Förutsättningarna för bedömningen har alltså förändrats.

Det är också tydligt att behovet av en möjlighet att i vissa fall knyta tillståndet till en person har ökat i takt med de kriminellas riskmedvetenhet. Enligt vår bedömning befinner vi oss nu i ett läge där möjligheterna till beslut om hemlig rumsavlyssning och hemlig kameraövervakning, särskilt på allmänna platser, måste förbättras och förtydligas om de brottsbekämpande myndigheterna ska ha rimliga möjligheter att utreda allvarlig brottslighet. Det är inte acceptabelt att regleringen möjliggör mycket olika bedömningar, och ytterst en icke förutsebar rättstillämpning. Det finns alltså mycket starka skäl för en möjlighet att knyta ett tillstånd till de nu aktuella hemliga tvångsmedlen till den skäligen misstänkte och inte enbart till en viss plats.

Hemlig dataavläsning är ett nytt tvångsmedel och den tekniska utvecklingen sedan införandet kan därför inte på samma sätt anföras som ett skäl för förändringar. Det som sagts i förra stycket om de kriminellas anpassning till risken för att utsättas för hemliga tvångsmedel och konsekvenserna av platskravet har dock samma relevans.

Effektivitet

Hemlig rumsavlyssning, hemlig kameraövervakning och hemlig dataavläsning är effektiva åtgärder för att utreda de allvarliga brott som kan föranleda respektive tvångsmedel. I vissa fall är det den enda möjligheten för de brottsbekämpande myndigheterna att få tillgång till den information de behöver för att kunna utreda brottet eller brottsligheten. Vi bedömer att en möjlighet att, när det är av synnerlig vikt för utredningen och på de premisser som utvecklas i avsnitt 10.6–10.8, kunna besluta om hemlig rumsavlyssning, hemlig kameraövervakning eller hemlig dataavläsning som gäller rumsavlyssnings- eller kameraövervakningsuppgifter avseende en viss person kan förväntas minska de påtagliga olägenheter som finns till följd av den nuvarande regleringen sammantagen med de kriminellas beteende. En sådan möjlighet kan därigenom förväntas vara tillräckligt effektiv för att det ska vara motiverat att införa den.

Proportionalitet och förenlighet med regler till skydd för den personliga integriteten

Hemlig rumsavlyssning, hemlig kameraövervakning och hemlig dataavläsning innebär en inskränkning av de rättigheter och det skydd som tillkommer enskilda enligt regeringsformen och Europakonventionen. Som vi utvecklat i kapitel 3 är det tillåtet att under vissa förutsättningar begränsa dessa rättigheter. Regler om hemliga tvångsmedel är hänförliga till intresset att bekämpa allvarlig brottslighet. Det är ett av de intressen som får ligga till grund för begränsningar av rättigheterna, se 2 kap. 21 § regeringsformen och artikel 8.2 Europakonventionen. Begränsningarna måste vidare ha ett tillräckligt tydligt lagstöd och vara proportionerliga i förhållande till ändamålet (se kapitel 3 för en närmare utveckling av innebörden av dessa krav).

En första fråga är om en reglering som inte ställer krav på angivande av en viss plats blir tillräckligt tydlig och förutsebar för att leva upp till de krav på lagstöd som följer av regeringsformen och artikel 8 i Europakonventionen. Bestämmelser om hemliga tvångsmedel innebär en allvarlig inskränkning av enskildas rätt till skydd för den personliga integriteten och kräver därför stöd i lag av särskilt tydlig karaktär. Bedömningen beror på regleringens konkreta utformning. Vi föreslår i avsnitt 10.6 ett antal begränsningar i fråga om den plats som åtgärden får verkställas på eller riktas mot. I avsnitt 10.7 föreslår vi att tillståndet alltid ska förenas med villkor som syftar till att minska risken för onödiga integritetsintrång. Det kan t.ex. handla om att tvångsmedlet endast får verkställas när spaning visar att den misstänkte är på plats, eller när den misstänkte sammanträffar med vissa andra personer. I avsnitt 10.8 föreslår vi att tillståndet får knytas till den skäligen misstänkte endast när det finns särskilda skäl för det. Sammantaget anser vi att regleringen med denna utformning blir tillräckligt tydlig och förutsebar för att leva upp till de krav som följer av regeringsformen och Europakonventionen (jfr Roman Zacharov mot Ryssland, punkt 264 med där hänvisad rättspraxis). Vi bedömer att regleringen med den utformning vi föreslår bättre svarar mot hur domstolarnas beslut i vissa fall utformas (se exemplen på beslut i avsnitt 10.4). Det innebär en förbättrad förutsebarhet för enskilda.

Nästa fråga är om regleringen är proportionerlig. En utgångspunkt är då att hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter kan medföra särskilt allvarliga in-

trång i den personliga integriteten. Tillämpningsområdet är dock begränsat, eftersom dessa tvångsmedel får användas endast vid mycket allvarlig brottslighet. Detta gäller även om man genomför våra förslag i kapitel 6 om en straffvärdeventil för viss flerfaldig brottslighet som utövats organiserat eller systematiskt. Vidare varierar graden av integritetsintrång av en rumsavlyssning eller dataavläsning avseende rumsavlyssningsuppgifter från fall till fall. Till detta kommer de nyss nämnda begränsningarna som vi föreslår i avsnitt 10.6–10.8. Vi anser att dessa begränsningar – och allra främst kravet på villkor – sedda tillsammans med att tvångsmedlet endast kan användas vid mycket allvarlig brottslighet, med de principer som styr all användning av hemliga tvångsmedel och de övriga rättssäkerhetsgarantier som gäller för hemlig rumsavlyssning och hemlig dataavläsning innebär en tillräcklig garanti för att man inte använder tvångsmedlet på ett sätt som medför oacceptabla integritetsintrång i de nu aktuella fallen. Det saknas enligt vår bedömning lämpligare eller mindre ingripande alternativ för att få del av de uppgifter som det finns behov av i dessa utredningar.

Tillämpningsområdet för hemlig kameraövervakning och hemlig dataavläsning avseende kameraövervakningsuppgifter är något större, eftersom kraven i fråga om brottets allvar är lägre ställda. Orsaken är att tvångsmedlen typiskt sett har ansetts innebära ett mindre allvarligt intrång i den personliga integriteten än hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter. Tvångsmedlen är dock begränsade till brottslighet av allvarligt slag. Det som i övrigt sagts i fråga om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter gäller även i fråga om hemlig kameraövervakning och hemlig dataavläsning avseende kameraövervakningsuppgifter.

Med hänsyn till det anförda bedömer vi att det är proportionerligt och förenligt med Sveriges åtaganden enligt Europakonventionen att införa en möjlighet att knyta ett tillstånd till hemlig rumsavlyssning, hemlig kameraövervakning och hemlig dataavläsning avseende rumsavlyssnings- och kameraövervakningsuppgifter till den skäligen misstänkte.

Det anförda innebär att vi gör en annan bedömning än den som regeringen gjorde i samband med införandet av hemlig dataavläsning (jfr prop. 2019/20:64 s. 86). Regeringen ansåg den gången att ett platskrav var en förutsättning för att hemlig dataavläsning skulle kunna införas. Regeringens ställningstagande bör ses i ljuset av att det för

de bakomliggande tvångsmedlen hemlig rumsavlyssning och hemlig kameraövervakning inte den gången fanns något alternativ till att knyta tillståndet till en viss plats. I propositionen fördes det inte några resonemang om alternativa möjligheter än platsangivelse för att begränsa integritetsintrånget och reglerna utformades med de bakomliggande hemliga tvångsmedlen som förebild. Visserligen gjordes det obligatoriskt att förena tillståndet till hemlig dataavläsning med villkor, men uttalandena om villkorskravet är relativt knapphändiga och några överväganden om att noggrant utformade villkor skulle kunna ersätta ett krav på platsangivelse fördes av naturliga skäl inte. Som kommer att utvecklas närmare i avsnitt 10.7 föreslår vi inte bara att villkor ska vara obligatoriska för samtliga de nu aktuella hemliga tvångsmedlen utan även att åklagaren i samband med ansökan ska vara skyldig att föreslå vilka villkor som ska gälla för tillståndet. Avsikten är att villkorskravet ska få en betydligt större betydelse än i dag, även när det gäller hemlig dataavläsning.

Sammanfattande bedömning

Resonemangen i det föregående utmynnar i bedömningen att skälen för att skapa en möjlighet att knyta ett tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning till den skäligen misstänkte överväger. Vi föreslår därför att det införs en möjlighet att, som ett komplement till möjligheten att fatta beslut om tvångsmedlet avseende en viss plats, besluta om tvångsmedlet avseende en skäligen misstänkt. Bedömningen och förslaget förutsätter att möjligheten begränsas på det sätt som föreslås i avsnitt 10.6–10.8.

När det gäller hemlig dataavläsning måste man beakta att det är fråga om en tidsbegränsad försökslagstiftning. Detta manar till viss försiktighet. Samtidigt bedömer vi, som framkommit ovan, att behovet av ett alternativ till platskravet är påtagligt även när det gäller hemlig dataavläsning och att en sådan reglering skulle vara effektiv och proportionerlig. Med hänsyn till detta och till att bestämmelserna är avsedda att spegla bestämmelserna om de bakomliggande hemliga tvångsmedlen anser vi, trots att lagen är tidsbegränsad, att skälen för en möjlighet att knyta tvångsmedlet till den misstänkte överväger. Våra förslag i denna del omfattar därför även hemlig dataavläsning avseende kameraövervaknings- och rumsavlyssningsuppgifter.

10.6 Begränsningar i fråga om platsen

Förslag: Ett beslut om hemlig rumsavlyssning som avser den skäligen misstänkte ska få verkställas endast på så sätt att avlyssningen riktas mot en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Avlyssningen får vid verkställighet riktas mot någon annan stadigvarande bostad än den misstänktes endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. De tekniska hjälpmedel som används ska inte få placeras på en plats som skyddas mot intrång eller på sådana platser som avses i 27 kap. 20 e § tredje stycket RB. Åtgärden ska inte heller få riktas mot sådana platser som avses i 20 e § tredje stycket.

Ett beslut om hemlig kameraövervakning som avser den skäligen misstänkte ska få verkställas endast på så sätt att övervakningen riktas mot en plats där det kan antas att den misstänkte kommer att uppehålla sig. De tekniska hjälpmedel som används ska inte få placeras på en plats som skyddas mot intrång.

Ett beslut om hemlig dataavläsning som knyts till den skäligen misstänkte och som gäller rumsavlyssningsuppgifter ska endast få verkställas där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Om platsen är någon annan stadigvarande bostad än den misstänktes, ska hemlig dataavläsning få användas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. Förbudet mot hemlig dataavläsning som gäller rumsavlyssningsuppgifter på platser dit tillträdestillstånd inte får beviljas ska gälla även i de nu aktuella fallen.

Ett beslut om hemlig dataavläsning som knyts till den skäligen misstänkte och som gäller kameraövervakningsuppgifter ska få användas endast på en plats där den misstänkte kan antas komma att uppehålla sig. En sådan plats ska dock inte få vara någons stadigvarande bostad.

Skälen för förslagen

Hemlig rumsavlyssning

För att en hemlig rumsavlyssning ska kunna äga rum i ett utrymme som inte är tillgängligt för allmänheten, såsom en bostad eller ett fordon, krävs i allmänhet relativt omfattande förberedelser. Den brottsbekämpande myndigheten behöver normalt få tillåtelse av någon som disponerar platsen eller tillstånd av rätten att bereda sig tillträde till platsen för installation av avlyssningsutrustning. Därefter behöver utbildad personal installera utrustningen. Det är naturligtvis inte möjligt att få tillstånd till tillträde avseende en okänd plats, eller att vidta en fysisk installation på en plats som man inte känner till.[3] I praktiken är det därför sällan som en möjlighet att koppla ett tillstånd till avlyssning till den skäligen misstänkte i stället för en plats skulle ha någon praktisk användning när den misstänkte befinner sig på intrångsskyddade platser. Detta talar för att möjligheten att knyta tillståndet till den skäligen misstänkte begränsas till situationer då denne befinner sig på platser som inte är skyddade mot intrång.

Vidare framstår integritetsintrånget typiskt sett som större när avlyssningen sker på en skyddad plats. Den som befinner sig i en bostad eller ett privat fordon har en befogad förväntan om att utomstående inte kan ta del av de samtal som förs. Det är visserligen tekniskt möjligt att under vissa förutsättningar begränsa avlyssningen i en bostad eller annan skyddad plats till ett visst utrymme, t.ex. det rum där spaning visar att den misstänkte befinner sig, vilket begränsar integritetsintrånget för andra personer (se avsnitt 10.5). På grund av den stora personalinsats som krävs används möjligheten dock för närvarande inte i praktiken. I andra fall är det över huvud taget inte möjligt med en sådan begränsning. Hemlig rumsavlyssning i exempelvis en bostad innebär alltså att alla som befinner sig på platsen kan komma att avlyssnas. Integritetsriskerna bedöms mot denna bakgrund i allmänhet vara högre vid avlyssning på platser dit allmänheten inte har tillträde. Det anförda talar för att möjligheten att knyta tillståndet till hemlig rumsavlyssning till den skäligen misstänkte bör avse situationer där den misstänkte befinner sig på allmän plats.

[3] I undantagsfall är det möjligt med en snabb installation. Ett exempel är när Tullverkets personal har möjlighet att i samband med uttagande av ett fordon för tullkontroll anbringa avlyssningsutrustning. Sådana fall tas i kapitel 11 upp som ett exempel på när det kan finnas behov av en möjlighet för åklagare att fatta ett interimistiskt beslut om hemlig rumsavlyssning och tillträdestillstånd.

För detta talar även i viss mån myndigheternas behovsbeskrivning. Det behov som framkommit av en möjlighet att knyta ett tillstånd till den skäligen misstänkte avser nämligen främst situationer där den misstänkte kan förväntas föra samtal på platser som inte är skyddade mot intrång, och att det på förhand är okänt var eller att samtalet sker under det att de samtalande förflyttar sig. Med uttrycket att platsen är skyddad mot intrång avser vi detsamma som i bestämmelserna om tillträdestillstånd i 27 kap. 25 a § RB. Som exempel kan nämnas bostäder, trädgårdar som hör till bostäder, arbetsplatser, föreningslokaler och trappuppgångar. Även offentliga lokaler som på vissa tider står öppna för allmänheten anses omfattas på de tider då lokalen är stängd. (Prop. 2005/06:178 s. 104.)

Hänsynen till enskildas personliga integritet pekar i samma riktning. Den möjlighet som numera kan finnas att utan föregående installation, eller genom en mycket snabb installation, utföra en hemlig rumsavlyssning på en plats som inte är skyddad mot intrång innebär inte bara att sådan avlyssning numera i betydligt fler fall kan utföras med mycket kort varsel utan även att man kan minska integritetsintrånget för utomstående. Avlyssningsutrustningen kan anbringas kort före avlyssningen och avlägsnas när den avslutats och så snart man avlyssnat samtalet och avlägsnande kan ske utan risk för upptäckt. Vidare är det, som tidigare sagts, numera möjligt att rikta in avlyssningen så att risken för att utomstående avlyssnas minimeras. Sådana möjligheter finns i praktiken inte vid avlyssning på intrångsskyddade platser. Vidare har den som befinner sig på en allmän plats, exempelvis en öppen restaurang, i många fall lägre anspråk på skydd mot att utomstående hör vad som sägs under samtal än den som befinner sig i exempelvis en bostad. Enligt uttalanden i förarbetena kan det rentav förhålla sig så att integritetsintrånget vid en rumsavlyssning som avser ett möte på en restaurang är en avsevärt lindrigare åtgärd från integritetssynpunkt än en hemlig avlyssning av en telefon som pågår under flera månader (jfr prop. 2005/06:178 s. 44). Integritetsintrånget kan alltså i allmänhet anses vara lägre på allmänna platser än på platser dit allmänheten inte har tillträde. Samtidigt bör det sägas att det givetvis finns allmänna platser, såsom allmänna toaletter, där det kan upplevas som mycket integritetskränkande att bli avlyssnad.

I vissa fall kan det dock vara tekniskt möjligt att rikta en hemlig rumsavlyssning mot en plats som inte är tillgänglig för allmänheten och utan att polisen behöver tillträde till platsen. Man kan exempel-

vis tänka sig att den skäligen misstänkte och i förekommande fall den han eller hon samtalar med beger sig in på en inhägnad tomt som allmänheten inte har tillträde till. Det kan då vara möjligt att utan risk för upptäckt snabbt placera avlyssningsutrustningen utanför det intrångsskyddade området och därigenom fånga upp det som sägs. I enstaka fall kan man tänka sig att personerna beger sig in i en bostad och att samtalet hörs ut t.ex. genom ett öppet fönster, och att avlyssning alltså kan ske utan att det behöver ske något intrång i bostaden. Situationer av det angivna slaget kan beroende på omständigheterna ge upphov till större integritetsrisker än en avlyssning av någon som befinner sig på allmän plats, bl.a. eftersom utomstående personer som kan tänkas befinna sig på platsen många gånger räknar med att kunna tala utan att andra fångar upp det som sägs. Detta talar för att avlyssning där tillståndet kopplas till den misstänkte inte bör vara tillåten i dessa fall. Mot detta talar den uppenbara risken för att kriminella personer utnyttjar den lucka som uppstår därigenom och sätter i system att samtala på olika platser dit allmänheten inte har tillträde.

Vid en avvägning där brottsbekämpningsintresset ställs mot behovet av skydd för den personliga integriteten anser vi att behovet av en möjlighet att kunna avlyssna även intrångsskyddade platser överväger. Integritetsriskerna bör i stället hanteras genom de villkor som vi i avsnitt 10.7 föreslår alltid ska läggas till ett tillstånd till hemlig kameraövervakning i de nu diskuterade fallen. Dock bör en eventuell möjlighet att knyta tillståndet till den skäligen misstänkte vara begränsad till fall då avlyssningsutrustningen placeras på en plats som inte är skyddad mot intrång. I annat fall skulle även bedömningen av om intrånget på en skyddad plats är godtagbart överlämnas till den verkställande myndigheten. Detta är inte lämpligt.

Vidare bör verkställigheten omfattas av motsvarande begränsningar som när tillståndet avser en viss plats. Det bör därför krävas att det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig på den plats där verkställighet sker. Om åtgärden riktas mot en stadigvarande bostad som inte är den skäligen misstänktes bör det krävas synnerlig anledning att anta att den misstänkte kommer att befinna sig där (jfr 27 kap. 20 e § andra stycket RB). Den tekniska utrustning som används bör aldrig få placeras på eller riktas mot sådana platser som enligt 20 e § tredje stycket RB är skyddade från hemlig rumsavlyssning.

Hemlig kameraövervakning

Även en hemlig kameraövervakning i ett utrymme som inte är tillgängligt för allmänheten kräver i allmänhet relativt omfattande förberedelser och antingen samtycke av någon som disponerar över platsen eller ett tillträdestillstånd (i dagsläget endast möjligt om man samtidigt ska utföra en hemlig rumsavlyssning). Så som vi framhållit i fråga om hemlig rumsavlyssning är det därför i praktiken sällan en möjlighet att koppla ett tillstånd till kameraövervakning mot den skäligen misstänkte i stället för en plats skulle ha någon praktisk användning när den misstänkte befinner sig på intrångsskyddade platser. Detta talar även i fråga om hemlig kameraövervakning för att möjligheten att knyta tillståndet till den skäligen misstänkte begränsas till situationer då denne befinner sig på allmän plats.

För detta talar även integritetsintrånget. Den som befinner sig på en intrångsskyddad plats räknar många gånger med att inte vara iakttagen och än mindre avbildad. Möjligheterna att begränsa övervakningen på ett sådant sätt att utomstående inte avbildas är enligt uppgift liten, även om sådana möjligheter kan finnas rent tekniskt. Det innebär att alla som befinner sig på platsen kan komma att övervakas. Integritetsriskerna bedöms därför vara högre vid kameraövervakning på platser dit allmänheten inte har tillträde.

I samma riktning talar myndigheternas behovsbeskrivning. I likhet med hemlig rumsavlyssning avser nämligen det behov som framkommit av en möjlighet att knyta ett tillstånd till den skäligen misstänkte främst situationer där den misstänkte befinner sig på allmän plats. Den möjlighet som numera kan finnas att med hjälp av drönare utföra en hemlig kameraövervakning på allmän plats innebär betydligt bättre möjligheter att utan upptäckt övervaka vissa platser där fysisk spaning är omöjlig. Som anförts i avsnitt 10.4 kan man även minska risken för integritetsintrång för utomstående. Övervakningen kan inriktas på den misstänkte och dennes förehavanden, och man kan undvika att avbilda utomstående på ett sådant sätt att de kan identifieras. Eftersom drönaren styrs manuellt på distans, kan man begränsa övervakningen så att den bara pågår precis när det är relevant. Sådana möjligheter kan även finnas när det gäller fast monterade kameror.

I första hand rör behovet alltså övervakning på allmän plats, dvs. en plats som är upplåten till eller frekventeras av allmänheten. Som nämnts ovan torde integritetsintrånget i allmänhet anses vara lägre

på allmänna platser än på platser dit allmänheten inte har tillträde, även om det finns exempel på allmänna platser, där det kan upplevas som mycket integritetskränkande att bli kameraövervakad.

I vissa fall kan det dock vara tekniskt möjligt att rikta en hemlig kameraövervakning mot en plats som inte är tillgänglig för allmänheten och utan att polisen behöver tillträde till platsen. Ett exempel som vi tagit upp även i fråga om hemlig rumsavlyssning är att den skäligen misstänkte beger sig in på en inhägnad tomt som allmänheten inte har tillträde till. I sådana fall kan det vara möjligt att övervaka platsen med hjälp av en kamera, exempelvis en kamerautrustad drönare. Det kan också hända att den misstänkte ger sig in i en byggnad och man kan kameraövervaka in genom något fönster. Även om det inte är tillåtet att installera kamerautrustning i en bostad är det enligt gällande rätt tillåtet att utföra kameraövervakning in i en bostad från någon plats utanför. Som vi konstaterat tidigare är integritetsintrånget typiskt sett större på platser som inte är tillgängliga för allmänheten och särskilt stort när övervakningen riktas mot en bostad. Detta talar emot att man tillåter kameraövervakning riktad mot sådana platser i de fall när själva tillståndet har knutits till den skäligen misstänkte och inte en plats. En sådan begränsning skulle nämligen minska risken för att kameraövervakningen verkställs på ett sätt som innebär alltför stora integritetsintrång. Samtidigt skulle det, som vi konstaterat i fråga om hemlig rumsavlyssning, innebära att man i systemet bygger in en möjlighet för kriminella att ganska enkelt undvika hemlig kameraövervakning. Något sådant skulle vara mycket olyckligt.

Vid en avvägning av brottsbekämpningsintresset mot behovet av skydd för den personliga integriteten gör vi samma bedömning som vi gjort i fråga om hemlig rumsavlyssning. Vi anser alltså att behovet av en möjlighet att kunna kameraövervaka även icke allmänna platser överväger och att integritetsriskerna bör hanteras genom de villkor som vi i avsnitt 10.7 föreslår alltid ska läggas till ett tillstånd till hemlig kameraövervakning i de nu diskuterade fallen. Vidare bör, som vi kommit fram till i fråga om hemlig rumsavlyssning, en eventuell möjlighet att knyta tillståndet till den skäligen misstänkte vara begränsad till fall då kamerautrustningen finns på en icke intrångsskyddad plats. Tillträdestillstånd för kameraövervakning kan aldrig avse stadigvarande bostäder och vi har inte i uppdrag att överväga ändringar i detta avseende.

Vidare bör verkställigheten omfattas av motsvarande begränsningar som när tillståndet avser en viss plats. Det bör därför krävas att det kan antas att den misstänkte kommer att uppehålla sig på den plats där verkställighet sker.

Hemlig dataavläsning

Hemlig dataavläsning avseende kameraövervakningsuppgifter och rumsavlyssningsuppgifter har begränsats på i huvudsak motsvarande sätt som hemlig kameraövervakning respektive hemlig rumsavlyssning. Således gäller det att ett tillstånd till hemlig dataavläsning som gäller kameraövervakningsuppgifter endast får avse en plats där den misstänkte kan antas uppehålla sig. Av integritetsskäl är det inte tillåtet att genom hemlig kameraövervakning övervaka någon som befinner sig i en stadigvarande bostad med en kamera som finns i den bostaden (se t.ex. prop. 1995/96:85 s. 30 och prop. 2013/14:237 s. 154–155). Detta följer av att ett tillträdestillstånd för installation av kameror inte kan meddelas avseende någons stadigvarande bostad (27 kap. 25 a § andra stycket RB). Däremot är det, som angetts tidigare, inte förbjudet att installera en kamera utanför en bostad och rikta den så att den genom ett fönster fångar in vad som händer i bostaden.

Vid införandet av lagen om hemlig dataavläsning ansågs det att möjligheten att få tillgång till kameraövervakningsuppgifter borde begränsas på motsvarande sätt som hemlig kameraövervakning. Eftersom hemlig dataavläsning inte sker efter installation av en kamera utan genom aktivering av en redan befintlig kamera i det informationssystem som den misstänkte använder, genomfördes begränsningen genom ett förbud mot hemlig dataavläsning som gäller kameraövervakningsuppgifter i någons stadigvarande hem (4 § fjärde stycket lagen om hemlig dataavläsning). De aktuella informationssystemen är som huvudregel rörliga och det ankommer därmed på den brottsbekämpande myndigheten som ska verkställa åtgärden att kontrollera var informationssystemet finns när åtgärden vidtas, t.ex. genom fysisk spaning (prop. 2019/20:64 s. 218).

Om tillståndet gäller rumsavlyssningsuppgifter krävs det, i likhet med vad som gäller för hemlig rumsavlyssning, att det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig på platsen. Om platsen är någon annan stadigvarande bostad än den miss-

tänktes, får tillstånd beviljas endast om det finns synnerligen anledning att anta att den misstänkte kommer att uppehålla sig där. Hemlig dataavläsning som gäller rumsavlyssningsuppgifter får aldrig beviljas på en plats dit tillträdestillstånd inte får beviljas. (6 § andra och tredje styckena lagen om hemlig dataavläsning.)

Vi har i avsnitten om hemlig rumsavlyssning och hemlig kameraövervakning kommit fram till att respektive tvångsmedel enbart ska få verkställas med hjälp av kameror respektive avlyssningsutrustning som finns på platser som inte är intrångsskyddade. De principiella ställningstaganden vi redovisar där är i allt väsentligt relevanta även när det gäller hemlig dataavläsning som avser rumsavlyssnings- och kameraövervakningsuppgifter. Emellertid verkställs hemlig dataavläsning i de nu aktuella fallen genom aktivering av kameran eller mikrofonen i ett informationssystem (exempelvis en mobiltelefon eller dator) som den misstänkte använder. Distinktionen mellan var kameran respektive inspelningsutrustningen finns och var den skäligen misstänkte befinner sig är därför i princip inte relevant när det gäller hemlig dataavläsning. I fråga om hemlig dataavläsning avseende kameraövervakningsuppgifter framgår detta genom att det är förbjudet att utföra åtgärden i någons stadigvarande bostad, fastän något sådant förbud inte finns beträffande hemlig kameraövervakning. Vid hemlig kameraövervakning gäller begränsningen avseende en stadigvarande bostad i stället möjligheten att få tillträdestillstånd för installation av en kamera, medan det är fullt tillåtet att rikta en på annan plats placerad kamera mot en bostad.

Det är inte alldeles uppenbart att förbudet mot hemlig dataavläsning avseende kameraövervakningsuppgifter i någons stadigvarande bostad helt korresponderar med reglerna om hemlig kameraövervakning. Som nyss sagts är det tillåtet att vid hemlig kameraövervakning filma in i en bostad så länge kameran finns någon annanstans. Det är alltså vid hemlig kameraövervakning intrånget i bostaden och att filmningen sker efter ett sådant intrång som är den springande punkten och inte enbart det faktum att man filmar in i bostaden (jfr prop. 2013/14:237 s. 154). Risken för att man fångar upp mycket integritetskänsliga bilder är dock större om kameran finns i bostaden än om den finns utanför och filmar in. Samma sak gäller vid hemlig dataavläsning. Förbudet mot hemlig dataavläsning i någons stadigvarande bostad bör därför gälla även när åtgärden knyts till den skäligen misstänkte i stället för till en viss plats.

Nästa fråga är om det bör gälla en begränsning till platser som inte är skyddade mot intrång. Vi har i det föregående föreslagit att tekniska hjälpmedel som används vid hemlig rumsavlyssning och hemlig kameraövervakning som knyts till den skäligen misstänkte endast får placeras på en sådan plats, men om möjligt får riktas mot en intrångsskyddad plats. Avgörande för vår bedömning har varit att verkställighet på en intrångsskyddad plats kräver ett intrång och en installation på den skyddade platsen. Vi har bedömt att beslut om sådana intrång inte bör överlämnas till den verkställande myndigheten. Man kan dock inte fullt ut jämställa ett fysiskt intrång på en intrångsskyddad plats med verkställigheten av en hemlig dataavläsning som sker genom att man aktiverar t.ex. en mobilkamera. Den hemliga dataavläsningen kan visserligen i vissa fall behöva föregås av ett intrång och en installation av någon sorts tekniskt hjälpmedel (12 § lagen om hemlig dataavläsning). Den åtgärden behöver dock inte alls avse den plats där åtgärden ska verkställas. Intrånget och installationen sker i stället på en plats där det finns särskild anledning att anta att det avläsningsbara informationssystem som ska avläsas finns tillgängligt. Om platsen är en stadigvarande bostad som används av någon annan än den misstänkte[4], får tillstånd beviljas endast om det finns synnerlig anledning att anta att informationssystemet finns där. Ett tillträdestillstånd får aldrig avse en plats som stadigvarande används eller är särskilt avsedd att användas i vissa typer av verksamheter, däribland advokatkontor och läkarmottagningar (13 § samma lag). I den mån det krävs ett intrång på en skyddad plats för att ett tekniskt hjälpmedel ska installeras kommer dessa begränsande regler alltså att gälla. Vi föreslår inte några ändringar av dessa bestämmelser.

Om man, på motsvarande sätt som i fråga om stadigvarande bostäder, inför en begränsning som går ut på att åtgärden enbart får verkställas på icke intrångsskyddade platser får den i praktiken ett snävare tillämpningsområde än vad vi föreslagit beträffande hemlig kameraövervakning och hemlig rumsavlyssning. En sådan begränsning skulle avsevärt minska värdet av en möjlighet att knyta hemlig dataavläsning till en person, eftersom det skulle innebära att man blev tvungen att avbryta avläsningen så fort den skäligen misstänkte går in på en privat tomt eller in i ett fordon, om det inte är möjligt att omedelbart få till stånd ett interimistiskt åklagarbeslut. Som vi anfört i fråga om hemlig rumsavlyssning och hemlig kameraövervak-

[4] Eller av en sådan person som anges i 7 § första stycket eller 9 § andra stycket.

ning vore det olyckligt att på detta sätt lämna en lucka som gör det möjligt för kriminella personer att undgå hemlig dataavläsning. De integritetsrisker som finns bör enligt vår mening hanteras genom de obligatoriska villkor som ska ställas för att begränsa integritetsintrånget. Vi utvecklar detta i avsnitt 10.7. Vi föreslår därför inte någon begränsning till icke intrångsskyddade platser rörande hemlig dataavläsning.

Med hänsyn till det anförda bedömer vi att det är tillräckligt att i regleringen ange att en hemlig dataavläsning avseende kameraövervakningsuppgifter enbart får användas på en plats där den misstänkte kan antas komma att uppehålla sig och aldrig i en stadigvarande bostad.

Hemlig dataavläsning avseende rumsavlyssningsuppgifter får användas endast på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig, se 6 § andra stycket lagen om hemlig dataavläsning. Någon orsak till att man i bestämmelsen har valt uttrycket ”användas på” och inte, som i 4 § fjärde stycket och bestämmelsens förebild i 27 kap. 20 e § andra stycket RB, ”avse” framgår inte av förarbetena (jfr SOU 2017:89 s. 353 och 354 och prop. 2019/20:64 s. 118–121). Någon skillnad i sak är uppenbarligen inte avsedd. För att underlätta tolkningen av bestämmelserna föreslår vi att bestämmelsen ändras så att terminologin blir enhetlig. Det bör alltså i 6 § andra stycket lagen om hemlig dataavläsning anges att hemlig dataavläsning får *avse* endast en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig.

När det gäller verkställigheten av ett beslut som avser den skäligen misstänkte i stället för en viss plats bör denna begränsas på motsvarande sätt som i övrigt gäller i fråga om plats. Verkställighet bör med andra ord få ske endast på en plats där det finns särskild anledning att anta att den misstänkte som tillståndet gäller kommer att befinna sig. Vidare bör motsvarande begränsningar gälla i fråga om någon annan stadigvarande bostad än den misstänktes.

Förbudet mot hemlig dataavläsning avseende rumsavlyssningsuppgifter på platser dit tillträdestillstånd inte får beviljas bör omfatta även de fall som avses i det nya tredje stycket. Detta bedöms, så som bestämmelsen är formulerad, gälla utan några innehållsändringar.

10.7 Tillståndet ska alltid förenas med villkor

Förslag: Ett tillstånd till hemlig rumsavlyssning eller hemlig kameraövervakning som avser en skäligen misstänkt i stället för en viss plats ska alltid förenas med villkor i syfte att minska onödiga integritetsintrång för enskilda. Åklagaren ska vara skyldig att i samband med ansökan föreslå de villkor som ska gälla. En sådan skyldighet för åklagaren ska även gälla i fråga om hemlig dataavläsning som avser en skäligen misstänkt i stället för en viss plats.

Bedömning: Det är redan nu obligatoriskt att förena ett beslut om hemlig dataavläsning med villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Detta bör gälla även vid hemlig dataavläsning som knyts till den skäligen misstänkte. Några författningsändringar är inte nödvändiga för att åstadkomma detta.

Skälen för förslagen och bedömningen

Hemlig rumsavlyssning och hemlig kameraövervakning

För att en möjlighet att knyta ett tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning till den skäligen misstanke ska vara godtagbar anser vi att kravet på angivande av en specifik plats i beslutet måste ersättas av krav på andra villkor som begränsar risken för onödiga integritetsintrång. Utan sådana villkor kan man inte skapa tillräckliga garantier för att åtgärden är proportionerlig i det konkreta fallet. Det bör därför att vara ett oeftergivligt krav att tillståndet förenas med sådana villkor.

I dagsläget finns det ingen skyldighet för åklagaren att lämna förslag på vilka villkor som kan behövas i syfte att begränsa integritetsintrånget. Detta framstår som naturligt, eftersom villkor endast ska meddelas om de behövs. I en situation där villkor inte bara är obligatoriska utan nödvändiga – vilket vi bedömer dem vara om platskravet tas bort – anser vi dock att frågan kommer i annan dager. Vi menar att ett lagstadgat krav på att åklagaren föreslår villkor kan förväntas leda till att villkoren ägnas mer uppmärksamhet och även får en högre kvalitet. Risken för att beslut meddelas utan villkor torde minska

påtagligt. Vår bedömning är därför att det i en ansökan om tillstånd som knyts till den skäligen misstänkte bör ankomma på åklagaren att i samband med sin framställan till rätten, t.ex. i den promemoria som ges in till rätten, föreslå sådana begränsande villkor som man anser lämpliga. Beroende på omständigheterna skulle sådana villkor kunna vara att tvångsåtgärden endast får verkställas när spaningsuppgifter bekräftar att den misstänkte är närvarande och agerar på ett visst sätt – t.ex. sammanträffar med vissa intressanta personer – och under vissa tider. För hemlig rumsavlyssning kan man bl.a. tänka sig som villkor att avlyssning bara får avse samtal som den misstänkte deltar i. Man kan i vissa fall tänka sig att beslutet kan avgränsas snävt, t.ex. på det sättet att man endast får avlyssna samtal mellan den skäligen misstänkte och en viss annan person under en viss angiven tidsperiod. Det kan också tänkas att vissa platser eller typer av platser uttryckligen undantas från tillståndet.

I princip bör det kunna krävas att villkoren är utformade så att åtgärden kan godtas oavsett var åtgärden – inom ramarna för tillståndet – kommer att verkställas.

Hemlig dataavläsning

Det som anförts i fråga om hemlig rumsavlyssning och hemlig kameraövervakning har motsvarande relevans i fråga om hemlig dataavläsning. Regleringen skiljer sig dock åt på det sättet att det enligt 18 § första stycket 4 lagen om hemlig dataavläsning redan är obligatoriskt att förena ett beslut om hemlig dataavläsning med villkor för användningen (se även prop. 2019/20:64 s. 93, 110 och 233 och SIN:s uttalande med beslut den 15 december 2021, dnr 92-2020). Någon lagändring är alltså inte nödvändig för att ett krav på villkor ska gälla. Emellertid får villkoren en större betydelse i de fall när kopplingen till en viss plats slopas. I princip bör det som nyss anförts kunna krävas att villkoren är utformade så att åtgärden kan godtas oavsett var avlyssningen kommer att verkställas. I sammanhanget bör det nämnas att SIN i en granskning av ärenden vid Åklagarmyndigheten där hemlig dataavläsning använts konstaterat att det i många av ärenden saknades villkor, trots att villkor alltså är obligatoriska (se det nyss nämnda beslutet).

I propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 156–157) diskuterades om det bör tas in bestämmelser om att den som ansöker om hemlig dataavläsning ska ange vilka villkor tillståndet bör förenas med för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Regeringen anförde att något sådant krav inte finns beträffande bakomliggande tvångsmedel och såg inte behov av att införa ett sådant krav avseende hemlig dataavläsning. Det ansågs tillräckligt att den som söker om tillstånd vid sammanträdet kan det motivera sin ansökan genom att på ett övergripande plan beskriva hur tvångsmedlet ska verkställas och att domstolen vid eventuella oklarheter eller behov av kompletteringar genom frågor kan skaffa sig ett tillräckligt underlag för att fatta beslut i ärendet, inklusive villkor för att skydda enskildas personliga integritet.

Som framgått tidigare anser vi att villkoren och deras utformning är av helt avgörande betydelse för att det ska vara möjligt att släppa platskravet. Av de skäl som vi tagit upp under föregående rubrik bör det därför krävas att åklagaren i samband med ansökan föreslår vilka villkor som bör gälla för tillståndet.

Beroende på omständigheterna skulle villkoren kunna vara exempelvis att hemlig dataavläsning endast får ske när det genom spaning eller på annat sätt har bekräftats att den misstänkte är på plats eller agerar på ett visst sätt, exempelvis sammanträffar med en viss annan person som är av intresse i utredningen. Det kan också tänkas att vissa platser eller typer av platser uttryckligen undantas från tillståndet.

10.8 Det ska krävas särskilda skäl

Förslag: Ett tillstånd till hemlig rumsavlyssning, hemlig kameraövervakning eller hemlig dataavläsning som gäller kameraövervaknings- eller rumsavlyssningsuppgifter ska få avse en skäligen misstänkt i stället för en viss plats endast om det finns särskilda skäl.

Skälen för förslaget

Utgångspunkten bör även i fortsättningen vara att det i beslutet ska anges en specifik plats som tvångsmedlet avser. Bestämmelserna om tillstånd som i stället knyts till den skäligen misstänkte bör därför

vara utformade som undantagsbestämmelser. Vi bedömer att en lämplig lösning är att tvångsmedlet enbart får knytas till person om det finns särskilda skäl. Med detta menar vi att möjligheten inte ska utnyttjas om det är möjligt och tillräckligt att besluta om tvångsmedlet avseende en viss utpekad plats. Däremot bör inget hindra att man beslutar om det hemliga tvångsmedlet både mot en viss plats, t.ex. den misstänktes bostad och mot den misstänkte. Det torde vara relativt vanligt att det finns ett behov av båda sortens tillstånd.

10.9 Närmare om regleringens utformning

Förslag: Bestämmelserna om hemlig rumsavlyssning som avser den skäligen misstänkte tas in i en ny 27 kap. 20 f § RB.

Bestämmelserna om hemlig kameraövervakning som avser den skäligen misstänkte tas in i ett nytt tredje stycke i 27 kap. 20 b § RB.

Bestämmelserna om hemlig dataavläsning som avser den skäligen misstänkte och som gäller kameraövervakningsuppgifter tas in i en ny 4 a § lagen om hemlig dataavläsning. Bestämmelsen om rumsavlyssningsuppgifter tas in i ett nytt tredje stycket i 6 § samma lag.

Skälen för förslagen

Den föreslagna bestämmelsen om hemlig rumsavlyssning kan lämpligen tas in i en ny paragraf som införs efter 27 kap. 20 e § RB. Den nya bestämmelsen om hemlig kameraövervakning bör tas in i ett nytt tredje stycke i 27 kap. 20 b § RB. Ändringar krävs i 21 § i fråga om vad beslutet ska innehålla och kravet på villkor (jfr avsnitt 10.7).

I lagen om hemlig dataavläsning bör bestämmelserna tas in i en ny paragraf som förs in efter 4 § när det gäller kameraövervakningsuppgifter och ett nytt tredje stycke i 6 § när det gäller rumsavlyssningsuppgifter. Som nämnts i avsnitt 10.7 krävs inte ändringar för att det ska gälla ett krav på villkor till skydd för den personliga integriteten.

Både i 27 kap. RB och i lagen om hemlig dataavläsning behöver det införas bestämmelser om det nya kravet på åklagaren att föreslå villkor.

10.10 Det bör inte krävas en särskild domstolsprövning i efterhand

Bedömning: Det bör inte införas ett krav på att beslut om hemlig rumsavlyssning, hemlig kameraövervakning eller hemlig dataavläsning som knutits till den skäligen misstänkte i efterhand prövas av domstol.

Skälen för bedömningen

Även med de begränsningar som vi tagit upp i det föregående skulle det kunna hävdas att en möjlighet till hemlig rumsavlyssning, hemlig kameraövervakning eller hemlig dataavläsning där beslutet inte är knutet till en bestämd plats innebära något försämrade möjligheter för rätten eller, vid interimistiska beslut, åklagaren att göra en prövning av risken för integritetsintrång för tredje man. Vi har övervägt om det finns något behov av ytterligare rättssäkerhetsgarantier för att kompensera för detta. En möjlighet skulle då kunna vara en obligatorisk domstolsprövning i efterhand, dvs. efter det att övervakningen, avlyssningen eller avläsningen har verkställts. Detta skulle kunna gå till på det sättet att åklagaren åläggs att anmäla till rätten hur verkställighet har skett och att rätten då skyndsamt ska pröva ärendet. Rätten skulle då kunna ta ställning till den konkreta åtgärden så som den kommit att verkställas. Annorlunda uttryckt skulle rätten pröva åtgärden på samma sätt som den hade gjort om rätten vid det ursprungliga beslutet hade haft tillgång även till uppgift om platsen eller platserna för tvångsmedlet. Om det vid domstolsprövningen visar sig att åtgärden inte borde ha företagits – dvs. inte skulle ha tillåtits om platsen för den varit känd – skulle det kunna föreskrivas de inhämtade uppgifterna inte får användas till nackdel för någon. Detta motsvarar till stor del regleringen när åklagare har fattat ett interimistiskt beslut. Skillnaden här är att rätten i efterhand kan komma att pröva en åtgärd som den redan prövat, men på ett mer fullständigt underlag.

Det är i och för sig inte främmande i rättegångsbalken att en domstol prövar en fråga flera gånger allt eftersom det tillkommer nytt underlag. Ett exempel på det är häktning, som rätten löpande ska pröva (24 kap. 18 § RB). Lösningen är därför inte utesluten av systematiska skäl. Däremot menar vi att det inte föreligger något på-

tagligt behov av den med den utformning av regleringen som vi föreslår, dvs. med krav på villkor till skydd för enskildas integritet och andra begränsningar. Vidare har det stor betydelse att ett offentligt ombud alltid finns med när rätten håller sammanträde om hemlig kameraövervakning respektive hemlig rumsavlyssning (27 kap. 26 och 28 §§ RB). Offentliga ombud ska bevaka enskildas integritetsintressen i ärenden hos domstol om bl.a. hemlig kameraövervakning och hemlig rumsavlyssning och har rätt att ta del av det som förekommer i ärendet, yttra sig i ärendet och överklaga rättens beslut. Vi bedömer att den domstolsprövning som ska ske enligt nuvarande regler är tillräcklig och att det alltså inte behövs ytterligare en prövning när verkställighet har skett.

Våra förslag i kapitel 11 om en möjlighet för åklagare att fatta interimistiskt beslut om hemlig rumsavlyssning innebär att beslutet, i likhet med vad som gäller vid andra interimistiska åklagarbeslut om hemliga tvångsmedel, skyndsamt ska prövas av en domstol. På de ovan anförda skälen anser vi det inte nödvändigt att införa krav på någon ytterligare domstolsprövning.

10.11 Problemet med gods som överlämnas

Ett problem som har kommit fram under vårt arbete rör situationer där misstänkta levererar något till andra personer och där det hade varit värdefullt att kunna följa leveransen efter överlämnandet. Ett typexempel kan vara att man bedriver hemlig kameraövervakning med drönare av ett fordon som är lastat med narkotika, vapen eller sprängämnen. Det kan vara känt i förväg att ett överlämnande ska ske, men det kan också förekomma att ett överlämnande sker utan att de brottsbekämpande myndigheterna på förhand har haft information om det. I båda fallen är det vanligt att man inte på förhand vet vem som ska ta emot leveransen och inte heller vilken väg mottagaren kommer att färdas. En annan liknande situation är att man övervakar en misstänkt som färdas till fots och bär med sig en väska med misstänkt innehåll som utan förvarning lämnas över till någon icke identifierad person.

I fall av det angivna slaget hade det varit av stort värde för utredningen att kunna följa leveransen vidare genom hemlig kameraövervakning med drönare. En sådan möjlighet skulle innebära ökade

möjligheter att utreda brottet och därigenom även att ingripa innan narkotikan har kommit ut på marknaden eller vapen eller sprängämnen har kunnat användas i våldsdåd. Vi bedömer det därför som synnerligen angeläget att en sådan möjlighet finns. Dagens regelverk hindrar dock detta redan genom kravet på att en plats för övervakningen måste anges.

Det kan finnas situationer där det är känt vem som ska ta emot narkotikan och att den personen är skäligen misstänkt för exempelvis förberedelse till grovt narkotikabrott. I ett sådant fall torde det vara möjligt att med stöd av den nya bestämmelse som vi föreslår i detta kapitel i förväg fatta ett beslut om hemlig kameraövervakning avseende mottagaren. Om ett beslut inte har fattats i förväg och mottagaren är identifierad torde det också vara tillåtet för åklagaren att fatta ett interimistiskt beslut i samband med leveransen, eftersom mottagaren senast då lär bli skäligen misstänkt.

En annan fråga är vad som gäller om mottagaren i motsvarande situation inte är identifierad. Man kan på goda grunder hävda att den icke identifierade person som ses ta emot leveransen är skäligen misstänkt för exempelvis grovt narkotikabrott. Vad innebär det då att identiteten inte är fastställd? JO uttalade i JO 2006/07 s. 30 att det för ett beslut om hemlig avlyssning av elektronisk kommunikation inte alltid behöver vara nödvändigt att känna till den misstänktes namn. Enligt JO bör det kunna vara tillräckligt att de uppgifter som finns om personen är ”i så hög grad särskiljande att förväxlingsrisk i praktiken saknas”. Enligt Lindberg kan motsvarande skäl om krav på identifiering anföras i fråga om hemlig rumsavlyssning, eftersom det krävs ett visst samband mellan den misstänkte och den plats som ska avlyssnas (Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas, 4 uppl., s. 782). Lindberg menar vidare att hemlig kameraövervakning som riktas mot någon som är skäligen misstänkt på motsvarande sätt förutsätter att personen är identifierad. I de fall som vi nu diskuterar kan de brottsbekämpande myndigheterna ha mottagaren av leveransen under i princip konstant övervakning under färd. Det innebär att det inte föreligger någon risk för att personen förväxlas med någon annan. Vår bedömning är därför att det bör vara tillåtet för åklagaren att fatta ett interimistiskt beslut om hemlig kameraövervakning avseende den icke namngivne mottagaren av leveransen, förutsatt att denne i beslutet identifieras på något annat sätt som innebär att förväxlingsrisk saknas. Beslutet skulle då

kunna villkoras snävt, t.ex. genom att övervakning bara får ske så länge som personen ses hantera den mottagna leveransen.

Av det anförda framgår att vårt förslag om en möjlighet att knyta ett beslut om hemlig kameraövervakning till den skäligen misstänkte innebär en rättslig möjlighet att fortsätta kameraövervakningen efter att leveransen lämnats över. I praktiken kan det dock i vissa fall förväntas vara omöjligt att få till stånd ett interimistiskt beslut med tillräcklig skyndsamhet. Om ett överlämnande av godset sker oväntat, lär det nämligen sällan finnas tid för drönarpiloten att ta kontakt med åklagare, föredra ärendet och få till stånd ett beslut innan mottagaren har försvunnit från platsen. Detta är otillfredsställande. Vi har övervägt om frågan kan lösas inom detta uppdrag men kommit fram till att de olika alternativa lösningar som kan tänkas – t.ex. en möjlighet att rikta en övervakning mot ett föremål eller en plats där ett brott kan förväntas ske eller pågår – aktualiserar svåra frågor som inte ryms inom uppdraget och som vi inte heller har möjlighet att ta hand om utan att redovisningen försenas avsevärt.

11 Interimistiska beslut om hemlig rumsavlyssning

11.1 Uppdraget

Åklagare får fatta interimistiska beslut om hemlig rumsavlyssning endast om landet är i krig eller om liknande extraordinära omständigheter råder (2 och 28 §§ lagen [1988:97] om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.). Frågan om att låta åklagare fatta interimistiska beslut om hemlig rumsavlyssning även i fredstid har tidigare varit föremål för regeringens överväganden i propositionen Hemliga tvångsmedel mot allvarliga brott (prop. 2013/14:237). Regeringen gjorde då bedömningen att någon sådan möjlighet inte skulle införas med hänsyn till att hemlig rumsavlyssning typiskt sett är det tvångsmedel som leder till det största intrånget i enskildas personliga integritet varför särskild försiktighet ansågs påkallad (s. 142).

Åklagare har möjlighet att under förundersökning fatta interimistiska beslut om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning (27 kap. 21 a § RB och 2 kap. 5 § andra stycket lagen om en europeisk utredningsorder). En sådan möjlighet finns även när någon av dessa åtgärder ska vidtas i Sverige på begäran av en annan stat (4 kap. 25 och 27 §§ lagen om internationell rättslig hjälp i brottmål och 3 kap. 10 § lagen om en europeisk utredningsorder). Varje år redovisar regeringen användningen av hemliga tvångsmedel till riksdagen. Av det underlag som myndigheterna gett in för tvångsmedelsanvändningen under 2019 framgår det att domstol endast har upphävt en handfull interimistiska beslut (Redovisning av användningen av vissa hemliga tvångsmedel under 2019 [Ju2020/02045/Å] s. 10–11, 21, 27 och 40). Bilden var densamma föregående år. Det kan därför enligt direktiven ifrågasättas om en särskild försiktighet verkligen är

påkallad när det gäller möjligheten att fatta interimistiska beslut om hemlig rumsavlyssning. Härtill kommer enligt direktiven dels det förhållandet att kriminella byter platser för sina möten med kort varsel, vilket gör att det finns ett behov av ett snabbt beslutsfattande, dels att ny teknik gör det möjligt att verkställa hemlig rumsavlyssning snabbare än tidigare.

I direktiven anges vidare att det även kan finnas skäl att anta att en möjlighet till interimistiskt beslutsfattande kan leda till ökad effektivitet när det rör sig om internationellt samarbete mot gränsöverskridande brottslighet där ett snabbt beslutsfattande är viktigt.

Vi har därför i uppdrag att

- ta ställning till om åklagare bör få möjlighet att fatta interimistiska beslut om hemlig rumsavlyssning inklusive tillträde för att installera utrustningen, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

I stort sett motsvarande bestämmelser om interimistiska beslut finns i lagen (2020:62) om hemlig dataavläsning. Enligt dessa får interimistiska beslut inte avse rumsavlyssningsuppgifter (17 § första stycket lagen om hemlig dataavläsning). Med hänsyn till sambandet mellan bestämmelserna om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter omfatta våra överväganden även frågan om det bör bli tillåtet med interimistiska beslut om hemlig dataavläsning som gäller rumsavlyssningsuppgifter och tillträde för att installera utrustning för sådan dataavläsning.

11.2 Gällande rätt

Bestämmelserna om prövning av och beslut om hemlig rumsavlyssning finns i 27 kap. 21 § RB. Där framgår att frågor om hemlig rumsavlyssning prövas av rätten på ansökan av åklagaren. Vidare framgår bl.a. vad beslutet ska innehålla. Om tillståndet är förenat med ett särskilt tillstånd enligt 25 a § att få tillträde till en plats för att installera tekniska hjälpmedel (tillträdestillstånd), ska det anges särskilt i beslutet.

Åklagare har ingen möjlighet att fatta beslut om hemlig rumsavlyssning. En sådan möjlighet finns däremot när det gäller hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektro-

nisk kommunikation och hemlig kameraövervakning (27 kap. 21 a § RB). Möjligheten får utnyttjas om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd. Åklagarens beslut fattas då i avvaktan på rättens beslut, vilket innebär att beslutet skyndsamt ska överprövas av rätten, som är skyldig att upphäva beslutet om den bedömer att det inte finns skäl för åtgärden. Om åklagarens beslut har verkställts innan rätten gjort en prövning, 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 avlyssningen eller övervakningen, eller för någon annan som uppgifterna avser.

Rumsavlyssningsuppgifter kan även inhämtas med hjälp av ett beslut om hemlig dataavläsning (2 § första stycket 4 lagen om hemlig dataavläsning). Åklagare har en möjlighet att fatta interimistiska beslut om hemlig dataavläsning inklusive ett beslut om tillträdestillstånd för installation av utrustning (prop. 2019/20:64 s. 231). Möjligheten till interimistiskt beslut omfattar dock inte rumsavlyssningsuppgifter.

Tillträdestillstånd

Bestämmelser om tillträde för installation av teknisk utrustning för hemlig rumsavlyssning finns i 27 kap. 25 a § RB. Ett beslut om tillträdestillstånd fattas av rätten. Ett tillträdestillstånd får endast avse den plats som ska avlyssnas eller, om det finns särskilda skäl, en plats som direkt angränsar till den platsen. Om tillståndet avser enbart hemlig rumsavlyssning får tillträdestillståndet till en sådan angränsande plats inte avse någon annan stadigvarande bostad än den misstänktes. Ett tillträdestillstånd som omfattar även hemlig kameraövervakning får över huvud taget inte avse någons stadigvarande bostad. Om ett tillstånd till tillträde och installation avser ett fordon, får den verkställande myndigheten, om det behövs, tillfälligt flytta fordonet i samband med tillträdet.

Om ett tekniskt hjälpmedel har installerats ska hjälpmedlet tas bort eller göras obrukbart så snart som möjligt efter det att tiden för tillståndet har gått ut eller tillståndet har upphävts. När ett beslut om hemlig rumsavlyssning verkställs får olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt

Vid hemlig dataavläsning får den verkställande myndigheten, efter särskilt tillstånd, i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång (12 §). Ett sådant tillstånd får endast avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller en sådan person som anges i 7 § första stycket eller 9 § första stycket, får tillstånd beviljas endast om det finns synnerlig anledning att anta att informationssystemet finns där. I 13 § finns bestämmelser som innebär att ett tillträdestillstånd aldrig kan omfatta vissa platser, däribland en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen. I konsekvens med förbudet mot interimistiska beslut om hemlig rumsavlyssning får ett interimistiskt beslut om tillträdestillstånd för hemlig dataavläsning inte avse rumsavlyssningsuppgifter.

Jourdomstolarna

Enligt 19 kap. 12 § RB gäller att de s.k. jourdomstolarna är behöriga att i brådskande fall besluta om tvångsmedel. Av förordningen (1988:31) om tingsrätternas beredskap för prövning av häktningsfrågor m.m. framgår att tingsrätterna ska ha beredskap att pröva bl.a. frågor om tvångsmedel under söndag, annan allmän helgdag, lördag och vissa aftnar. Beredskapen fullgörs genom att domstolen är tillgänglig för beslut vissa tider under dagtid. Domstolarna har alltså möjlighet att i vissa fall snabbt kunna ta hand om brådskande frågor om tvångsmedel, men någon beredskap dygnet runt finns inte. I praktiken torde det numera främst vara brådskande framställningar om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter som hanteras av jouren, eftersom åklagare kan fatta interimistiska beslut om övriga hemliga tvångsmedel.

11.3 Bakgrund

Åklagarmyndigheten har anfört att lagstiftningen om hemlig rumsavlyssning måste anpassas så att åklagare ges möjlighet att fatta interimistiska beslut, inklusive beslut om tillstånd till tillträde för att installera utrustningen (Framställning om ändringar i lagstiftningen om hemliga tvångsmedel i 27 kap. rättegångsbalken (Ju2019/03572/Å s. 5–11). Myndigheten har i samband med detta anfört i huvudsak följande.

Hemlig rumsavlyssning har ursprungligen varit avsedd att användas i lokaler eller fordon som brottsmisstänkta personer disponerar. För att man ska kunna verkställa beslut om hemlig rumsavlyssning på sådana platser krävs det ofta en omfattande kartläggning och planering och ofta även ett intrång i det utrymme där avlyssningsutrustningen ska installeras och eventuellt även avläsas. Det har därför inte funnits något behov av snabba beslut om hemlig rumsavlyssning. Teknikutvecklingen och förändringar i brottsliga personers beteende har emellertid ändrat dessa förutsättningar. Bland annat har det tillkommit utrustning som ger möjlighet att på visst avstånd avlyssna kommunikation utan en föregående teknisk installation.

När de brottsbekämpande myndigheterna får kännedom om ett nära förestående möte mellan misstänkta personer som det skulle vara värdefullt att avlyssna med hemlig rumsavlyssning behövs ett snabbt beslut om tillstånd till åtgärden. Som regel är det dock i sådana situationer omöjligt att hinna inhämta tillstånd från domstol. En annan situation som kräver snabba beslut om hemlig rumsavlyssning är när det finns misstanke om att brott begås i samband med gränspassage. Tullverket har numera möjlighet att installera avlyssningsutrustning, t.ex. i fordon som blir föremål för tullkontroll när de passerar gränsen. Av tidsskäl är det dock inte möjligt att få tillstånd av domstol. Detta är otillfredsställande, särskilt vid en jämförelse med den situationen att en misstänkt kommer ensam i en bil som tillåts köra vidare och vars telefonsamtal under den fortsatta färden – t.ex. med en uppdragsgivare eller mottagare av det insmugglade, kan bli föremål för hemlig avlyssning i enlighet med ett interimistiskt åklagarbeslut. Möjligheterna att på kvällar och helger få tillstånd av domstol till hemlig rumsavlyssning är i det närmaste obefintliga.

Åklagarmyndigheten har vidare anfört att en möjlighet för åklagarna att fatta interimistiskt beslut om hemlig rumsavlyssning i stora

delar skulle möta de behov som beskrivits ovan. En åklagare kan då enligt myndigheten involveras tidigt inför en eventuell avlyssning och sedan löpande stå i kontakt med en spanare eller annan polisman och närmast fortlöpande bedöma frågan om hemlig rumsavlyssning beroende på hur de aktuella platserna och övriga omständigheter vid tillfället ter sig. Platsen liksom tiden för åtgärden kan lättare begränsas, eftersom beslutet kan fattas i tidsmässigt nära samband med det samtal som ska avlyssnas.

11.4 Tidigare överväganden

I samband med införandet av lagen om hemlig rumsavlyssning övervägdes det om åklagaren skulle ha en möjlighet att fatta interimistiska beslut (prop. 2005/06:178 Hemlig rumsavlyssning s. 72). Rikspolisstyrelsen hade framfört att det borde finnas en sådan möjlighet, eftersom det i vissa fall kan krävas att polisen agerar mycket snabbt och att ett beslut från domstol då inte kan inväntas. Som exempel nämndes den gången att det kan röra sig om en mycket kort tidsperiod från det att polisen får kännedom om ett möte till dess mötet ska äga rum. Rikspolisstyrelsen hade angett att den beskrivna situationen är typisk för kontrollerade leveranser av narkotika, där leverantör och mottagare inte sällan stämmer träff på t.ex. en restaurang för att diskutera hur kuriren ska lämna över narkotikan till mottagaren. Regeringen ifrågasatte inte att det i vissa fall skulle vara värdefullt med en möjlighet för åklagare att fatta interimistiska beslut i ärenden om hemlig rumsavlyssning. Mot detta måste dock enligt regeringen ställas att det var fråga om ett nytt hemligt tvångsmedel som typiskt sett är mycket ingripande. Vidare menade regeringen att det vid fara i dröjsmål torde vara möjligt för en jourdomstol i de flesta fall att ta upp frågan till prövning. Bedömningen gjordes därför att någon möjlighet för åklagaren att fatta interimistiska beslut i fråga om hemlig rumsavlyssning inte borde införas.

Som framgått i avsnitt 11.1 har frågan om att låta åklagare fatta interimistiska beslut om hemlig rumsavlyssning även i fredstid även varit föremål för regeringens överväganden i propositionen Hemliga tvångsmedel mot allvarliga brott (prop. 2013/14:237). Regeringen uttalade då att behovet av en möjlighet att fatta interimistiska beslut inte i någon beaktansvärd grad kunde anses skilja sig åt beroende på vilket

hemligt tvångsmedel det är fråga om (s. 140). Inte heller ansågs det avgörande för behovet vara vilket brott det är fråga om. I stället ansågs de relevanta faktorerna vara dels i vilket skede tvångsmedlen används, dels omfattningen av det integritetsintrång som respektive tvångsmedel typiskt sett för med sig. Vad gäller det typiska integritetsintrånget konstaterade regeringen att det finns skillnader mellan de hemliga tvångsmedlen och att hemlig rumsavlyssning är det tvångsmedel som typiskt sett leder till det största intrånget i enskildas personliga integritet.

En ordning med efterföljande obligatorisk domstolsprövning ansågs innebära att det saknades skäl att anta att en utökad möjlighet för åklagare att fatta interimistiska beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och kvarhållande av försändelse skulle få några negativa konsekvenser för enskildas rättssäkerhet (s. 141). Starka behovsskäl ansågs också tala för att det var nödvändigt att införa en sådan ordning. Bedömningen vilade även på den särskilda begränsningsregel som innebär att redan inhämtade uppgifter inte får användas till nackdel för någon om rätten vid den efterföljande brottsutredningen finner att det saknats skäl för åtgärden (s. 144). Regeln ansågs nödvändig för att säkerställa att utökade möjligheter till interimistiska beslut inte skulle få negativa konsekvenser för enskildas rättssäkerhet. Regeringen ansåg vidare att alternativet att tillåta interimistiska åklagarbeslut i fler situationer var att föredra från rättssäkerhetssynpunkt framför att ta bort kravet på en viss adress, plats eller kommunikationsutrustning alltid ska anges i tvångsmedelsbesluten, något som också diskuterades.

När det gällde hemlig rumsavlyssning gjorde regeringen motsatt bedömning. Eftersom hemlig rumsavlyssning är det tvångsmedel som typiskt sett leder till det största intrånget i enskildas personliga integritet ansågs särskild försiktighet påkallad (s. 142). Regeringen var därför vid den tidpunkten inte beredd att föreslå att interimistiska beslut om hemlig rumsavlyssning skulle tillåtas.

Frågan om en möjlighet för åklagare att fatta interimistiska beslut behandlades även i propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 152–154). Där anförde regeringen i huvudsak samma argument till stöd för bedömningen att en interimistisk beslutanderätt borde finnas. Utan möjlighet till interimistiska beslut fanns det enligt regeringen en risk för att hemlig dataavläsning skulle bli utan verkan när verkställighetsåtgärder behöver vidtas med mycket kort varsel. De rätts-

säkerhetsgarantier som föreslogs gälla för hemlig dataavläsning i allmänhet borde enligt regeringen också gälla när åklagare fattar interimistiska beslut. Regeringen gjorde bedömningen att dessa krav var tillräckliga. Vidare ansåg regeringen att förutsättningarna för interimistisk åklagarprövning borde vara desamma som för befintliga tvångsmedel. När det gällde rumsavlyssningsuppgifter anfördes endast att det inte borde finnas någon möjlighet till interimistiska beslut avseende sådana uppgifter, eftersom det inte finns någon rätt för åklagare att ge interimistiska beslut vid hemlig rumsavlyssning.

11.5 Interimistiska beslut bör tillåtas

Förslag: Åklagare ska få fatta interimistiskt beslut om hemlig rumsavlyssning och tillträdestillstånd för installation av utrustning för hemlig rumsavlyssning, om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd. Åklagare ska även få möjlighet att, på motsvarande villkor, fatta interimistiskt beslut om hemlig dataavläsning avseende rumsavlyssningsuppgifter och tillträdestillstånd för installation av tekniska hjälpmedel i syfte att inhämta sådana uppgifter.

Skälen för förslaget

Frågorna

Sedan den 1 juli 2012 har åklagaren interimistisk beslutanderätt beträffande hemlig övervakning av elektronisk kommunikation. Den 1 januari 2015 infördes en motsvarande beslutanderätt i fråga om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och kvarhållande av försändelse. En sådan möjlighet fanns tidigare endast enligt lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott och lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. Åklagare har även en interimistisk beslutanderätt beträffande hemlig dataavläsning, med undantag för sådan dataavläsning som gäller rumsavlyssningsuppgifter eller hemlig dataavläsning vid särskild utlänningskontroll enligt 9 § lagen om hemlig dataavläs-

ning. Regeringen framhöll i propositionen Hemliga tvångsmedel mot allvarliga brott (s. 138) att domstolsprövningen är en viktig del av det system med rättssäkerhetsgarantier som omgärdar tillämpningen av de hemliga tvångsmedlen, varför det är en självklar utgångspunkt att befogenheter för åklagare att fatta interimistiska beslut om tvångsmedlen enbart bör förekomma om starka skäl talar för det. I propositionen gjorde regeringen bedömningen att det inte vid den tidpunkten var lämpligt att införa en möjlighet för åklagare att fatta interimistiska beslut om hemlig rumsavlyssning. Frågan är om det i dag finns skäl för en annan bedömning, och i så fall om det även bör finnas en möjlighet till interimistiska beslut om hemlig dataavläsning avseende rumsavlyssningsuppgifter.

Hemlig rumsavlyssning

Det kan enligt vår mening knappast ifrågasättas att det finns ett behov av en möjlighet till interimistiska beslut avseende hemlig rumsavlyssning. Det är ett tvångsmedel som kan vara avgörande för möjligheten att framgångsrikt förhindra och utreda mycket allvarlig brottslighet. Detta gäller inte minst då yrkeskriminella har goda kunskaper om de brottsbekämpande myndigheternas möjligheter att avlyssna eller avläsa elektronisk kommunikation, och därför i många fall väljer bort sådan kommunikation till förmån för fysiska möten. Hemlig rumsavlyssning kan då vara den enda möjligheten för de brottsbekämpande myndigheterna att kunna ta del av de samtal som förs, och som kan vara av synnerlig vikt för utredningen.

I propositionen Hemliga tvångsmedel mot allvarliga brott (s. 138 och 139) anfördes att det ibland kan finnas behov av att mycket snabbt kunna utverka beslut om hemliga tvångsmedel och att den dåvarande ordningen medförde problem vid minutoperativa åtgärder. Som exempel nämndes att polisen med mycket kort varsel kan få reda på möten som ska äga rum i hotellrum eller fordon. Tullverket framhöll att snabbheten i förfarandet kan vara en avgörande faktor vid exempelvis kontrollerade leveranser, eller när det finns behov av att snabbt kunna montera utrustning vid t.ex. färjelägen i samband med att fordon finns inne för tullkontroll. Regeringen ansåg som självklart att behovet av ett snabbt beslut om ett hemligt tvångsmedel kan uppstå även på tider då det inte finns någon beredskap

hos tingsrätterna, och att det inte var tillfredsställande att möjligheterna att använda hemliga tvångsmedel i dessa fall var beroende av att polis och åklagare lyckas få tag i en domare som var beredd att pröva ärendet utanför arbetstid. Med hänsyn till detta ansågs det föreligga starka skäl för en effektivisering av reglerna för att behovet av snabba beslut bättre skulle kunna tillgodoses. I sammanhanget uttalade regeringen vidare att det inte är rimligt att bygga upp en organisation för dygnetruntberedskap hos domstolarna och att det kunde ifrågasättas om en sådan organisation fullt ut skulle kunna tillgodose behovet av snabba beslut. Redan den tidsutdräkt som uppkommer genom att åklagaren måste ta sig till domstolen för att få framställan prövad kan nämligen enligt regeringen få allvarliga konsekvenser.

De skäl som regeringen anförde i samband med att möjligheterna till interimistiska beslut om hemliga tvångsmedel utökades har under de år som gått inte förlorat sin relevans. Tvärtom är det enligt de brottsbekämpande myndigheterna vanligt förekommande att man med kort varsel får kännedom om att ett för brottsutredningen intressant möte ska äga rum, eller att platsen för mötet har ändrats. Det kan vara så enkelt att myndigheterna har vetskap om att ett möte ska ske på ett visst café som sedan visar sig vara fullsatt, varför personerna i stället sätter sig på ett annat närliggande café. Det krävs i sådana och liknande fall ett skyndsamt beslut för att en hemlig rumsavlyssning av mötet ska kunna ske. Andra situationer där det kan krävas ett snabbt beslut är vid gränspassage. Som nämndes i 2013/14 års proposition kan Tullverket då i vissa fall ha möjlighet att installera utrustning för hemlig avlyssning i samband med tulltjänstemän tar ut ett fordon för tullkontroll. I praktiken är det dock nödvändigt att detta kan ske snabbt. Det kan även vara så att ett annat land har en pågående rumsavlyssning i ett fordon som har passerat eller inom kort kommer att passera den svenska gränsen. Det andra landets brottsbekämpande myndigheter kan då begära svenskt bistånd med att fortsätta avlyssningen på svenskt territorium. Även då kan det krävas ett skyndsamt beslut.

Som regeringen konstaterade i 2013/14 års proposition kan det vara svårt eller omöjligt att få till stånd en domstolsprövning med den skyndsamhet som krävs. Detta gäller generellt men särskilt när behovet uppstår utanför ordinarie arbetstid eller jourtid. Något jourdomstolssystem med dygnetruntberedskap finns inte och det är, som regeringen tidigare framhållit, tveksamt om ett sådant system fullt

ut skulle motsvara behovet av snabba beslut i verkligt brådskande fall. Avsaknaden av en möjlighet till snabba beslut om hemlig rumsavlyssning i brådskande fall får i praktiken kännbara konsekvenser för de brottsbekämpande myndigheternas möjligheter att utreda allvarlig brottslighet och kan även leda till att våra brottsbekämpande myndigheter inte kan bistå andra länder när skyndsamhet krävs.

Behovet av en möjlighet till interimistiska beslut om hemlig rumsavlyssning förelåg redan när möjligheten till interimistiska beslut avseende de andra hemliga tvångsmedlen infördes. Det var alltså inte avsaknaden av behov, utan hänsynen till enskildas integritet som ledde till att regeringen vid den tidpunkten inte var beredd att införa en möjlighet till interimistiska beslut avseende hemlig rumsavlyssning. Sedan dess har det skett tekniska framsteg. Till skillnad från vad som i allmänhet gällde då kan det numera vara möjligt att snabbt installera avlyssningsutrustning, eller att genomföra en avlyssning utan någon föregående installation. Det kan därför i vissa fall finnas möjlighet att snabbt och utan större förberedelser verkställa ett beslut om hemlig rumsavlyssning – något som sällan var möjligt när frågan om interimistiska beslut senast var uppe till bedömning. Behovet och den förväntade nyttan av snabba beslut har därför ökat jämfört med hur situationen såg ut när regeringen senast tog ställning till frågan.

Med hänsyn till det anförda finns det enligt vår bedömning tveklöst ett behov av en möjlighet för åklagare att kunna fatta interimistiska beslut om hemlig rumsavlyssning.

Att det i och för sig finns ett behov innebär inte med automatik att det är godtagbart att överlämna beslutsfattandet till åklagare. Som konstaterades i propositionen Hemliga tvångsmedel mot allvarliga brott anses hemlig rumsavlyssning som det typiskt sett mest integritetskänsliga tvångsmedlet. Detta avspeglas på flera sätt i regelverket, bl.a. genom att hemlig rumsavlyssning endast kan komma i fråga för den allra allvarligaste brottsligheten. Regeringen ansåg med hänsyn till detta att en särskild försiktighet var motiverad. Vid den tidpunkten var möjligheten till interimistiska beslut om hemlig övervakning av elektronisk kommunikation ny (prop. 2011/12:55 s. 78 f.) och det fanns ingen möjlighet till interimistiska åklagarbeslut om övriga hemliga tvångsmedel enligt rättegångsbalken. En sådan möjlighet fanns däremot enligt den tidsbegränsade lagen om åtgärder för att utreda vissa samhällsfarliga brott, som gällde vid förundersökning angående vissa brott som ansågs särskilt allvarliga för landets säkerhet och lagen

om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. De möjligheter som fanns till interimistiska beslut användes dock mycket sparsamt (prop. 2013/14:237 s. 140). Erfarenheten av interimistiska åklagarbeslut avseende hemliga tvångsmedel var alltså relativt begränsad. Det ställningstagande som gjordes den gången i fråga om hemlig rumsavlyssning bör ses i ljuset av detta förhållande.

Vi konstaterar, liksom Åklagarmyndigheten gjort i den tidigare nämnda framställningen från 2019, att möjligheten till interimistiska åklagarbeslut beträffande andra hemliga tvångsmedel numera har funnits under ett antal år och i huvudsak utnyttjats på ett korrekt sätt. Det framgår av regeringens redogörelser för användningen av hemliga tvångsmedel 2018 och 2019 att det är ovanligt att åklagares interimistiska beslut om hemliga tvångsmedel upphävs vid den efterföljande domstolsprövning som alltid ska ske (Regeringens skrivelse [2020/21:59] Redovisning av användningen av hemliga tvångsmedel under 2018 och Regeringens skrivelse [2020/21:59] Redovisning av användningen av hemliga tvångsmedel under 2019). Enligt regeringens redovisning av användningen av hemliga tvångsmedel under 2020 (skr. 2021/22:79) står sig bilden. Av redovisningen framgår att endast ett litet fåtal interimistiska beslut upphävdes av domstol under året, samtliga avseende hemlig övervakning av elektronisk kommunikation. Under 2020 gavs 13 497 tillstånd till hemlig övervakning av elektronisk kommunikation, varav 139 var interimistiska åklagarbeslut. Av dessa upphävdes fyra av domstol. När det gäller övriga hemliga tvångsmedel fastställdes samtliga interimistiska beslut av domstol.

Av det anförda drar vi slutsatsen att åklagare som fattar beslut om hemliga tvångsmedel har goda kunskaper om förutsättningarna för användning av sådana tvångsmedel och som regel gör samma bedömning som domstolarna i frågan om ett tillstånd får meddelas. Det finns ingen anledning att tro att det skulle förhålla sig annorlunda med hemlig rumsavlyssning. Som nyss sagts är det fråga om ett tvångsmedel som endast får användas vid misstanke om mycket allvarlig brottslighet. Förundersökningar om sådan brottslighet hanteras ofta av erfarna åklagare med stor vana av att handlägga frågor om hemliga tvångsmedel. Risken för felaktiga bedömningar kan därför antas vara låg. Om en möjlighet till interimistiska beslut kombineras med en ordning med obligatorisk domstolsprövning – något som framstår som en självklarhet – finns det ingen anledning att tro

att möjligheten skulle leda till negativa konsekvenser för enskildas rättssäkerhet (jfr prop. 2013/14:237 s. 141). Här bör man även beakta bestämmelsen i 27 kap. 21 a § RB, som går ut på att uppgifter som hämtats in innan rätten prövat ett interimistiskt beslut, inte får användas till nackdel för den avlyssnade eller någon annan som uppgifterna avser, om rätten vid sin prövning kommer fram till att det saknats skäl för åtgärden. Bestämmelsen bör, om det införs en möjlighet till interimistiska beslut om hemlig rumsavlyssning, omfatta även uppgifter som hämtats in genom detta tvångsmedel. Någon risk för att uppgifter som hämtats in till följd av ett felaktigt åklagarbeslut används till någons nackdel skulle därmed inte finnas. Däremot innebär själva avlyssningen och granskningen av materialet ett integritetsintrång i sig.

Till ovanstående kommer, som vi utvecklat närmare i avsnitt 10.5, att tekniken och de brottsbekämpande myndigheternas arbetssätt numera möjliggör en mycket hög grad av precision. Vid en avlyssning på exempelvis ett café eller någon annan allmän plats används numera utrustning som riktas in enbart på de misstänkta. Utrustningen fångar alltså inte upp samtal som förs i omgivningen. I fall där hemlig avlyssning äger rum i lokaler och på platser som är tillgängliga för allmänheten är därmed risken för att utomståendes samtal oavsiktligt fångas upp mycket liten.

Med hänsyn till det påtagliga behovet, de ändrade förhållandena och till det som anförts om Åklagarmyndighetens hantering av möjligheten till interimistiskt beslutsfattande, anser vi att tiden nu är mogen för en annan bedömning än den som gjordes i propositionen Hemliga tvångsmedel mot allvarliga brott. Vi föreslår därför att åklagare ges en möjlighet att, i avvaktan på rättens prövning, meddela tillstånd till hemlig rumsavlyssning. Möjligheten bör gälla även när beslutet, i enlighet med våra förslag i kapitel 10, avser den skäligen misstänkte i stället för en plats. Samma villkor för meddelande av ett interimistiskt beslut bör gälla som för andra hemliga tvångsmedel, dvs. att det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd (jfr 27 kap. 21 a § första stycket RB). Som redan antytts bör även bestämmelserna om obligatorisk domstolsprövning och om förbud mot att använda de uppgifter man fått tillgång till om rätten upphäver beslutet efter verkställighet göras tillämpliga (andra och tredje styckena i samma paragraf).

Hemlig dataavläsning

Den beskrivning av behovet som gjorts under föregående rubrik är i allt väsentligt relevant även när det gäller hemlig dataavläsning som avser rumsavlyssningsuppgifter. Det kan med kort varsel vara möjligt att utföra en hemlig dataavläsning avseende rumsavlyssningsuppgifter, t.ex. genom att använda den misstänktes telefon. Vi gör bedömningen att det finns ett behov av en möjlighet till interimistiska åklagarbeslut avseende hemlig dataavläsning som gäller rumsavlyssningsuppgifter. Lagen om hemlig dataavläsning är en tidsbegränsad försökslag som, om Riksdagen inte vidtar åtgärder för att göra den permanent, kommer att upphöra att gälla vid utgången av mars 2025. Eftersom lagen endast varit i kraft under en kort tid är erfarenheten av att tillämpa den begränsad. Samma sak gäller åklagarnas möjlighet att i vissa fall fatta interimistiska beslut. Detta talar emot att man nu gör ändringar i lagen. Som vi har konstaterat på flera andra ställen i betänkandet finns det samtidigt en stark koppling mellan hemlig dataavläsning och övriga hemliga tvångsmedel. Av särskild betydelse är det att hemlig dataavläsning kan vara en annan metod för att få tillgång till samma slags uppgifter som man kan komma åt med hjälp av något av de andra hemliga tvångsmedlen. Möjligheten att använda hemlig dataavläsning för att åtkomma olika slags uppgifter korresponderar därför i princip med möjligheten att komma åt motsvarande uppgifter genom respektive annat hemligt tvångsmedel. Sålunda korresponderar möjligheten att genomföra en hemlig dataavläsning i syfte att få tillgång till rumsavlyssningsuppgifter i princip med möjligheten att genomföra en hemlig rumsavlyssning. Likaledes motsvarar möjligheten för åklagare att fatta ett interimistiskt beslut om hemlig dataavläsning möjligheten till sådana beslut avseende respektive hemligt tvångsmedel. Både effektivitetsskäl och systematiska skäl talar för att man behåller denna koppling. I de fåtal fall där åklagare hittills fattat ett interimistiskt beslut om hemlig dataavläsning har beslutet fastställts av domstol. Underlaget är dock så litet att det inte tillåter några långtgående slutsatser. Däremot menar vi att det saknas anledning att anta att åklagare skulle ha sämre förmåga att hantera ärenden om hemlig dataavläsning avseende rumsavlyssningsuppgifter än andra interimistiska ärenden om hemliga tvångsmedel. Med hänsyn till det anförda bedömer vi att möjligheten för åklagare att fatta ett interimistiskt beslut om hemlig dataavläsning under en förundersökning

bör utvidgas så att den även omfattar rumsavlyssningsuppgifter. Möjligheten bör gälla även när beslutet, i enlighet med våra förslag i kapitel 10, avser den skäligen misstänkte i stället för en plats. I övrigt bör förutsättningarna för ett interimistiskt beslut vara desamma som nu.

Tillträdestillstånd

I en del fall är det möjligt att utföra en hemlig rumsavlyssning eller en hemlig dataavläsning avseende rumsavlyssningsuppgifter utan att någon fysisk utrustning behöver installeras på en plats som är skyddad mot intrång. I andra fall kan det vara möjligt att få tillstånd till installation av utrustningen av den som förfogar över den skyddade platsen. Det finns dock även situationer där det, för att tvångsmedlet ska kunna verkställas, är nödvändigt att få tillträde till en plats som är skyddad mot intrång för att man där ska kunna installera någon form av hårdvara eller annan teknisk utrustning. Enligt bestämmelserna i 27 kap. 25 a § RB respektive 12 § lagen om hemlig dataavläsning kan rätten ge den verkställande myndigheten ett särskilt tillstånd att i hemlighet skaffa sig tillträde till en skyddad plats i syfte att kunna genomföra en sådan installation. För att möjligheten till interimistiska åklagarbeslut ska kunna användas på ett effektivt sätt finns det enligt vår bedömning ett behov av att åklagaren samtidigt kan fatta beslut om tillträdestillstånd för installation av den utrustning som behövs för avlyssningen (jfr vårt ställningstagande i frågan om tillträdestillstånd för enbart hemlig kameraövervakning i avsnitt 12.5). Frågan är om detta kan godtas från andra aspekter.

Åklagare har stor vana av att hantera ärenden som handlar om tillträde till bostäder och andra skyddade utrymmen, eftersom de ofta fattar beslut om husrannsakan i sådana utrymmen. Även om det är en viktig principiell skillnad att det i det nu aktuella fallet är fråga om en hemlig åtgärd, framstår själva intrånget i lokalen inte i övrigt som mer integritetskänsligt än en husrannsakan. Vidare kan konstateras att åklagare redan i dag har möjlighet att interimistiskt besluta om tillträdestillstånd när det gäller hemlig dataavläsning, med undantag för avläsning som avser rumsavlyssningsuppgifter. Hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter innebär typiskt sett att större integritetsintrång än hemlig dataavläsning avseende andra slags uppgifter. Detta innebär dock inte att det

integritetsintrång som själva tillträdet och installationen innebär är större. Det finns alltså inte med hänsyn till integritetsaspekten anledning att göra en annan bedömning än den som gjorts i fråga om hemlig dataavläsning avseende andra slags uppgifter än rumsavlyssningsuppgifter. Med hänsyn till detta och då starka behovsskäl talar för det, bör åklagaren ges möjlighet att besluta interimistiskt om tillträdestillstånd för hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter.

12 Tillträdestillstånd för hemlig kameraövervakning

12.1 Uppdraget

För att man ska kunna installera utrustning för hemlig kameraövervakning på en plats som är skyddad mot intrång krävs det antingen att den som förfogar över platsen har gett sitt samtycke till installationen eller att rätten har beslutat om tillträdestillstånd med stöd av 27 kap. 25 a § RB. Rätten kan endast meddela ett tillträdestillstånd för hemlig kameraövervakning om man samtidigt ska verkställa ett beslut om hemlig rumsavlyssning. När regeln infördes ansågs den medföra att möjligheten till tillträdestillstånd för hemlig kameraövervakning skulle begränsas till de mycket allvarliga och samhällsfarliga brotten (prop. 2013/14:237 s. 154).

Åklagarmyndigheten har uppgett att ett tillträde för enbart hemlig kameraövervakning ofta fås genom att samtycke inhämtas från den som förfogar över platsen. Det kan dock finnas fall där sådant samtycke inte lämnas eller där det inte är lämpligt att inhämta ett sådant samtycke, t.ex. om den som kan lämna samtycke är misstänkt för inblandning i brottsligheten (Ju2019/03572/Å s. 13).

Vid hemlig dataavläsning får den verkställande myndigheten, efter särskilt tillstånd, i hemlighet ska få skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång (12 § lagen [2020:62] om hemlig dataavläsning). Det är även möjligt för åklagare att under vissa förutsättningar fatta sådana interimistiska beslut (17 § samma lag). Reglerna om hemlig dataavläsning skiljer sig alltså i dessa avseenden från reglerna om hemlig kameraövervakning. Mot denna bakgrund har regeringen ansett att frågan om införande av en möjlighet till tillträdestillstånd för enbart hemlig kameraövervakning bör övervägas och att det då även bör övervägas om åklagare bör få möjlighet att fatta interimistiska tillträdesbeslut.

Vi ska därför

- ta ställning till om den verkställande myndigheten bör kunna få tillstånd att i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång för att verkställa ett beslut om enbart hemlig kameraövervakning,
- ta ställning till om åklagare bör få möjlighet att interimistiskt besluta om sådant tillträde, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

12.2 Gällande rätt

Hemlig kameraövervakning

Hemlig kameraövervakning kan ske såväl på offentliga platser dit allmänheten har tillträde som på platser som är straffrättsligt skyddade mot intrång enligt bl.a. bestämmelserna om hemfridsbrott och olaga intrång i 4 kap. brottsbalken. Skyddet mot intrång gäller t.ex. för garage, trapphus, vindsgångar och andra gemensamma utrymmen i flerfamiljshus. Det gäller även för platser som endast är tillgängliga för allmänheten på vissa tider, under sådana tider då allmänheten inte har tillträde. Ett beslut om tillstånd till hemlig kameraövervakning omfattar inte tillstånd att bereda sig tillträde till den plats som ska övervakas för installation av kamerautrustningen. En möjlighet som ofta utnyttjas är att den brottsbekämpande myndigheten inhämtar tillåtelse från en behörig person, t.ex. en fastighetsägare, att installera kamerautrustning på den intrångsskyddade plats som ska kameraövervakas. Det finns även bestämmelser om tillträdestillstånd i 27 kap. 25 a § RB. Ett tillstånd för att installera kamerautrustning får dock endast meddelas om tillståndet även avser hemlig rumsavlyssning. Det är inte tillåtet att placera ut utrustning i ett skyddat utrymme i samband med att man gör intrång i det skyddade utrymmet under exempelvis en husrannsakan. Detta skulle strida mot ändamålsprincipen och har även ansetts innebära ett kringgående av regleringen om hemlig kameraövervakning (prop. 2013/14:237 s. 152 och Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas? 4:e uppl. s. 570 och 571).

Ett tillträdestillstånd får endast avse den plats som ska avlyssnas eller, om det finns särskilda skäl, en plats som direkt angränsar till den platsen. Om tillståndet avser enbart hemlig rumsavlyssning får tillträdestillståndet till en sådan angränsande plats inte avse någon annan stadigvarande bostad än den misstänktes. Ett tillträdestillstånd som omfattar även hemlig kameraövervakning får över huvud taget inte avse någons stadigvarande bostad. Det är alltså inte möjligt att installera kamerautrustning i en stadigvarande bostad.

Om ett tillstånd till tillträde och installation avser ett fordon, får den verkställande myndigheten, om det behövs, tillfälligt flytta fordonet i samband med tillträdet.

Om ett tekniskt hjälpmedel har installerats ska hjälpmedlet tas bort eller göras obrukbart så snart som möjligt efter det att tiden för tillståndet har gått ut eller tillståndet har upphävts. När ett beslut om hemlig rumsavlyssning eller hemlig kameraövervakning verkställs får olägenhet eller skada inte förorsakas utöver vad som är absolut nödvändigt

Hemlig dataavläsning

Kameraövervakningsuppgifter kan även inhämtas med hjälp av ett beslut om hemlig dataavläsning (2 § första stycket 4 lagen om hemlig dataavläsning). Vid hemlig dataavläsning får den verkställande myndigheten, efter särskilt tillstånd, i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång (12 §). Ett sådant tillstånd får endast avse en plats där det finns särskild anledning att anta att det avläsningsbara informationssystemet finns tillgängligt. Om platsen är en bostad som stadigvarande används av någon annan än den misstänkte eller en sådan person som anges i 7 § första stycket eller 9 § första stycket, får tillstånd beviljas endast om det finns synnerlig anledning att anta att informationssystemet finns där. I 13 § finns bestämmelser som innebär att ett tillträdestillstånd aldrig kan omfatta vissa platser, däribland en plats som stadigvarande används eller är särskilt avsedd att användas för verksamhet där tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen.

Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen eller för möjligheterna att förebygga,

förhindra eller upptäcka den brottsliga verksamheten att inhämta rättens tillstånd i frågor om hemlig dataavläsning, får åklagaren ge tillstånd i avvaktan på rättens beslut. Ett sådant interimistiskt beslut kan omfatta även tillträdestillstånd (prop. 2019/20:64 s. 231). I konsekvens med förbudet mot interimistiska beslut om hemlig rumsavlyssning får ett interimistiskt beslut om hemlig dataavläsning inte avse rumsavlyssningsuppgifter.

12.3 Tidigare överväganden

Bestämmelserna om en möjlighet att meddela tillträdestillstånd beträffande hemlig kameraövervakning när hemlig rumsavlyssning samtidigt förekommer infördes i enlighet med förslag i propositionen Hemliga tvångsmedel mot allvarliga brott (prop. 2013/14:237 s. 154 och 155). Regeringen framhöll att möjligheten skulle tillgodose faktiska behov hos de brottsbekämpande myndigheterna och medföra nytta främst genom att det skulle kunna klarläggas vilka som har deltagit i och vem som fällt olika yttranden under ett samtal. Regeringen framhöll vidare att kopplingen till hemlig rumsavlyssning medför att en möjlighet till tillträdestillstånd för hemlig kameraövervakning begränsas till de mycket allvarliga och samhällsfarliga brott som det förstnämnda tvångsmedlet omfattar.

Övervakning med kameror som placeras på platser som är skyddade mot intrång skulle enligt regeringen kunna medföra mycket betydande integritetsintrång. Detta ansågs särskilt gälla beträffande bostäder. Regeringen ansåg därför, i likhet med Utredningen om vissa hemliga tvångsmedel och majoriteten av remissinstanserna, att det inte heller i fortsättningen borde vara tillåtet att övervaka någon från en kamera som efter intrång placerats i en stadigvarande bostad.

I propositionen betonades vikten av att det görs en noggrann proportionalitetsbedömning också beträffande tillträdestillståndet och dess effekter för kamerans placering. Regeringen framhöll att det sammantagna integritetsintrång som kan bli aktuellt måste beaktas och att platsens karaktär blir betydelsefull. Hemlig kameraövervakning bör t.ex. endast i undantagsfall kunna komma i fråga med kameror placerade på en toalett, i ett omklädningsrum eller i ett annat liknande utrymme.

I propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 143–146) konstaterade regeringen att det vid verkställighet av hemlig dataavläsning i vissa fall kommer att vara nödvändigt för den som ska verkställa åtgärden att komma närmare informationssystemet eller ha det i sin fysiska besittning. Som exempel nämns fall då hårdvara ska användas vid verkställighet eller när det inte är möjligt att på distans installera programvara. Vidare anförde regeringen följande.

> När det står klart var informationssystemet finns behöver den verkställande myndigheten få tillgång till det. Ett sätt att få tillgång till informationssystemet är att tillåta den brottsbekämpande myndigheten att få tillträde till utrymmen som annars är skyddade mot intrång, t.ex. enligt reglerna i 4 kap. brottsbalken. En möjlighet till tillträdestillstånd för hemlig dataavläsning utgör en utvidgning av möjligheterna till tillträdestillstånd eftersom det i dag endast är tillåtet vid hemlig rumsavlyssning. Åtgärden innebär dock på ett principiellt plan – när det gäller själva det tvångsvisa tillträdet till ett sådant utrymme som skyddas mot intrång – inte något ytterligare intrång än vad som redan är tillåtet vid en husrannsakan, vilken endast kräver anledning att anta att ett brott har begåtts på vilket fängelse kan följa, vilket är ett mycket lägre ställt krav än kravet för hemlig dataavläsning. Ett tillträdestillstånd för hemlig dataavläsning kan emellertid inte i övrigt jämföras med en husrannsakan eftersom den förra åtgärden görs i hemlighet. Samtidigt är hemlig dataavläsning en metod som fordrar att hårdvara kan installeras. För att tvångsmedlet ska ha önskad effektivitet måste de brottsbekämpande myndigheterna emellanåt kunna få tillträdestillstånd till annars skyddade utrymmen.

Regeringen ansåg på grund av det anförda och till skillnad från Säkerhets- och integritetsskyddsnämnden, Civil Rights Defenders och Sveriges advokatsamfund, att en möjlighet till tillträdestillstånd skulle införas.

12.4 Det bör vara möjligt med tillstånd för att enbart installera utrustning för hemlig kameraövervakning

Förslag: Det införs en möjlighet att besluta om tillträdestillstånd för installation av kamerautrustning utan något krav på att även hemlig rumsavlyssning ska ske.

Skälen för förslaget

Enligt dagens reglering kan ett tillstånd att installera utrustning för hemlig kameraövervakning på platser som är skyddade mot intrång endast meddelas i samband med ett tillstånd att installera utrustning för hemlig rumsavlyssning. Eftersom hemlig rumsavlyssning är det hemliga tvångsmedel som typiskt sett innebär störst integritetsintrång är möjligheterna att använda det tvångsmedlet betydligt mer inskränkta än möjligheterna att använda hemlig kameraövervakning. Huvudregeln är att det krävs att brottet som utreds har ett minimistraff på fyra års fängelse eller mer, medan motsvarande huvudregel för hemlig kameraövervakning är två års fängelse eller mer. I samband med införandet anförde regeringen att en möjlighet att installera kamerautrustning på platser där det ska utföras en hemlig rumsavlyssning skulle medföra nytta främst genom att det skulle kunna klarläggas vilka som har deltagit i och vem som fällt olika yttranden under ett samtal (prop. 2013/14:237 s. 154 och 155). Tanken tycks alltså i första hand ha varit att kameraövervakningen i dessa fall skulle vara ett komplement till rumsavlyssningen. Regeringen framhöll vidare att kopplingen till hemlig rumsavlyssning medför att en möjlighet till tillträdestillstånd för hemlig kameraövervakning begränsas till de mycket allvarliga och samhällsfarliga brott som det förstnämnda tvångsmedlet omfattar.

Det är enligt uppgift från Åklagarmyndigheten (Ju2019/03572/Å s. 13) vanligt att det är tillräckligt med en hemlig kameraövervakning, och att det alltså inte är nödvändigt att även utföra hemlig rumsavlyssning för att utredningen ska kunna tillföras nödvändig information. Eftersom möjligheterna att använda hemlig rumsavlyssning är begränsad till de allra allvarligaste brotten medan hemlig kameraövervakning är tillåtet i betydligt fler fall är det också vanligt att det finns rättsliga förutsättningar för hemlig kameraövervakning men inte för hemlig rumsavlyssning. I båda dessa situationer kan det förekomma ett behov av att installera kamerautrustning på en plats som annars är skyddad från intrång. I praktiken löser de brottsbekämpande myndigheterna ofta detta genom att man inhämtar samtycke från den som förfogar över platsen. Ett vanligt exempel är att en fastighetsägare samtycker till att kamerautrustning placeras i en trappuppgång, ett vindsförråd eller garage. Det inträffar dock även att den som förfogar över platsen inte ger sitt samtycke, eller att personen

inte kan nås med tillräcklig skyndsamhet. Det förekommer också att det inte är lämpligt att fråga om samtycke, exempelvis för att den som förfogar över platsen kan misstänkas för inblandning i brottsligheten eller kan befaras avslöja åtgärden för de misstänkta. I dessa situationer kan det enligt de brottsbekämpande myndigheterna förekomma att det i onödan söks och beviljas tillstånd till hemlig rumsavlyssning, i syfte att det ska bli möjligt att installera kamerautrustningen på den skyddade platsen. Vanligare torde det dock enligt myndigheterna vara att konsekvensen blir att någon kameraövervakning inte kommer till stånd, fastän det egentligen finns ett behov av åtgärden. Bilden bekräftas av de övriga brottsbekämpande myndigheterna. Enligt vad som uppgetts till oss är det vanligt att myndigheterna avstår från att ansöka om tillstånd till hemlig kameraövervakning fastän förutsättningar i övrigt finns eftersom kameran inte kan installeras utan att man får tillåtelse av någon av de misstänkta.

Av regeringens skrivelse Redovisning av användningen av hemliga tvångsmedel under 2020 (skr. 2021/22:79) framgår det att hemlig kameraövervakning är vanligare än hemlig rumsavlyssning. Under 2020 omfattades 212 personer av hemlig kameraövervakning, vilket var en ökning jämfört med 2019 då 128 personer övervakades. Antalet meddelade tillstånd var 211, jämfört med 131 tillstånd under 2019. Uppgifterna kan jämföras med redovisningen för hemlig rumsavlyssning, som visar att 80 personer omfattades av hemlig rumsavlyssning under 2020 och att 135 tillstånd meddelades. Under 2019 omfattades 61 personer och antalet tillstånd uppgick till 89.

Hemlig kameraövervakning förutsätter i många fall att utrustning kan installeras på eller i nära anslutning till den plats som ska övervakas. Av framställningen i det föregående framgår det att det finns ett behov av en möjlighet att få tillträdestillstånd även i fall där det inte ska ske någon hemlig rumsavlyssning. En sådan möjlighet finns enligt bestämmelserna om hemlig dataavläsning. De skäl som anfördes i propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 143–146) och som vi har redovisat i avsnitt 12.3 gör sig i huvudsak gällande även i fråga om hemlig kameraövervakning. Liksom i den propositionen konstaterar vi att en möjlighet till tillträdestillstånd för enbart hemlig kameraövervakning skulle utgöra en utvidgning av möjligheterna till tillträdestillstånd, men att åtgärden på ett principiellt plan – när det gäller själva det tvångsvisa tillträdet – inte innebär något ytterligare intrång än vad som redan är tillåtet vid en husrannsakan.

En husrannsakan kräver endast att det finns anledning att anta att ett brott har begåtts på vilket fängelse kan följa, vilket är ett mycket lägre ställt krav än kravet för hemlig kameraövervakning. Som framhållits i propositionen Hemlig dataavläsning kan ett tillträdestillstånd för ett hemligt tvångsmedel emellertid inte i övrigt jämföras med en husrannsakan eftersom den förra åtgärden görs i hemlighet. Samtidigt är hemlig kameraövervakning, i likhet med hemlig dataavläsning, en metod som ofta fordrar att tekniska hjälpmedel kan installeras. För att tvångsmedlet ska ha önskad effektivitet måste de brottsbekämpande myndigheterna emellanåt kunna få tillträdestillstånd till annars skyddade utrymmen även när det inte är möjligt att få ett samtycke till tillträdet. Det bör i sammanhanget beaktas att tillträdestillstånd avseende hemlig kameraövervakning aldrig kan avse en stadigvarande bostad. Med hänsyn till det stora behovet av åtgärden anser vi att det integritetsintrång som det tvångsvisa tillträdet innebär är godtagbart, även om man inte samtidigt ska installera utrustning för hemlig rumsavlyssning och även om kraven för en hemlig rumsavlyssning inte behöver vara uppfyllda.

Bedömningen att tillträdestillstånd bör kunna ges för enbart en kameraövervakning överensstämmer med den bedömning som har gjorts i fråga om hemlig dataavläsning, som i praktiken kan vara en metod för att verkställa kameraövervakning. De grundläggande förutsättningarna för en hemlig kameraövervakning är i allt väsentligt desamma som för hemlig dataavläsning. Något skäl som talar för att möjligheten att meddela tillträdestillstånd bör vara mer begränsad för hemlig kameraövervakning än för hemlig dataavläsning har inte framkommit. Även systematiska skäl talar därför starkt för att samma sak bör gälla i fråga om tillträdestillstånd för hemlig kameraövervakning som för tillträdestillstånd för hemlig dataavläsning.

Det ingår inte i vårt uppdrag att överväga ändringar i fråga om vilken plats ett tillträdestillstånd ska kunna avse. De begränsningar i fråga om plats som gäller för sådana tillstånd bör alltså gälla även i fortsättningen.

12.5 Det bör vara möjligt för åklagare att fatta interimistiska beslut om tillträde

Förslag: Åklagare ges möjlighet att fatta interimistiska beslut om tillträdestillstånd vid hemlig kameraövervakning, om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd.

Skälen för förslaget

Det är möjligt för åklagare att i brådskande fall fatta ett interimistiskt beslut om hemlig kameraövervakning (27 kap. 21 a § RB). I de fall där tillträdestillstånd krävs för att åtgärden ska kunna verkställas blir möjligheten dock i praktiken meningslös, om åklagaren inte samtidigt kan fatta ett beslut om tillträdestillstånd. Redan den omständigheten talar starkt för att även beslut om tillträdestillstånd ska kunna fattas interimistiskt. En sådan möjlighet finns vid hemlig dataavläsning, och detta även när det tvångsmedlet används som en metod för att verkställa hemlig kameraövervakning (12 § lagen om hemlig dataavläsning). Även detta talar starkt för att åklagare bör ges rätt att interimistiskt besluta om tillträdestillstånd vid hemlig kameraövervakning. Tillträdestillståndet kan knappast ses som mer ingripande i enskildas personliga sfär om det avser hemlig kameraövervakning än om det avser hemlig dataavläsning. Det har inte heller framkommit några andra skäl som talar för att man bör göra en annan bedömning än den som gjorts i fråga om hemlig dataavläsning. Vi gör därför samma bedömning som nyligen gjorts i fråga om hemlig dataavläsning och föreslår således att åklagaren ska kunna fatta interimistiska beslut om tillträdestillstånd vid hemlig kameraövervakning (jfr prop. 2019/20:64 s. 144 och 154).

13 Bör det införas en straffvärdeventil i inhämtningslagen?

13.1 Uppdraget

Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) reglerar de brottsbekämpande myndigheternas möjligheter att i underrättelseverksamhet hämta in uppgifter om elektronisk kommunikation. Tillstånd till sådan inhämtning kan ges antingen för brott för vilket det inte är föreskrivet lindrigare straff än fängelse två år eller för vissa särskilt angivna samhällsfarliga brott. Lagen innehåller inte någon straffvärdeventil.

Frågan om införande av en straffvärdeventil i inhämtningslagen har väckts vid flera tillfällen. Framför allt har Ekobrottsmyndigheten påtalat behovet av införande av en sådan ventil, eftersom myndigheten i princip inte handlägger några brott med ett minimistraff om fängelse i två år, se Slutredovisning av regeringsuppdrag till Tullverket, Polismyndigheten, Ekobrottsmyndigheten och Skatteverket om illegal hantering av punktskattepliktiga varor – Fi 2015/05353/S3 (Ju 2018/02964/Å s. 16). Frågan har även tagits upp i olika utredningar och propositioner. Regeringen har därför bedömt att det finns skäl att se över frågan.

I direktiven anges att man vid ställningstagandet till om en straffvärdeventil ska införas på underrättelsestadiet särskilt måste beakta att en sådan ventil är svårtillämpad eftersom bristen på konkretion av brottsmisstanken i det skedet medför svårigheter att göra den straffvärdebedömning som krävs. Vidare framhålls att man måste ta hänsyn till internationell praxis på området, inklusive den s.k. Tele2-domen (dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15), och de uttalanden som där gjorts i fråga om personkrets och brottets allvar när det gäller i vilka fall som brottsbekäm-

pande myndigheter får ges tillgång till trafikuppgifter. Det framhålls i direktiven att en eventuell utvidgning av tillämpningsområdet för inhämtningslagen måste vara förenlig med internationell praxis.

Vårt uppdrag är därför att

- ta ställning till om en straffvärdeventil bör införas i inhämtningslagen, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Genom lagen (2020:62) om hemlig dataavläsning finns möjlighet att, på samma sätt som följer av inhämtningslagen, hämta in kommunikationsövervakningsuppgifter och platsuppgifter om åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som anges i 2 § inhämtningslagen. Med hänsyn till sambandet mellan bestämmelserna omfattar våra överväganden även hemlig dataavläsning.

13.2 Underrättelseverksamhet

Allmänt

Underrättelseverksamhet är i vid bemärkelse verksamhet som inte utgör förundersökning och som består i att samla, bearbeta och analysera information för att klarlägga om brottslig verksamhet har utövats eller kan komma att utövas. Ett övergripande mål med underrättelseverksamheten kan sägas vara att förse brottsutredande myndigheter med kunskap som kan omsättas i operativ verksamhet. Det framtagna underrättelsematerialet kan då läggas till grund för ett beslut om att inleda en förundersökning. Genom de uppgifter som kommer fram kan brottsmisstankarna bli starka nog för att förundersökning ska inledas, eller så kan det visa sig att misstankarna saknar grund.

I Polismyndighetens handbok för underrättelsetjänst (PM 2021:17) anges bl.a. följande.

Målet med polisiär underrättelsetjänst är att förse Polismyndighetens beslutsfattare med underlag avseende förhållanden som står utanför myndighetens kontroll men som påverkar förmågan att utföra myndighetens uppdrag. Ytterst strävar arbetet mot att ge medborgarna skydd.

Syftet är att möjliggöra för beslutsfattare att kunna fatta proaktiva beslut om brottsbekämpning med hög säkerhet för Polismyndighetens medarbetare och väl underbyggda beslut vid myndighetsutövning. Det brottsbekämpande underrättelsearbetet stödjer rättsprocesser.

Polismyndighetens underrättelsetjänst har i uppdrag att direkt eller i samverkan med andra förebygga, förhindra och upptäcka brottslig verksamhet genom att:

- genomföra undersökningar av brottslig verksamhet, inklusive leda eller bedriva förspaning,
- generera kunskap om nationell och internationell brottslig verksamhet samt brottsaktiva aktörer inklusive deras metoder,
- skapa förutsättningar för underrättelsebaserad brottsbekämpande polisverksamhet mot allvarlig och organiserad brottslighet,
- identifiera och förvarna om hot eller företeelser som påverkar myndighetens förmåga att utföra sitt brottsbekämpande eller ordningshållande uppdrag samt
- bedriva säkerhetsunderrättelsetjänst mot aktörer eller företeelser som utgör ett hot mot Polismyndighetens skyddsintressen.

Utifrån ovanstående ska underrättelsetjänsten producera och tillhandahålla:

- underrättelseprodukter till intressenter inom brottsbekämpande verksamheter inom och utanför myndigheten,
- underrättelseprodukter som underlag för beslut,
- säkerhetsunderrättelseprodukter till intressenter samt
- underrättelseprodukter till intressenter utanför myndigheten utifrån författningar, uppdrag och identifierade behov.

Till Säkerhetspolisens uppgifter hör bl.a. att förebygga, förhindra och upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet eller terrorbrott och att delta i det myndighetsgemensamma arbetet mot den grova och organiserade brottsligheten, 3 och 3 a §§ polislagen (1984:387). Säkerhetspolisen tillämpar i stort sett samma modell som den öppna polisen för att styra underrättelsearbetet.

Även i Tullverket bedrivs underrättelseverksamhet genom insamling, inhämtning, bearbetning och analys av uppgifter. Resultatet av underrättelseverksamhet, de slutsatser eller produkter som tas fram, delges beslutsfattare på olika nivåer och ingår som beslutsunderlag vid beslut om inriktning och prioriteringar av Tullverkets verksamhet.

Underrättelseverksamheten på Ekobrottsmyndighetens område leds av Ekobrottskansliet som organisatoriskt ligger under den nationella operativa avdelningen (Noa) vid Polismyndigheten. I Polismyndighetens uppdrag ingår att bedriva underrättelseverksamhet och att leda sådan verksamhet vid Ekobrottsmyndigheten som endast får utföras av polismän, se 2 § polislagen (1984:387) jämfört med 6 § förordningen (2014:1102) med instruktion för Polismyndigheten. Vidare är Polismyndigheten skyldig att ställa personal till förfogande för den polisverksamhet som bedrivs vid Ekobrottsmyndigheten (47 § instruktionen för Polismyndigheten). Underrättelseverksamheten producerar anmälningar som sedan ska utredas av Ekobrottsmyndighetens kammarverksamhet. Underrättelseverksamheten kan också lämna information till andra aktörer inom området som har möjlighet att agera. Underrättelseverksamheten bedrivs vid de så kallade polisoperativa enheterna i Umeå, Stockholm, Linköping, Göteborg och Malmö men styrs som en nationell resurs.

13.3 Inhämtningslagen

Enligt inhämtningslagen finns möjlighet att inhämta vissa uppgifter om elektronisk information redan på underrättelsestadiet. I 1 § anges att Polismyndigheten, Säkerhetspolisen eller Tullverket i underrättelseverksamhet får hämta in vissa uppgifter i hemlighet från den som enligt lagen (2003:389) om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Inhämtning får ske under de förutsättningar som anges i lagen och avse uppgifter om

1. meddelanden som i ett elektroniskt kommunikationsnät har överförts till eller från ett telefonnummer eller annan adress (historiska meddelanden),
2. vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller

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

Möjligheten att hämta in uppgifter motsvarar vad som gäller enligt 27 kap. 20 § andra stycket RB när hemlig övervakning av elektronisk kommunikation används i syfte att utreda vem som skäligen kan misstänkas för brottet. Således får endast uppgifter om historiska meddelanden hämtas in enligt första punkten. Det bör vidare noteras att lagen endast gör det möjligt att hämta in uppgifter från leverantörer och inte att med egna tekniska hjälpmedel hämta in uppgifter om elektronisk kommunikation.

Enligt 2 § får uppgifter hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott med ett lägsta minimistraff på fängelse i två år. Vidare medges inhämtande av uppgifter om elektronisk kommunikation för vissa särskilt uppräknade samhällsfarliga brott inom Säkerhetspolisens ansvarsområde även om det för dessa inte stadgas ett straffminimum på två år. De särskilt uppräknade brotten fanns tidigare i en tidsbegränsad bestämmelse. Sedan den 1 oktober 2019 är dock bestämmelsen permanent (prop. 2018/19:86). Skälen för åtgärden måste uppväga det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse. Från och med samma datum fattas beslut om inhämtning av uppgifter av åklagare vid Åklagarmyndigheten efter ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket (3 §). Före lagändringen fattades beslut av myndigheterna själva.

Genom rekvisitet ”brottslig verksamhet” framgår att det inte ställs krav på att det ska finnas en misstanke om ett specifikt brott. Det föreligger därmed en principiell skillnad i förhållande till tillämpningsområdet för straffprocessuella tvångsmedel enligt RB. Uppgifterna får alltså hämtas in om någon del av den brottsliga verksamhet, som t.ex. en viss gruppering antas vara delaktig i, innefattar brott med ett minimistraff om lägst två års fängelse. (Prop. 2011/12:55 s. 121.) Med begreppen ”förebygga, förhindra och upptäcka brottslig verksamhet” avses framför allt att insamla, bearbeta och analysera information för att förhindra eller upptäcka brottslig verksamhet när det ännu inte finns konkreta misstankar om att ett visst brott har begåtts.

Att omständigheterna ska vara sådana att åtgärden ska vara av särskild vikt för att förebygga, förhindra eller upptäcka viss brottslig

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

Det framgår av förarbetena att kravet på konkretion innebär att utrymmet för att inhämta uppgifter för att förebygga brott är begränsat. Ett exempel inom Säkerhetspolisens ansvarsområde på när sådan inhämtning ändå under vissa omständigheter kan vara tillåten är inhämtning i syfte att förebygga terroristbrott. Om det finns uppgifter om att personer som får viss träning eller utbildning utomlands kan komma att begå ett terroristbrott, kan inhämtning i syfte att kartlägga personer som deltar i eller verkar för att sådana tränings- eller utbildningsaktiviteter kommer till stånd bedömas vara av särskild vikt för att förebygga brottslig verksamhet som innefattar ett terroristbrott. Däremot innebär kraven på konkretion bl.a. i fråga om vilken typ av brottslighet som ska förebyggas att det t.ex. inte kan bli fråga om att rutinmässigt inhämta uppgifter i syfte att kartlägga personer enbart på grund av att de är kriminellt belastade eller ingår i en viss grupp eller ett visst nätverk.

Vidare ska proportionalitetsprincipen tillämpas vid ett beslut om inhämtning. Principen brukar i korthet beskrivas på det sättet att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden. Vid inhämtningen ska bl.a. hänsyn tas till om åtgärden innebär intrång i ett rättsligt skyddat intresse, t.ex. meddelarskyddet i tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Innebär inhämtningen ett kringgående av förbudet för massmedier att röja sina källor eller för det allmänna att efterforska vem som är meddelare får inhämtning inte ske. Proportionalitetsprincipen får betydelse också för i vilken omfattning inhämtning ska få ske och vilka villkor som beslutet eventuellt ska förenas med. Den gäller vidare under hela verkställighetsförfarandet och ska alltså, även sedan beslut om inhämtning har fattats, beaktas av myndigheten. Integritetsintrånget under verkställigheten

kan bli så stort att åtgärden att hämta in uppgifter inte längre kan anses tillåten, trots att rekvisiten fortfarande är uppfyllda.

I ett beslut om inhämtning av uppgifter ska det enligt 5 § anges vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller vilken annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet avser. Tiden får inte bestämmas längre än nödvändigt och får, när det gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.

Om det inte längre finns skäl för ett beslut om inhämtning av uppgifter ska den ansökande myndigheten omedelbart häva beslutet.

Till skillnad från vad som i allmänhet gäller vid användning av hemliga tvångsmedel enligt RB ställs det i inhämtningslagen inget krav på att tvångsmedlet ska rikta sig mot en viss person (prop. 2011/12:55 s. 84). Tvångsmedlet kan alltså i princip rikta sig mot vem som helst, även om de inte kan antas ha någon anknytning till den brottsliga verksamheten (Gunnel Lindberg, Straffprocessuella tvångsmedel – när och hur får de användas? Fjärde upplagen, s. 753). Några begränsningar i fråga om anknytningen till den adress eller kommunikationsutrustningen som tvångsmedlet avser kan av naturliga skäl inte heller ställas.

13.4 Användningen av inhämtningslagen

Av regeringens redovisning av användningen av hemliga tvångsmedel under 2020 (skr. 2021/22:79) framgår följande om tillämpningen av inhämtningslagen.

Åklagare fattade under 2020 på ansökan av Polismyndigheten och Tullverket 551 beslut, varav 15 avslagsbeslut, om inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet under 2020 (694 beslut 2019). Det har alltså skett en minskning i förhållande till tidigare år.

Antalet beslut har under 2020 fördelat sig mellan olika brottstyper på följande sätt (avrundat till hela procent):

- 64 procent grovt narkotikabrott, synnerligen grovt narkotikabrott, grov narkotikasmuggling eller synnerligen grov narkotikasmuggling (76 procent 2019, 72 procent 2018),

- 24 procent grovt vapenbrott eller synnerligen grovt vapenbrott (16 procent 2019, 17 procent 2018),
- 0 procent grovt rån (0 procent 2019, 0 procent 2018),
- 8 procent mord (2 procent 2019, 8 procent 2018), och
- 4 procent andra grova brott, t.ex. allmänfarlig ödeläggelse och människohandel (5 procent 2019, 3 procent 2018).

Nyttan av inhämtningen i underrättelseverksamhet redovisas genom anonymiserade exempel (se vidare i skr. 2021/22:79).

Åklagare har i Säkerhetspolisens ärenden under 2020 fattat 119 beslut med stöd av inhämtningslagen (103 beslut 2019).

13.5 Lagen om hemlig dataavläsning

Enligt 10 § lagen om hemlig dataavläsning får ett tillstånd till hemlig dataavläsning som gäller kommunikationsövervaknings- eller platsuppgifter beviljas om åtgärden är av synnerlig vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott som anges i 2 § inhämtningslagen. Vid sådan hemlig dataavläsning får meddelanden inte hindras att nå fram och ett tillstånd som gäller kommunikationsövervakningsuppgifter får endast avse uppgifter i förfluten tid. En skillnad i förhållande till inhämtningslagen är att det krävs att åtgärden är av synnerlig vikt för det ändamål som är aktuellt i ärendet. Regeringen ansåg det lämpligt att införa detta strängare krav när hemlig dataavläsning ska användas i inhämtningslagsfallen, framför allt med hänsyn till att det kravet föreslogs gälla för hemlig dataavläsning i övrigt (propositionen Hemlig dataavläsning, prop. 2019/20:64 s. 134).

En annan viktig skillnad i förhållande till vad som gäller enligt inhämtningslagen är att beslutet som huvudregel fattas av domstol på ansökan av åklagare (14 §). Motivet till skillnaden är att hemlig dataavläsning, i vart fall vid verkställigheten, har ansetts vara en mer ingripande åtgärd än den inhämtning som kan ske enligt inhämtningslagen (prop. 2019/20:64 s. 148). Åklagare kan fatta ett interimistiskt beslut, om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för möjligheterna att förebygga, förhindra eller

upptäcka den brottsliga verksamheten att inhämta rättens tillstånd (17 §). I sådana fall ska beslutet domstolsprövas i efterhand.

Det har ansetts att det vid hemlig dataavläsning kan uppstå komplicerade avvägningar gällande bl.a. integritet och informationssäkerhet, oavsett åtgärd och uppgiftstyp som ska läsas av eller tas upp. Regeringen ansåg därför att det skulle införas bestämmelser om att offentliga ombud ska förordnas i samtliga fall av hemlig dataavläsning, trots att det i vissa fall avviker från vad som gäller för bakomliggande tvångsmedel (prop. 2019/20:64 s. 148). Även i detta avseende avviker regleringen om hemlig dataavläsning i inhämtningsfallen från vad som gäller enligt inhämtningslagen.

Vid hemlig dataavläsning gäller alltid proportionalitetsprincipen (3 §).

13.6 Användningen av lagen om hemlig dataavläsning i inhämtningsfallen

Såvitt framgår av regeringens redogörelse för användningen av hemliga tvångsmedel 2020 förekom det inte någon hemlig dataavläsning med stöd av 10 § lagen om hemlig dataavläsning under året. Det bör dock anmärkas att Säkerhetspolisen redovisning avser hemlig dataavläsning i stort, varför det av den inte framgår om Säkerhetspolisen använt hemlig dataavläsning i inhämtningsfallet.

13.7 Tidigare överväganden

De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation

Inhämtningslagen infördes i enlighet med förslag i propositionen De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation (prop. 2011/12:55 s. 81). Redan under remissbehandlingen av Polismetodutredningens bakomliggande förslag framförde Ekobrottsmyndigheten, Åklagarmyndigheten och Skatteverket att det borde införas en straffvärdeventil även för underrättelseverksamheten för att inte en stor del av den grova organiserade brottsligheten skulle falla utanför regleringen. Flera andra myndigheter med

brottsbekämpande uppgifter framförde synpunkten att två års straffminimum var ett för högt ställt krav. (Prop. 2011/12:55 s. 82.)

Enligt dåvarande bestämmelse i lagen (2003:389) om elektronisk kommunikation (6 kap. 22 § första stycket 3) hade de brottsbekämpande myndigheterna möjlighet att inhämta andra uppgifter än innehållsuppgifter om elektronisk kommunikation, om misstankarna rörde brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Regeringen resonerade kring möjligheten att ha en lägre straffröskel och anförde följande (s. 85 och 86).

> Även om en sänkt tröskel naturligtvis som flera remissinstanser påpekat skulle ge de brottsbekämpande myndigheterna förbättrade förutsättningar i sin underrättelseverksamhet har det inte framkommit att behovet är så stort att det överväger de nackdelar en sådan utökad inhämtningsmöjlighet skulle innebära från integritetssynpunkt. I stället är det med hänsyn till den breda informations- och kunskapsinsamlingen och det framåtblickande perspektivet i underrättelseverksamheten, som Polismetodutredningen särskilt framhållit, av integritetsskäl lämpligt att som utgångspunkt behålla en lika hög tröskel som tidigare. Det förhållandet att uppgifter i underrättelseskedet om brottslig verksamhet innefattande vissa brott normalt sett har mindre konkretion än uppgifter om specifika brott i en förundersökning talar också för att möjligheten att inhämta uppgifter om elektronisk kommunikation i underrättelseskedet normalt bör vara mer begränsad jämfört med i en förundersökning. Med hänsyn härtill och till att lagen i många fall kommer att tillämpas innan det finns någon anknytning till ett specifikt brott eller en konstaterad brottsmisstanke anser regeringen, till skillnad från bl.a. Åklagarmyndigheten, att det inte är lämpligt att införa en straffvärdeventil. När det finns en misstanke om ett konkret brott kan inhämtning i stället komma att ske inom ramen för en förundersökning innan det finns en skäligen misstänkt person. För sådan inhämtning föreslås en straffvärdeventil.

När det gällde de särskilt samhällsfarliga brotten i brottskatalogen i 3 § anförde regeringen i korthet att säkerhetsunderrättelseverksamheten vid Säkerhetspolisen skiljer sig från den övriga polisverksamheten bl.a. på så sätt att uppdraget främst är inriktat på att förhindra brott och i mindre utsträckning på att utreda brott som redan har begåtts. För att kunna förhindra särskilt samhällsfarlig brottslighet ansågs Säkerhetspolisen därför i vissa fall ha ett särskilt behov av tillgång till övervakningsuppgifter i ett tidigt skede även då den brottsliga verksamheten inte innefattar brott med ett minimistraff om två års fängelse. (S. 86.)

Datalagringsutredningen

I betänkandet Datalagring och integritet (SOU 2015:31 s. 314–316) anges att Ekobrottsmyndigheten hade framfört ett behov av en möjlighet att hämta in uppgifter enligt inhämtningslagen. Ekobrottsmyndigheten anförde att det i myndighetens underrättelseverksamhet finns ett behov av en möjlighet till inhämtning enligt inhämtningslagen, men att det saknas möjligheter till detta då grovt bokföringsbrott och grovt skattebrott inte når upp till strafftröskeln i lagen. Som grund för behovet anförde myndigheten följande.

- Ekonomisk brottslighet har ofta en nära koppling till systemhotande grov och organiserad brottslighet. Personer inom grov och organiserad brottslighet tenderar att i större utsträckning ägna sig åt ekonomisk brottslighet och det finns stora möjligheter att med rätt förutsättningar kunna lagföra dem för ekonomiska brott. En ökad möjlighet att kartlägga dessa personer ökar möjligheten till lagföring av personerna i fråga.
- Såväl grova skatte- och bokföringsbrott som grov oredlighet har relativt höga straffmaximum och betraktas av rättsordningen som allvarlig brottslighet. Brotten begås ofta systematiskt och avser många brottsmisstankar med omfattande skatteundandraganden.
- Ekonomiska brottslingar samarbetar ofta i nätverk. För att identifiera de kontakter som finns inom nätverken är kartläggning via telefonlistor av signifikant betydelse. Att upptäcka kontaktnätverk och kartlägga dess förgreningar genom traditionell spaning är i princip omöjligt. Eftersom personer i dag vanligen sköter sina kontakter via telefon eller epost är det svårt att utan trafikdata, genom traditionell spaning, uppnå tillräckliga skäl för att inleda förundersökning. Underrättelseärendena tenderar då i stället att fokusera isolerat på individer som det redan finns uppgifter om. Det är ofta frågan om mindre centrala aktörer som mot ersättning utför vissa centrala uppgifter. Andra – ofta mer relevanta personer – undgår då upptäckt.
- De personer som Ekobrottsmyndigheten utreder kan vara personer som utför kriminella handlingar eller hjälper andra att utföra sådana handlingar inom ramen för sina ordinarie arbetsuppgifter, t.ex. genom att övervärdera fastigheter, bevilja lån på osäkra grunder,

bistå med ekonomisk rådgivning eller hantera misstänkta penningtransaktioner utan att anmäla misstänkt penningtvätt. Dessa personer fungerar ofta som ”spindeln i nätet”. För att kunna kartlägga deras kontaktnät och därefter besluta om andra åtgärder är elektronisk inhämtning central.

- De grundläggande punkterna för telefonanalysen i ett underrättelseskede bedöms vara geografisk lokalisering, kontaktmönster och identifiering av för myndigheten eventuella okända viktiga aktörer, modus och för att hitta nya vägar.
- En ökad möjlighet till elektronisk inhämtning ger möjlighet att få mer konkretiserade uppgifter om exempelvis faktiska företrädare, rörelsemönster, kontakter, såväl fasta som mer ad hoc-kontakter eller meddelandeinformation om faktiska brott.
- Olika individers roller och inblandning i en verksamhet kan klargöras. Exempelvis kan detta användas i underrättelseärenden avseende punktskattebrott där en kartläggning av vilka som vistats i närheten av ett skatteupplag hade kunnat uppdaga fler misstänkta eller huvudmännen.
- Inhämtning av trafikdata kan också användas i syfte att kunna avskriva personer som inte är intressanta. Exempelvis kan myndigheten ha fått indikatorer via källor om att personer begår ekonomisk brottslighet. Om inte slagningar och inre spaning kan avfärda detta kan elektronisk inhämtning vara enda möjligheten att verifiera eller förkasta sådana uppgifter.
- Ett mål för Ekobrottsmyndigheten, tillsammans med många andra myndigheter, är återvinning av brottsutbyte. Användandet av målvakter, elektroniska valutor eller andra hjälpmedel för att dölja penningtransaktioner samt bolag där vinsterna hanteras utgör ett stort hinder i att skaffa information som möjliggör ett framgångsrikt arbete med återvinning av brottsutbyte. Det är helt enkelt mycket svårt att fysiskt följa pengarnas väg, och elektronisk information kan användas exempelvis till att lokalisera fastigheter/bostäder.

Utredningen ansåg att det utifrån Ekobrottsmyndighetens beskrivning – och utifrån de uppgifter som genom utredningens egen kartläggning hade kommit fram i fråga om hur inhämtningslagen används

och vilken nytta den leder till i den brottsbekämpande verksamheten – inte var svårt att se att en möjlighet att hämta in uppgifter enligt inhämtningslagen skulle kunna vara till stor nytta även i Ekobrottsmyndighetens verksamhet. Det ingick dock inte i utredningens uppdrag att överväga den typen av förändringar i lagens tillämpningsområde. Utredningen ansåg dock att det kunde finnas anledning att överväga den frågan i ett annat sammanhang.

Betänkandet behandlades i propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten (prop. 2018/19:86). Det anges där (s. 91) att några remissinstanser, bl.a. Ekobrottsmyndigheten, Polismyndigheten och Tullverket, ansåg att inhämtningslagens tillämpningsområde är för begränsat och att delar av den grova organiserade brottsligheten faller utanför. Myndigheterna hade i sina remissyttranden föreslagit att en straffvärdeventil införs för att även t.ex. grov stöld, grovt häleri, grovt bokföringsbrott och narkotikasmuggling av normalgraden ska omfattas. Regeringen angav att en möjlighet att hämta in uppgifter enligt inhämtningslagen säkert skulle kunna vara till nytta i myndigheternas verksamhet, men att frågan kräver noggranna överväganden och att det saknades beredningsunderlag för förslaget.

Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden

Utredningen om organiserad och systematisk ekonomisk brottslighet mot välfärden gjorde i betänkandet Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra (SOU 2017:37 s. 418–421) bedömningen att det finns skäl att se över de brottsbekämpande myndigheternas förutsättningar att inhämta information i underrättelseverksamhet vid vissa typer av allvarlig brottslighet mot välfärdssystemen.

Det hade förts fram till utredningen att inhämtningslagen varit ett viktigt verktyg för de brottsbekämpande myndigheternas underrättelseverksamhet i den fördjupade bearbetningen av information om annan brottslighet. Informationen angavs bl.a. kunna fylla eventuella kunskapsluckor eller verifiera befintlig information eller motstridiga uppgifter. Genom information som inhämtas genom inhämtningslagen skapas enligt utredningen ett bättre underlag för olika beslut än vad som annars är möjligt. Detta innebär vidare att under-

lagen kan bli mycket mer precisa, vilket också sannolikt leder till att man på ett mer säkert sätt kan avfärda viss information och vissa misstankar. Enligt uppgift till utredningen var de förundersökningar som startats efter att inhämtningslagen använts i underrättelsestadiet överlag mer väl underbyggda. Det hade även förts fram att den kunskap som inhämtas på detta sätt ger förutsättningar för att identifiera den del av den organiserade brottsligheten som rymmer s.k. specialister och möjliggörare bl.a. inom den ekonomiska brottsligheten. Sådana aktörer får man sällan kunskap om vid annan informationsinhämtning i underrättelsestadiet.

När det gäller allvarliga brott som riktas mot välfärdssystemen hade det lyfts fram till utredningen att uppgifter om elektronisk kommunikation bör kunna inhämtas också när det gäller mer avancerade upplägg. Uppgifter om elektronisk kommunikation angavs då kunna vara avgörande för att man ska nå upp till en sådan nivå i fråga om misstankarna att förundersökning kan inledas.

Av den information om den kvalificerade välfärdsbrottsligheten som framkommit i utredningens kartläggning kunde utredningen konstatera att en del av den brottslighet som riktas mot välfärdssystemen är såväl allvarlig och omfattande som avancerad. Brottsligheten i sig beskrevs också som särskilt svårupptäckt varför förutsättningarna att upptäcka den här typen av brottslighet angavs ställa särskilda krav på effektiva verktyg i underrättelseverksamheten. Inte minst gäller det enligt utredningen när det är många personer och företag inblandade i brottsupplägg.

Då syftet med inhämtningslagen är att komma åt grov och organiserad brottslighet och det enligt utredningens mening även riktas sådan brottslighet mot välfärdssystemen, ansåg utredningen att det borde ges möjligheter att tillämpa inhämtningslagen även för grova bidragsbrott när det finns skäl för det. Utredningen anförde att detta naturligtvis måste omgärdas med rättssäkerhetsgarantier och endast få ske när intresset av att beivra ett allvarligt brott uppväger det integritetsintrång som en sådan inhämtning innebär.

Utredningen anförde vidare följande.

> De typer av ageranden som kan föranleda ansvar för grovt bidragsbrott uppvisar stora olikheter. Det kan, som framgår av de rättsfall som återfinns i kartläggningen, vara fråga om allt från att gärningsmannen använt falska dokument till mycket avancerade brottsupplägg som är organiserade och systematiska.

> Med den utformning som inhämtningslagen har i dag faller såväl grova bedrägerier som grova bidragsbrott utanför dess tillämpningsområde på grund av brottens breda straffskala. Vissa av dessa brott är dock precis lika allvarliga och avancerade som annan brottslighet för vilken inhämtningslagen kan tillämpas. En sådan ordning är enligt vår mening inte tillfredsställande, varför förutsättningarna för att inhämta information om elektronisk kommunikation bör ses över.

Med hänsyn till det då färska avgörandet i den s.k. Tele2-domen och att regeringen tillsatt Utredningen om datalagring och EU-rätten avstod man från att närmare gå in på frågan om utformningen av inhämtningslagen. Dock menade man att det var av stor vikt att man i särskild ordning särskilt ser över förutsättningarna för att inhämta uppgifter om elektronisk kommunikation i underrättelseverksamhet även vid sådana brott vars straffminimum i dag inte medger en tillämpning av lagen, men trots det kan vara lika allvarliga, omfattande och avancerade som brott för vilka lagen kan tillämpas.

Några överväganden om utvidgning av möjligheterna att tillämpa inhämtningslagen finns inte i utredningens delbetänkande Datalagring – brottsbekämpning och integritet (SOU 2017:75).

Propositionen Vissa kontrollfrågor och andra frågor på punktskatteområdet

I propositionen Vissa kontrollfrågor och andra frågor på punktskatteområdet (prop. 2017/18:294 s. 70) tog regeringen ställning till de förslag som lagts fram i Slutredovisning av regeringsuppdrag till Tullverket, Polismyndigheten, Ekobrottsmyndigheten och Skatteverket om illegal hantering av punktskattepliktiga varor – Fi 2015/05353/S3 (Ju 2018/02964/Å s. 16), se avsnitt 13.1. När det gällde förslaget om ändringar i inhämtningslagen uttalade regeringen att en utökad möjlighet att hämta in uppgifter med stöd av lagen kunna vara till nytta i myndigheternas brottsbekämpande verksamhet. Man konstaterade dock vidare att frågor om hur intresset av en effektiv brottsbekämpning bör balanseras mot integritetsintresset kräver noggranna överväganden som tar hänsyn till hela systemet med hemliga tvångsmedel. Det angavs som regeringens avsikt att framöver närmare analysera om det finns förutsättningar att gå vidare med förslaget i denna del.

Propositionen Hemlig dataavläsning

I sitt remissyttrande över betänkandet Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89) anförde Ekobrottsmyndigheten att hemlig dataavläsning inte skulle kunna användas i myndighetens underrättelseverksamhet och påtalade därför vikten av att det införs en straffvärdeventil i inhämtningslagen för att det ska bli möjligt. I propositionen Hemlig dataavläsning (prop. 2019/20:64 s. 134) anfördes att regeringen inte ifrågasätter att en straffvärdeventil i inhämtningslagen skulle kunna effektivisera myndighetens arbete i vissa underrättelsefall. Det finns dock enligt regeringen en svårighet med en straffvärdeventil i underrättelseverksamhet eftersom det är svårt att bedöma straffvärdet av den brottsliga verksamheten i ett så tidigt skede. Det ansågs i vart fall vara en fråga som behövde ses över i ett större sammanhang och som inte kunde hanteras inom ramen för det aktuella lagstiftningsarbetet.

Riksrevisionens rapport Ekobrottsmyndigheten – arbetet mot den organiserade ekonomiska brottsligheten

Riksrevisionen har nyligen granskat Ekobrottsmyndighetens arbete mot organiserad ekonomisk brottslighet. Resultatet av granskningen redovisas i rapporten Ekobrottsmyndigheten – arbetet mot den organiserade ekonomiska brottsligheten (RiR 2021:30). I rapporten finns uttalanden om Ekobrottsmyndighetens underrättelseverksamhet och inhämtningslagen. Riksrevisionen (s. 34 och 35) uppmärksammar att inhämtningslagen inte är och aldrig har varit tillämplig på Ekobrottsmyndighetens underrättelseverksamhet. Man konstaterar att Ekobrottsmyndigheten uppmärksammade detta redan i redovisningen av 2015 års myndighetsuppdrag (se ovan) att även intervjupersoner inom underrättelseverksamheten framfört till Riksrevisionen att den omständigheten att inhämtningslagen inte är tillämplig begränsar verksamhetens tillgång till information.

> Ekobrottskansliet vid EBM menar att konsekvenserna av att underrättelseverksamheten inte kan tillämpa inhämtningslagen är att de inte kan använda sig av information som lagen ger tillgång till: positionering och trafikdata. Dessa båda informationselement kan spela stor roll för möjligheten att både kartlägga och uppdaga/avslöja brott. Ekobrottskansliet menar vidare att avsaknaden av de delar som inhämtningslagen ger i kombination med avsaknaden av tillgång till finansiell information,

> en ganska skral verktygslåda för att avslöja ekonomisk brottslighet. Ekobrottskansliet påpekar att en viss del av denna information kan inhämtas i begränsad omfattning, men på ett mer resurskrävande och integritetskränkande sätt. Kommunikationsmönster och trafikdata går däremot inte att kompensera med någon annan inhämtningsmetod.

Riksrevisionen hänvisar vidare till denna utredning och vårt uppdrag att överväga om det bör införas en straffvärdeventil i inhämtningslagen. Det anges vidare att Ekobrottsmyndigheten under beredningen av våra direktiv hade framhållit att det även finns skäl att se över den nuvarande brottskatalogen och överväga om denna bör utvidgas till att omfatta fler brott än i dag. Ekobrottsmyndigheten hade enligt rapporten angivit att det saknas möjlighet för de brottsbekämpande myndigheterna att inhämta relevanta uppgifter för att exempelvis utreda grova skattebrott eftersom detta brott inte omfattas av brottskatalogen.

Riksrevisionen (s. 47) gör bl.a. bedömningen att regeringen inte gett Ekobrottsmyndigheten vissa yttre förutsättningar för att fullt ut kunna arbeta effektivt. Som ett exempel nämns att underrättelseverksamheten saknar vissa rättsliga förutsättningar för att kunna arbeta effektivt med att upptäcka och förhindra den organiserade ekonomiska brottsligheten. En av dessa är enligt rapporten en möjlighet att tillämpa inhämtningslagen (s. 51). En av Riksrevisionens rekommendationer till regeringen är att regeringen bör säkerställa att Ekobrottsmyndigheten får förutsättningar för att bedriva ett effektivt arbete mot den organiserade ekonomiska brottsligheten, bl.a. genom att se till att underrättelseverksamheten har rättsliga förutsättningar för att upptäcka och förhindra ekonomisk brottslighet (s. 53).

13.8 En straffvärdeventil bör inte införas

Bedömning: Det bör inte införas en straffvärdeventil i inhämtningslagen.

Skälen för bedömningen

Som framgår av våra direktiv och framställningen i avsnitt 13.7 har frågan om ett bredare tillämpningsområde för inhämtningslagen väckts vid flera tillfällen. Det har i olika sammanhang framförts önskemål

om att t.ex. grov stöld, grovt häleri, grovt bokföringsbrott och narkotikasmuggling av normalgraden ska omfattas (se bl.a. propositionen Datalagring vid brottsbekämpning – anpassningar till EU-rätten, prop. 2018/19:86 s. 91). Det handlar främst om brott med en bred straffskala, där straffminimum är relativt lågt men där maximistraffet är högt. Även om också andra myndigheter har anfört att det finns ett behov av ett bredare tillämpningsområde (se avsnitt 13.3) har frågan särskilt drivits av Ekobrottsmyndigheten, som inte utreder något brott med lägst två års minimistraff. Inhämtningslagen är därför aldrig tillämplig i Ekobrottsmyndighetens underrättelseverksamhet. Myndigheten har under lång tid anfört att detta hämmar dess underrättelseverksamhet. En redogörelse för svårigheterna finns i betänkandet Datalagring och integritet (SOU 2015:31 s. 314–316), som vi i relevanta delar har redogjort för i avsnitt 13.7. Nyligen har Riksrevisionen (RiR 2021:30) gjort bedömningen att Ekobrottsmyndigheten saknar vissa yttre förutsättningar för att kunna arbeta effektivt med att upptäcka och förhindra den organiserade ekonomiska brottsligheten. En av dessa är enligt Riksrevisionen en möjlighet att tillämpa inhämtningslagen (RiR 2021:30 s. 51).

Tullverket har till utredningen framfört att det i även Tullverkets underrättelseverksamhet finns ett behov av en möjlighet att använda inhämtningslagen i fråga om grova brott avseende punktskatter och grovt tullbrott. Polismyndigheten har framfört att det finns ett behov av en möjlighet att använda inhämtningslagen när det gäller främst organiserade tillgrepp och bedrägerier.

Vårt uppdrag är enbart att ta ställning till om en straffvärdeventil bör införas i inhämtningslagen. Vi anser att det hade varit fördelaktigt att ta ett bredare grepp om frågan och låta en utredning överväga om inhämtningslagens tillämpningsområde bör utvidgas och i så fall hur en sådan utvidgning bör ske. En av de frågor som hade behövt lösas är vem som ska fatta beslut i ekobrottsärenden. Beslut enligt inhämtningslagen fattas i dag av åklagare vid Åklagarmyndigheten på begäran av Polismyndigheten, Säkerhetspolisen eller Tullverket. Någon rätt till domstolsprövning finns inte och offentliga ombud deltar inte vid handläggningen. Förfarandet har således inget inslag av kontradiktion, det finns ingen rätt att överklaga, och inte heller någon som kan överklaga beslutet. Samtidigt har åklagare vid Åklagarmyndigheten i allmänhet begränsade kunskaper om den lagstiftning som hör till Ekobrottsmyndighetens ansvarsområde. Det kan tala för att Eko-

brottsmyndighetens åklagare ges befogenhet att fatta beslut. Med tanke på hur underrättelseverksamheten på ekobrottsområdet är organiserad behöver det i så fall övervägas om en beslutsbefogenhet för Ekobrottsmyndighetens åklagare hade varit förenlig med kraven på att beslut om hemliga tvångsmedel fattas av en oberoende myndighet (jfr bl.a. EU-domstolens dom [stora avdelningen] den 2 mars 2021 i mål C-746/18). Det ingår inte i vårt uppdrag att överväga beslutsordningen.

Vidare är det inte givet att en straffvärdeventil är den enda tänkbara möjligheten för att åstadkomma ett utökat tillämpningsområde, om man kommer fram till att en utökning bör ske. Vi har visserligen möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska utredas men endast under förutsättning att uppdraget ändå kan redovisas i tid. Vi bedömer att detta inte är möjligt. Våra överväganden gäller därför enbart frågan om en straffvärdeventil.

I direktiven anges att det särskilt måste beaktas att en straffvärdeventil är svårtillämpad i underrättelseskedet eftersom bristen på konkretion av brottsmisstanken i det skedet medför svårigheter att göra den straffvärdebedömning som ska ske. Det är inte meningsfullt att undersöka behovet och nyttan av en utvidgning om det inte är en framkomlig väg. Vi börjar därför med den frågan.

Typiskt för situationen där beslut om inhämtning fattas är att det ofta inte finns en misstanke om ett konkret brott. Beslutet avser inte heller ett visst brott utan en viss brottslighet, som innefattar brott som antingen har lägst två års minimistraff eller räknas upp bland de samhällsfarliga brotten i brottskatalogen. Redan det att man på ett mycket tidigt skede är tvungen att sätta en rubrik på de brott som den brottsliga verksamheten innefattar måste anses innebära en viss osäkerhet i fråga om när inhämtning får ske jämfört med en förundersökning där tvångsmedlen avser en konkret brottsmisstanke. Det framstår inte som rimligt att det därutöver ska kunna göras en tillförlitlig bedömning av straffvärdet av den ingående brottsligheten, som det i det aktuella skedet alltså inte ens finns underlag att inleda en förundersökning om. Redan detta inger mycket starka betänkligheter i fråga om lämpligheten av en straffvärdeventil på underrättelsestadiet. Utifrån den behovsbeskrivning som gjorts kan det vidare diskuteras hur stort tillämpningsområdet i praktiken skulle bli på ekobrottsområdet för en straffvärdeventil som enbart avser enstaka brott och som inte gör det möjligt att lägga samman flera brott och utgå från

det samlade straffvärdet. Mycket talar för att man, för att säkerställa att straffvärdeventilen skulle bli effektiv, skulle bli tvungen att även införa en motsvarighet till den straffvärdeventil för viss flerfaldig brottslighet som vi föreslår i kapitel 6. Redan det anförda leder till bedömningen att det inte är lämpligt att införa en straffvärdeventil i inhämtningslagen. Vi lämnar därför inte något sådant förslag.

14 Skyddet för den personliga integriteten

14.1 Uppdraget

En del av vårt uppdrag är att noga väga behovet av en effektiv brottsbekämpning mot den enskildes rätt till skydd för sin personliga integritet. En sådan avvägning ska göras för varje förslag för sig och även när det gäller förslagen sammantaget. Vi ska även ta ställning till om skyddet för den personliga integriteten bör stärkas och i så fall lämna förslag till de författningsändringar som bedöms nödvändiga. Förslagen ska uppfylla högt ställda krav på rättssäkerhet.

Vi har i kapitel 6–13 redovisat de avvägningar vi gjort mellan behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet för varje förslag. I detta kapitel redovisar vi hur vi ser på förhållandet mellan de sammantagna förslagen och enskildas rätt till personlig integritet och rättssäkerheten. I avsnitt 14.5 överväger vi behovet av ett förstärkt skydd för den personliga integriteten och ytterligare rättssäkerhetsgarantier.

14.2 Personlig integritet

Som framgår i kapitel 3 finns ett grundlagsstadgat skydd för den enskildes privatliv – den personliga integriteten. Det har i flera statliga utredningar gjorts försök att definiera begreppet personlig integritet (se bl.a. betänkandena Skyddet för den personliga integriteten, Del 1, SOU 2007:22, s. 53–62, Integritet och straffskydd, SOU 2016:7 s. 63–75 och Hur står det till med den personliga integriteten?, SOU 2016:41 s. 136–147). Det är svårt att ge en positiv bestämning av den personliga integriteten, dvs. att formulera en beskrivning som pekar ut alla de situationer i vilka individen har rätt att få sin integ-

ritet respekterad och skyddad. Trots svårigheterna är det nödvändigt att veta vad som avses när begreppet används. Integritetskommittén uttryckte detta som att innebörden måste vara tillräckligt tydlig för att det ska vara möjligt att avgöra vad som innebär en kränkning eller ett otillbörligt intrång (SOU 2016:41 s. 148). När det gäller hemliga tvångsmedel uttryckte Utredningen om vissa hemliga tvångsmedel att den personliga integritetens kärnområden, dvs. sådant som rör individen och dennes personlighet, var det relevanta för den analys som utredningen hade att göra. Den personliga integritetens kärnområden omfattar information om den enskilde inklusive identifieringsdata avseende den enskildes bild, namn och liknande. Utredningen konstaterade också att varje befogenhet för staten att bereda sig tillgång till personlig information om den enskilde och varje nyttjande av sådan information leder till ingrepp i den personliga integriteten. Graden av integritetsintrång varierar med tvångsmedlets utformning och tillämpning (SOU 2012:44 s. 480).

14.3 Hemliga tvångsmedel och den personliga integriteten

Olika integritetsintrång

Hemliga tvångsmedel kan aktualisera flera slags integritetsintrång. Lagring eller insamling av personuppgifter utgör i sig ingrepp i den personliga integriteten. Detta gäller även om de brottsbekämpande myndigheterna aldrig tar del av de uppgifter som åtgärden gett och oavsett om uppgifterna kommer till användning (jfr bl.a. EU-domstolens dom den 6 oktober 2020 i de förenade målen C-511/18, C-512/18 OCH C-520/18, La Quadrature du Net m.fl. punkterna 115 och 116 och där hänvisade rättsfall). Även åtgärder i realtid, såsom hemlig avlyssning i realtid av ett visst telefonnummer eller hemlig rumsavlyssning utgör ett ingrepp i den personliga integriteten. Genomgång och analys av materialet samt annan behandling av det utgör ytterligare intrång.

Risken för integritetsintrång

Regeringen har tidigare uttalat att av de tvångsmedel som riktas mot elektronisk kommunikation anses hemlig övervakning av elektronisk kommunikation typiskt sett medföra ett klart mindre integritetsintrång än hemlig avlyssning av elektronisk kommunikation, eftersom det förstnämnda tvångsmedlet inte ger någon information om innehållet i samtal eller meddelanden (se t.ex. prop. 2002/03/74 s. 23 f.). Samtidigt bör det framhållas att tvångsmedlet i vissa fall kan innebära insamling av uppgifter om kommunikations- och rörelsemönster som gör det möjligt att dra precisa slutsatser om den enskildes privatliv.

Hemlig kameraövervakning och hemlig avlyssning av elektronisk kommunikation har ansetts kunna medföra integritetsintrång på i stort sett likvärdiga nivåer (t.ex. prop. 1995/96:85 s. 22).

Hemlig rumsavlyssning har från integritetssynpunkt ansetts vara en mer ingripande åtgärd än hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. I propositionen Hemliga tvångsmedel (prop. 2013/14:237 s. 70) ansåg regeringen att det anförda typiskt gäller, men betonade samtidigt att det alltid beror på omständigheterna i det enskilda fallet vilket hemligt tvångsmedel som har mest kännbara effekter. Som exempel angavs att en hemlig rumsavlysning av ett möte på en restaurang kan vara avsevärt lindrigare från integritetssynpunkt än avlyssning av en bostadstelefon som pågår under en längre tid. Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel ifrågasatte för sin del om det är självklart att integritetsintrånget är större vid hemlig rumsavlyssning än vid exempelvis hemlig avlyssning av elektronisk kommunikation (SOU 2018:61 s. 179). Utredningen framhöll att hemliga tvångsmedel som rör elektronisk kommunikation kan leda till en kartläggning av vardagsvanor, kontaktnät och vanliga resmål och att den brottsbekämpande myndigheten kan få del av vilka webbsidor en person har besökt, vad som står i e-postmeddelanden, sms och andra meddelanden samt vad som sägs i telefon- och videosamtal, oavsett var personen befinner sig. Hemlig rumsavlyssning är däremot begränsad till ljud på en avgränsad plats och tillståndet innehåller ofta särskilda villkor till skydd för integriteten, i synnerhet när utomstående personer kan befaras bli föremål för avlyssningen.

Särskilt om hemlig dataavläsning

Genom en hemlig dataavläsning kan man få tillgång till kommunikationsövervakningsuppgifter och platsuppgifter. Kommunikationsövervakningsuppgifter motsvarar de uppgifter som man kan få tillgång till genom en hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § första stycket 1 RB. Platsuppgifter är samma sorts uppgifter som kan erhållas genom en hemlig övervakning av elektronisk kommunikation enligt 27 kap. 19 § första stycket 3. Man kan dock genom en hemlig dataavläsning få tillgång till mer detaljerade uppgifter om geografisk position än vid en hemlig övervakning av elektronisk kommunikation. Detta ansåg regeringen innebära att hemlig dataavläsning för att ta del av uppgifter om geografisk position medför en viss ökad risk för den personliga integriteten jämfört med då gällande ordning (prop. 2019/20:64 s. 86.) Kraven avseende brottets allvar för att kunna hämta in dessa uppgiftstyper är högre vid en hemlig dataavläsning än vid hemlig övervakning av elektronisk kommunikation och motsvarar de krav som gäller för en hemlig avlyssning av elektronisk kommunikation (prop. s. 93 och 94).

Hemlig dataavläsning för att läsa av innehållet i meddelanden (kommunikationsavlyssningsuppgifter, 2 § första stycket 1) ansågs inte innebära någon beaktansvärd ökad risk för den personliga integriteten (prop. 2019/20:64 s. 85). Kraven avseende brottets allvar för att man ska få vidta åtgärden överensstämmer med kraven för hemlig avlyssning av elektronisk kommunikation (prop. s. 93 och 94).

Hemlig dataavläsning kan vidare ge tillgång till samma uppgifter som kan samlas in med hemlig kameraövervakning eller hemlig rumsavlyssning, t.ex. genom att en mobiltelefons kamera eller mikrofon aktiveras och att uppgifterna därefter läses av (kameraövervakningsuppgifter respektive rumsavlyssningsuppgifter). Regeringen ansåg att åtgärden, med de begränsningar som gäller för hemlig kameraövervakning eller hemlig rumsavlyssning, inte skulle medföra någon ökad risk för den personliga integriteten eftersom uppgifter som kan läsas av med hemlig dataavläsning skulle motsvaras av dem som får hämtas in i dag. Samtidigt anfördes att bedömningen dock skulle bli annorlunda om motsvarande begränsningar avseende plats som gäller för hemlig kameraövervakning och hemlig rumsavlyssning inte skulle gälla för hemlig dataavläsning. Regeringen framhöll att hemlig dataavläsning kan användas för att t.ex. aktivera en mikrofonfunktion i

en mobiltelefon och göra det möjligt att höra varje ord på alla de platser som den misstänkte befinner sig. Detta ansågs innebära risker för den personliga integriteten för såväl den som utsätts för åtgärden som för andra som befinner sig i närheten. Samma risker ansågs gälla vid aktivering av en kamera i t.ex. en mobiltelefon. (Prop. 2019/20:64 s. 86, 95 och 96.) Bestämmelserna begränsades därför på samma sätt som hemlig kameraövervakning och hemlig rumsavlyssning när det gäller krav på plats. Med denna begränsning ansåg regeringen att hemlig dataavläsning för att ta del av kameraövervakningsuppgifter och rumsavlyssningsuppgifter inte skulle innebära någon beaktansvärd ökad risk för den personliga integriteten. Kraven i fråga om brottets allvar sattes på samma nivå som för hemlig kameraövervakning respektive hemlig rumsavlyssning.

Slutligen infördes det genom hemlig dataavläsning en möjlighet att ta del av dels uppgifter som finns lagrade i ett avläsningsbart informationssystem, dels uppgifter som visar hur ett informationssystem används (2 § första stycket 6 och 7). Exempel på lagrade uppgifter kan vara fotografier och textfiler som har lagrats men inte skickats till någon, eller utkast till meddelanden. Regeringen uttalade följande (prop. 2019/20:64 s. 87).

> Å ena sidan är det uppenbart att en fullständig avläsning av t.ex. någons mobiltelefon utgör ett mycket stort intrång i den drabbades personliga sfär då en mobiltelefon eller annan liknande utrustning kan innehålla mycket känsliga och personliga uppgifter. Å andra sidan måste beaktas att risken för ett sådant intrång finns redan i dag vid beslag av en mobiltelefon under en förundersökning. Denna risk finns dock enbart under en förundersökning då det enligt dagens regler inte är möjligt att beslagta en mobiltelefon i underrättelseverksamhet. Det går således redan i vissa situationer att få tag på uppgifterna i fråga, men vid ett senare skede än vad som kan bli fallet med hemlig dataavläsning. Det kan hävdas att integritetsintrånget vid genomsökning av en teknisk utrustning efter ett beslag är högre än om åtgärden vidtas utan att den tekniska utrustningen fråntas den som åtgärden gäller, även om integritetsintrånget av att vid ett visst givet tillfälle inte få disponera elektronisk utrustning generellt sett får sägas vara begränsat. Samtidigt ökar integritetsintrånget genom att åtgärden vidtas i hemlighet.

Vid en samlad bedömning ansåg regeringen att insamling av elektroniskt lagrade uppgifter innebär en ökad risk för den personliga integriteten jämfört med förhållandena vid tidpunkten.

Uppgifter om användning kan vara t.ex. uppgifter om vilka appar eller program som har använts, vilka inloggningsuppgifter som an-

getts eller webbsidor som har besökts. Regeringen ansåg att sådana uppgifter typiskt sett är integritetskänsliga (prop. 2019/20:64 s. 87). Det konstaterades att sådana uppgifter ibland finns lagrade eller i vart fall är möjliga att återskapa vid t.ex. en undersökning av ett beslag. I och med att hemlig dataavläsning utförs i hemlighet och ger tillgång till fler och mer fullständiga uppgifter ansågs åtgärden, i synnerhet om den genomförs utanför en förundersökning, innebära en ökad risk för den personliga integriteten jämfört med då rådande förhållanden.[1]

För att uppgifter om lagrat innehåll eller användning ska få hämtas in gäller samma villkor i fråga om bl.a. brottets allvar som för hemlig avlyssning av elektronisk kommunikation respektive hemlig kameraövervakning.

14.4 Tidigare översyner

14.4.1 Utredningen om rättssäkerhet vid hemliga tvångsmedel

Utredningen om rättssäkerhet vid hemliga tvångsmedel överlämnade betänkandet Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m. (SOU 2006:98) i november 2006.

Utredningens uppdrag bestod i att överväga ytterligare garantier för enskildas rättssäkerhet vid användning av hemliga tvångsmedel i brottsbekämpande verksamhet. Uppdraget bestod bl.a. i att utforma en skyldighet att underrätta brottsmisstänkta personer och andra enskilda som har avlyssnats eller övervakats med hemliga tvångsmedel. Vidare ingick det i uppdraget att undersöka om det behövdes förbättringar av systemet med offentliga ombud.

Utredningen föreslog att det skulle införas en särskild skyldighet att underrätta enskilda personer som påtagligt har berörts av sådan verkställighet av hemliga tvångsmedel som sker i brottsutredningar.

Vidare föreslog utredningen att det skulle inrättas ett oberoende organ, Säkerhets- och integritetsskyddsnämnden (SIN), med uppgift att löpande granska användningen av hemliga tvångsmedel. Om underrättelse inte kunde lämnas till den enskilde, på grund av sekretess, skulle i stället det oberoende organet underrättas. Det föreslogs även att varje person skulle ha rätt att begära att det oberoende organet

[1] Med undantag för frågorna i kapitel 13 omfattar våra överväganden endast hemlig dataavläsning under en förundersökning.

kontrollerar om han eller hon har varit föremål för ett hemligt tvångsmedel i strid med gällande författningar. Utöver dessa uppgifter skulle nämnden utföra löpande tillsyn genom inspektioner och andra undersökningar.

Slutligen bedömde utredningen att systemet med offentliga ombud fungerade väl och föreslog inga förändringar i den delen.

Bestämmelser om underrättelseskyldighet och om inrättande av Säkerhets- och integritetsskyddsnämnden trädde i kraft den 1 januari 2008 (prop. 2006/07:133, bet. 2007/08:JuU3, rskr. 2007/08:11).

14.4.2 Utredningen om utvärdering av vissa hemliga tvångsmedel

Utredningen om utvärdering av vissa hemliga tvångsmedel överlämnade betänkandet Utvärdering av buggning och preventiva tvångsmedel (SOU 2009:70) i juli 2009.

Utredningens uppdrag bestod i att utvärdera bl.a. hur den då tidsbegränsade lagen (2007:978) om hemlig rumsavlyssning hade tillämpats. Ett av syftena med utvärderingen var att analysera om kontrollmekanismerna och övriga rättssäkerhetsgarantier var tillräckliga. I utvärderingen ingick även att belysa vilken inverkan som tvångsmedelsanvändningen hade haft på den personliga integriteten.

Utredningen bedömde att de rättssäkerhetsgarantier och kontrollmekanismer som lagen om hemlig rumsavlyssning hade kringgärdats av var omfattande och att den sammanlagda effekten av regelverket utgjorde ett tillräckligt gott skydd mot otillbörliga integritetsintrång. Tvångsmedelsanvändningens inverkan på den personliga integriteten var enligt utredningen svårbedömd när det gällde hemlig rumsavlyssning. Intrånget bedömdes visserligen som högre än för andra hemliga tvångsmedel men avlyssningen användes endast i ett mycket begränsat antal fall, vilket betydde att ökningen av intrånget i den personliga integriteten bedömdes som liten i förhållande till om tvångsmedlet inte hade varit tillåtet.

14.4.3 Utredningen om vissa hemliga tvångsmedel

Utredningen om vissa hemliga tvångsmedel överlämnade i juni 2012 betänkandet Hemliga tvångsmedel mot allvarliga brott (SOU 2012:44). Utredningens huvudsakliga uppdrag var att utvärdera hur de tids-

begränsade lagarna lagen om hemlig rumsavlyssning, preventivlagen och lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott (utredningslagen) hade tillämpats, samt analysera om regleringen av hemliga tvångsmedel för särskilt allvarlig eller annars samhällsfarlig brottslighet borde förändras i något eller några avseenden. Syftet med uppdraget var också att ta slutlig ställning till lagarnas fortsatta giltighet och därmed till hur en framtida permanent reglering av hemliga tvångsmedel för särskilt allvarlig eller annars samhällsfarlig brottslighet borde utformas. Utredningens uppgifter var omfattande och en del av uppdraget avsåg rättssäkerhetsgarantier. I den delen skulle utredningen, med utgångspunkt från kartläggningen av hur de tre lagarna hade tillämpats, analysera regleringen om offentliga ombud, underrättelseskyldighet, domstolsprövning och om SIN:s efterhandskontroll i förhållande till Europakonventionens krav. Utredningen skulle också analysera om det av rättssäkerhetsskäl behövdes förändringar av de rättssäkerhetsgarantier som omgärdar tvångsmedelsanvändningen enligt de tre lagarna.

Utredningen konstaterade att användningen av tvångsmedel enligt de undersökta lagarna var begränsad och att besluten om tvångsmedel inte hade riktats mot ett stort antal personer. Däremot hade en hel del personlig information samlats in i de enskilda fallen. Tvångsmedlen bedömdes därför ha medfört icke obetydliga integritetsintrång. En del av den insamlade informationen hade rört tredje man och viss information hade inte haft betydelse för att utreda eller förhindra brott. Det bedömdes inte föreligga någon beaktansvärd skillnad när hemlig teleavlyssning och hemlig teleövervakning använts enligt de tidsbegränsade lagarna jämfört med när de använts med stöd av rättegångsbalken. Hemlig rumsavlyssning bedömdes ha utgjort ett större integritetsintrång än övriga tvångsmedel även om såväl domstolarna som de brottsbekämpande myndigheterna sökt begränsa mängden kringinformation och därmed också integritetsintrånget.

Utredningen bedömde att den svenska regleringen av de kartlagda hemliga tvångsmedlen och deras rättssäkerhetsgarantier levde upp till regeringsformens och Europakonventionens krav. Domstolsprövningen fungerade enligt utredningen på ett tillfredsställande sätt och det föreslogs att interimistiska tillståndsbeslut av åklagaren skulle tillåtas för samtliga hemliga tvångsmedel. Vidare konstaterade utredningen att begränsningarna kring överskottsinformation skiljde sig mellan lagarna och föreslog att rättegångsbalkens regler skulle gälla

för samtliga de aktuella tvångsmedlen. Gällande avlyssningsförbudet ansåg utredningen att det strängare förbud som fanns i preventivlagen skulle gälla även för avlyssning inom en förundersökning. Enligt utredningen borde det inte införas bestämmelser om att offentliga ombud ska medverka i ärenden om hemlig övervakning av elektronisk kommunikation. Det fanns inte heller behov av att i övrigt göra några förändringar i systemet med offentliga ombud. Utredningen föreslog att bestämmelserna i de tre tidsbegränsade lagarna skulle permanentas på så sätt att bestämmelserna i utredningslagen och lagen om hemlig rumsavlyssning infördes i 27 kap. RB och att preventivlagen skulle fortsätta gälla utan tidsbegränsning.

De tidsbegränsade lagarna om hemliga tvångsmedel gjordes permanenta den 1 januari 2015 med vissa justeringar (prop. 2013/14:237, bet. 2014/15:JuU2, rskr. 2014/15:22). Samtidigt utvidgades förbudet mot att avlyssna vissa samtal och möjligheten för domstolen att fatta beslut om hemliga tvångsmedel utan att ett offentligt ombud medverkat togs bort. Något krav på medverkan av ett offentligt ombud i ärenden om hemlig övervakning av elektronisk kommunikation infördes inte.

14.4.4 Utredningen om datalagring och EU-rätten

I oktober 2017 överlämnade Utredningen om datalagring och EU-rätten delbetänkandet Datalagring – brottsbekämpning och integritet (SOU 2017:75). Uppdraget var att göra en översyn av reglerna om lagring av uppgifter om elektronisk kommunikation med anledning av EU-domstolens Tele2-dom. Utredningen skulle bl.a. se över bestämmelserna om tillgång till lagrade uppgifter. Utredningen analyserade därför reglerna om hemlig övervakning av elektronisk kommunikation vid förundersökning, i preventivt syfte och för särskild utlänningskontroll samt bestämmelserna om inhämtning enligt inhämtningslagen. Analysen gjordes främst i förhållande till EU-domstolens dom men även regeringsformens och Europakonventionens krav beaktades.

Utredningen konstaterade att EU-rätten kräver att tillgång till lagrade trafik- och lokaliseringsuppgifter bara kan ges efter förhandskontroll av domstol eller annan oberoende myndighet samt endast för bekämpning av grov brottslighet. Därtill måste uppgifterna som

huvudregel avse personer som på något sätt är inblandade i grov brottslighet. Vidare konstaterade utredningen att de personer som utsatts för tvångsmedlet måste informeras så snart det inte längre skadar myndigheternas utredningar.

Utredningen bedömde att de svenska bestämmelserna om tillgång till lagrade uppgifter om elektronisk kommunikation med ett undantag är förenliga med EU-rätten och Sveriges folkrättsliga åtaganden. Undantaget gällde att det saknades förhandsprövning av en oberoende myndighet vid inhämtning enligt inhämtningslagen. Sådana beslut fick fattas av Polismyndigheten, Säkerhetspolisen och Tullverket.

Genom lagändringar som trädde i kraft den 1 oktober 2019 flyttades beslutsbefogenheten vid inhämtning enligt inhämtningslagen över till åklagare (prop. 2018/19:86, bet. 2018/19:JuU27, rskr. 2018/19:296).

14.4.5 Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel

Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel hade i uppdrag att se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när hemliga tvångsmedel för särskilt allvarlig brottslighet används. Arbetet redovisades i slutbetänkandet Rättssäkerhetsgarantier och hemliga tvångsmedel (SOU 2018:61).

Utredningen övervägde om bestämmelserna om vilket slags brottslighet och vilken personkrets som aktuella hemliga tvångsmedel får användas mot uppfyller de krav som regeringsformen och Europakonventionen ställer på precision och förutsebarhet. Utredningen bedömde att så är fallet förutom i det avseendet att hemlig avlyssning av elektronisk kommunikation enligt bestämmelsens ordalydelse kan avse meddelanden mellan personer som varken är misstänkta eller kan ha upplysningar om brott. Utredningen föreslog därför att hemlig avlyssning av elektronisk kommunikation endast får avse meddelanden som den som åtgärden riktas mot deltar i.

Man uppmärksammade vidare att platsen som ska omfattas av hemlig rumsavlyssning anges olika specifikt i tillstånden. Utredningen ansåg att tillståndet som huvudregel måste avse en så tydligt begränsad yta, så att det vid tillståndsprövningen ska vara möjligt att överblicka risken för onödiga integritetsintrång, och att vida platser bör förenas med särskilda villkor. Det som framkommit föranledde dock inte

utredningen att lämna något förslag på författningsändringar eller andra åtgärder.

När det gäller förhandskontrollen bedömde utredningen att systemet med domstolsprövning och med interimistiska åklagarbeslut fungerar bra och uppfyller kraven i regeringsformen och Europakonventionen. Utredningen ansåg vidare att det behöver införas ett krav på att beslut om till tillstånd till postkontroll innehåller uppgift om vilka försändelser som tillståndet omfattar eftersom det annars ansågs finnas en risk för att besluten blir oprecisa och inte tillräckligt avgränsade. Systemet med offentliga ombud bedömdes fungera bra och utöver andra rättssäkerhetsgarantier bidra till att uppfylla kraven avseende förhandskontroll i regeringsformen och Europakonventionen.

Även avlyssningsförbudet ansågs uppfylla kraven i regeringsformen och Europakonventionen medan bestämmelserna om hur överskottsinformation får användas av olika anledningar inte ansågs vara förenliga med kraven i Europakonventionen. Utredningen menade att bestämmelserna är otydliga och det är oklart om uttryckligt lagstöd finns för all avsedd användning. Därtill bedömde utredningen att vissa av begränsningarna i enskilda fall kan leda till att Sverige inte kan uppfylla Europakonventionens krav på att förhindra och utreda brott som begås mot enskildas privatliv. Utredningen föreslog därför att bestämmelserna om överskottsinformation i rättegångsbalken och preventivlagen förändras. Vidare föreslog man att överskottsinformation ska få användas i större utsträckning för att bekämpa brott samt att överskottsinformation inte ska få användas utan beslut från åklagare.

I rättegångsbalken regleras när upptagningar och uppteckningar ska förstöras. Utformningen av bestämmelsen i rättegångsbalken överensstämmer enligt utredningen inte med hur den tillämpas. En tillämpning enligt ordalydelsen ansågs i det enskilda fallet kunna innebära att en misstänkts rätt till en rättvis rättegång kränks. Man föreslog därför att bestämmelsen ändras, så att den bättre stämmer överens med hur den tillämpas och med rätten till en rättvis rättegång. Förslaget ansågs även leda till en ökad tydlighet i fråga om när material från hemliga tvångsmedel ska bevaras och förstöras.

Bestämmelserna om granskning av materialet från hemliga tvångsmedel ansågs förenliga med kraven i regeringsformen och Europakonventionen. Däremot menade man att det behöver införas en lag-

stadgad skyldighet för brottsbekämpande myndigheter att dokumentera åtgärder hänförliga till hemliga tvångsåtgärder.

Systemet med underrättelser till den som utsatts för ett hemligt tvångsmedel ansågs förenligt med kraven i regeringsformen och Europakonventionen.

Systemet med tillsyn av bl.a. SIN, Justitiekanslern och Riksdagens ombudsmän (Justitieombudsmannen) samt genom regeringens skrivelse till riksdagen bedömdes uppfylla de krav som ställs på efterhandskontroll i regeringsformen och Europakonventionen.

Det finns en möjlighet att begära skadestånd för den som blivit utsatt för olaglig användning av hemliga tvångsmedel. Däremot kan domstolen inte avvisa bevisning endast för att den kommit från olaglig användning av hemliga tvångsmedel. Detta bedömdes förenligt med allmänna principer om bevisföring och strida varken mot regeringsformen eller Europakonventionen.

Om hemliga tvångsåtgärder har använts under en förundersökning utgör uppgifterna, upptagningarna och uppteckningarna en del av förundersökningsmaterialet. Den misstänkte har i samband med slutdelgivning av förundersökningen rätt att ta del av allt material som ligger till grund för åtalet och som bedöms relevant för rättegången, dvs. i princip det som finns i förundersökningsprotokollet. Den misstänkte har även rätt att ta del av förundersökningens sidomaterial, såvida det inte av hänsyn till allmänt eller enskilt intresse är av synnerlig vikt att sekretessbelagd uppgift i materialet inte röjs. Den misstänkte har däremot inte någon rätt till insyn i domstolens tvångsmedelsärende på grund av partsställning. Rätten till insyn och förevarande begränsningar ansågs förenliga med kraven i regeringsformen och Europakonventionen. Utredningen konstaterade dock att det för rätten till insyn är viktigt att sidomaterialet lätt kan överskådas. För att säkerställa att så sker föreslog utredningen att den misstänkte ska få en förteckning över förundersökningens sidomaterial, om han eller hon begär det.

Betänkandet bereds inom Regeringskansliet.

14.5 Våra förslag och den personliga integriteten

14.5.1 Förslagen innebär ökade integritetsrisker

Bedömning: Våra förslag innebär sammantaget vissa ökade integritetsrisker.

Skälen för bedömningen

En straffvärdeventil för viss flerfaldig brottslighet

I kapitel 6 föreslår vi i att det införs en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning i vissa fall där det enskilda brottet inte når upp till de strafftrösklar som i dag gäller men där den misstänkta brottsligheten sammantaget kan antas överstiga ett visst straffvärde. Förslagen gäller endast vid flerfaldig brottslighet av kvalificerat slag, nämligen sådan brottslighet som kan antas ha begåtts organiserat eller systematiskt. Vidare krävs det att brottet är häktningsgrundande eller, när det gäller hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter, att minimistraffet är lägst sex månaders fängelse. I kapitlet föreslår vi även att man avskaffar den brottskatalog som i dag begränsar tillämpningsområdet för straffvärdeventilen avseende hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter, och att någon sådan katalog inte heller ska gälla för den nya straffvärdeventilen för flerfaldig brottslighet.

Förslagen innebär att hemliga tvångsmedel kan användas i fler fall och för lindrigare brott än i dag, förutsatt att den samlade brottsligheten är av allvarligt slag. I den bemärkelsen innebär förslagen ett ökat integritetsintrång för enskilda. Däremot innebär förslagen inte några nya integritetsrisker. Det kan diskuteras om förutsebarheten försämras genom att bedömningen kan komma att omfatta flera brott och att bedömningen av det samlade straffvärdet kan bli mer osäker. Vi menar dock att sådana farhågor inte bör överdrivas, dels eftersom det krävs att straffvärdet inte bara uppnår utan kan antas överstiga två års fängelse, dels eftersom varje osäkerhet ska tillgodoräknas den misstänkte.

Utvidgade brottskataloger

I kapitel 7 föreslår vi att man lägger till ett antal brott till brottskatalogerna för hemlig avlyssning och hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig dataavläsning avseende motsvarande uppgiftstyper samt även hemlig dataavläsning som gäller lagrade uppgifter och uppgifter om användningen av informationssystemet. Förslagen rör allvarliga brott som anses särskilt svåra att utreda, bl.a. på grund av att de ofta begås i miljöer där få personer vill medverka i brottsutredningen, och brott där det av andra skäl är särskilt viktigt att man kan få tillgång till de uppgifter som omfattas av förslagen. Förslagen innebär inte några nya integritetsrisker men däremot att hemliga tvångsmedel kan aktualiseras i fler fall än i dag.

Hemlig övervakning mot målsäganden

I kapitel 8 diskuterar vi hemlig övervakning av elektronisk kommunikation riktad mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet. Vi gör där bedömningen att detta redan är tillåtet. I kapitlet föreslår vi emellertid att det ska bli tillåtet att vid hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen ska misstänkas för brottet, och motsvarande hemlig dataavläsning, hämta in uppgifter om meddelanden i realtid. Förslagen innebär utökade möjligheter att kartlägga den enskildes personliga förhållanden och detta i synnerhet om man även hämtar in lokaliseringsuppgifter. Ett slopande av begränsningen till uppgifter om meddelanden i förfluten tid innebär därför ett ökat integritetsintrång.

Hemlig avlyssning i syfte att utreda vem som skäligen kan misstänkas

Kapitel 9 innehåller förslag om en möjlighet att använda hemlig avlyssning av elektronisk kommunikation och även hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i syfte att utreda vem skäligen kan misstänkas för brottet. Förslagen innebär ett nytt användningsområde för befintliga hemliga tvångsmedel. I den bemärkelsen uppstår inga nya integritetsrisker. Det ligger dock i sakens

natur att det, när det saknas en skäligen misstänkt, finns en ökad risk för att personer som senare visar sig vara ovidkommande för utredningen utsätts för hemlig avlyssning eller hemlig dataavläsning. Med hänsyn till bl.a. detta har vi bedömt att möjligheten att använda tvångsmedlen i det angivna syftet bör vara betydligt snävare än möjligheten att använda hemlig avlyssning respektive hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter generellt. Även med beaktande av detta innebär förslagen vissa ökade integritetsrisker.

Hemlig rumsavlyssning och hemlig kameraövervakning som knyts till den skäligen misstänkte

I kapitel 10 föreslår vi att det införs en möjlighet att i undantagsfall knyta ett tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning till den skäligen misstänkte i stället för till en viss plats. Möjligheten föreslås vara begränsad på så sätt att det krävs särskilda skäl för att den ska få användas. Vidare föreslås vissa begränsningar när det gäller de platser där tvångsmedlet får verkställas och att det ska vara obligatoriskt att förena tillståndet med villkor som begränsar integritetsintrånget. Villkoren bör vara utformade på ett sådant sätt att åtgärden är proportionerlig och i övrigt godtagbar oavsett var den sedermera kommer att verkställas.

Den föreslagna regleringen överensstämmer i väsentliga avseenden med hur domstolarna i vissa fall tillämpar regleringen om hemlig rumsavlyssning och hemlig kameraövervakning redan i dag. Det förekommer nämligen att domstolarna godtar mycket vida platsangivelser – t.ex. en hel kommun eller flera hela kommuner. Det har dock även framkommit att det i andra fall ställs krav på betydligt mer precisa platsangivelser. Våra förslag innebär därmed ett förtydligande av vad som gäller när det av olika skäl inte går att på förhand ange en specifik och precist avgränsad plats. Vi lämnar motsvarande förslag i fråga om hemlig dataavläsning som avser rumsavlyssningsuppgifter respektive kameraövervakningsuppgifter. För hemlig dataavläsning gäller redan ett krav på att tillståndet förenas med villkor. Detta krav får dock en än större betydelse, liksom villkorens utformning. Villkoren bör även när det gäller hemlig dataavläsning vara utformade på ett sådant sätt att åtgärden är proportionerlig och i övrigt godtagbar oavsett var den sedermera kommer att verkställas.

Med hänsyn till att reglerna i vissa fall redan synes tillämpas på ett sätt som väsentligen överensstämmer med våra förslag kan det diskuteras om våra förslag i praktiken innebär ökade integritetsrisker. Man kan med visst fog hävda att skyddet för enskildas integritet förstärks genom att regleringen förtydligas och att det uppställs ett absolut krav på att tillstånden förenas med villkor. Våra förslag har också beaktat den tekniska utvecklingen, som innebär större möjligheter att rikta tvångsmedlet på ett sådant sätt att integritetsintrånget för utomstående minimeras. Motsvarande möjlighet finns dock inte när det gäller hemlig dataavläsning. Sammantaget bedömer vi att förslagen innebär vissa ökade integritetsrisker.

Interimistiska beslut om hemlig rumsavlyssning

Våra förslag i kapitel 11, som går ut på att åklagare får en möjlighet att fatta interimistiskt beslut om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter, samt om tillträdestillstånd för respektive tvångsmedel, bedöms inte innebära något ökat integritetsintrång eller några ökade integritetsrisker.

Tillträdestillstånd för enbart hemlig kameraövervakning

I kapitel 12 föreslår vi att det ska bli möjligt med ett beslut om tillträdestillstånd för att möjliggöra verkställighet av enbart en hemlig kameraövervakning. Vi föreslår vidare att åklagare ges möjlighet att fatta interimistiska beslut om sådana tillstånd. Det är inte tillåtet att meddela tillträdestillstånd till någons stadigvarande bostad och det ingår inte i vårt uppdrag att överväga några ändringar i detta avseende. Förslaget kan förväntas medföra att fler hemliga kameraövervakningar kan genomföras. Detta innebär att fler personer kan komma att utsättas för såväl det integritetsintrång som det hemliga tillträdet som själva tvångsmedlet innebär. Effekten mildras dock av förhållandet att tillträdet aldrig kan avse en stadigvarande bostad. Regeringen har tidigare uttalat att tillträde till utrymmen som inte utgör någons bostad i normalfallet får förväntas ge upphov till begränsade integritetsintrång (prop. 2013/14:237 s. 153). Vårt förslag om att åklagare ska få en möjlighet att fatta interimistiska beslut om tillträde bedöms inte innebära något ökat integritetsintrång eller några ökade integritetsrisker.

Samlad bedömning

Våra förslag innebär både sedda för sig och sammantagna ökade risker för den personliga integriteten både på det sättet att de befintliga hemliga tvångsmedlen kan användas i fler fall och på det sättet att vissa av våra förslag innebär en ökad risk för att ovidkommande personer utsätts för hemliga tvångsmedel. Det bör samtidigt framhållas att den tekniska utvecklingen har inneburit att hemlig rumsavlyssning och hemlig kameraövervakning numera i många fall kan genomföras på ett sätt som begränsar integritetsintrånget för andra än den som åtgärden faktiskt avser.

14.5.2 Förslagen innebär även en förstärkning av enskildas rätt till skydd för sin personliga integritet

Bedömning: Förslagen bedöms leda till förbättrade möjligheter att utreda allvarlig brottslighet mot enskilda och att avbryta pågående sådan brottslighet. I detta avseende innebär förslagen ett förstärkt skydd för enskildas personliga integritet.

Skälen för bedömningen

Av det anförda följer att våra förslag sammantaget innebär ökade integritetsrisker. Det handlar delvis om att fler misstänkta personer kan bli föremål för hemliga tvångsmedel. Av större betydelse är dock enligt vår mening att fler personer som inte är misstänkta, och som i vissa fall är ovidkommande för brottsutredningen, kan utsättas för hemliga tvångsmedel. Det bör dock framhållas att det inte alltid behöver vara enbart till nackdel för någon att utsättas för ett hemligt tvångsmedel. Åtgärden kan nämligen ge information som leder till att brottsmisstankar mot en viss person kan avfärdas och personen avskrivas från utredningen.

En annan viktig aspekt är att hemliga tvångsmedel kan leda till att allvarlig brottslighet kan utredas och de ansvariga ställas till svars. Detta kan innebära en upprättelse för eventuella brottsoffer och i förlängningen leda till att gärningspersonen hindras från att begå nya brott. Man kan uttrycka detta som att förslagen förväntas leda till en ökad rättstrygghet. Rätten till skydd för den personliga integriteten

handlar inte enbart om den som utsätts för ett hemligt tvångsmedel utan även i högsta grad om enskildas rätt att slippa bli utsatta för kränkningar från andra enskilda, och att rättsväsendet effektivt ingriper när en kränkning har ägt rum. Av artikel 8 i Europakonventionen följer inte bara ett förbud för staten att göra otillåtna ingrepp i privatlivet utan även en skyldighet för staten att genom bl.a. lagstiftning och andra åtgärder skydda den enskildes privatliv, familjeliv och korrespondens mot ingrepp från andra. (Se X och Y mot Nederländerna punkt 23, von Hannover mot Tyskland punkt 57 och K.U. mot Finland punkterna 47–49). Ett sådant skydd tillförsäkras bl.a. genom kriminalisering av olika åtgärder som innefattar allvarliga intrång i den personliga integriteten, såsom sexuella övergrepp, men även genom en väl fungerande och effektiv brottsbekämpning. Detta krav innebär t.ex. att myndigheterna ska ha tillgång till effektiva utredningsverktyg – även i den elektroniska miljön – för att utreda brott som innefattar allvarliga kränkningar. När så inte har varit fallet har staten ansetts kränka de rättigheter som följer av artikel 8. Ett exempel på detta var målet K.U. mot Finland. I målet hade en okänd person lagt upp en kränkande kontaktannons avseende ett 12-årigt barn på en dejtingsajt. Europadomstolen fann att avsaknaden av en möjlighet enligt finsk rätt att från operatören inhämta uppgift om vem som använt en ip-adress, vilket ledde till att personen inte kunde identifieras, utgjorde en kränkning av artikel 8. Europadomstolen uttalade i domen att konfidentialitet för kommunikation och yttrandefrihet ibland måste få vika för brottsbekämpande ändamål. Målet Khadija Ismayilova mot Azerbajdzjan (punkterna 105–132) gällde en hemlig filmning av en journalist i hennes hem och publiceringen av bildmaterialet. I det fallet fanns det tillämpliga straffbestämmelser och en brottsutredning hade inletts. Emellertid fann Europadomstolen att myndigheterna genom att inte genomföra en effektiv brottsutredning av det mycket allvarliga intrånget i hennes privatliv hade underlåtit att tillförsäkra klaganden ett tillräckligt skydd för hennes privatliv (punkterna 119–131).

Av det anförda framgår att hemliga tvångsmedel aktualiserar två aspekter av skyddet för enskildas personliga integritet som måste balanseras mot varandra. Vi bedömer att våra förslag sammantagna påtagligt förbättrar möjligheterna att utreda allvarlig brottslighet som går ut över enskilda. I vissa fall kan dessutom en möjlighet att komma framåt i utredningen vara den enda möjligheten att avbryta en på-

gående brottslighet mot någon enskild. Det kan t.ex. handla om upprepade sexuella övergrepp mot barn som begås med digitala hjälpmedel. Våra förslag innebär således såväl ett ökat integritetsintrång i vissa avseenden som en förstärkning av enskildas rätt till skydd mot allvarliga brott, dvs. en ökad rättstrygghet och ett förstärkt skydd för den personliga integriteten.

14.5.3 Förändrade förhållanden har lett till ett ökat behov av hemliga tvångsmedel

Bedömning: Förhållandena har ändrats på ett sätt som innebär att behovet av hemliga tvångsmedel för att allvarlig brottslighet ska kunna utredas har ökat.

Skälen för bedömningen

Våra förslag handlar om bekämpning av allvarlig och typiskt sett svårutredd brottslighet. Starka behovsskäl talar för samtliga de ändringar som vi föreslår.

Som vi har lyft fram tidigare i betänkandet har det blivit allt vanligare att enskilda inte vill eller vågar medverka i brottsutredningar. Detta hänger bl.a. samman med förekomsten av s.k. tystnadskulturer. I takt med denna utveckling ökar behovet av en möjlighet att få tillgång till informationen på annan väg. Många gånger är hemliga tvångsmedel den enda framkomliga möjligheten för att man ska kunna komma framåt i utredningar om allvarlig brottslighet.

Det har vidare betydelse att den it-relaterade brottsligheten har ökat kraftigt (se bl.a. redogörelsen i prop. 2019/20:64 s. 61 och 62). Med it-relaterad brottslighet avses här alla brott som på något sätt har koppling till informationsteknologi. It kan vara målet för brottet eller ett verktyg för att begå brottet men brott kan även i andra fall vara it-relaterade genom att det finns digitala spår och bevisning i t.ex. mobiltelefoner, chattforum eller på hårddiskar.[2] Med hjälp av digital teknik kan gärningspersoner nå fler potentiella brottsoffer utan att hindras av geografiska, fysiska eller språkliga barriärer. Ett exem-

[2] Definitionen är hämtad från Brå, It-inslag i brottsligheten och rättsväsendets förmåga att hantera dem. Rapport 2016:17.

pel på detta är bedrägeribrottslighet. Bedrägerier är en typ av brottslighet som ökat i både omfång och komplexitet till följd av den tekniska utvecklingen och den ökade internetanvändningen (SOU 2021:85 Vägar till ett tryggare samhälle, s. 48). Andelen datorbedrägerier har ökat succesivt sedan mitten av 2000-talet och utgjorde under 2018 hälften av de anmälda bedrägerierna.[3] Ett annat exempel är sexualbrott mot barn som i allt högre grad utförs via internet (SOU 2021:85 s. 65). Enligt en fördjupad studie hade närmare en fjärdedel av gymnasieleverna som ingick i den bakomliggande undersökningen uppgett att någon i vuxen ålder försökt kontakta dem i sexuellt syfte före 15 års ålder.[4] Ytterligare ett exempel är näthandeln med narkotika. De angivna brotten är exempel på brott som ofta begås med digitala hjälpmedel, men det är viktigt att framhålla att så gott som alla typer av brott i dag kan ha någon form av it-inslag (se bl.a. SOU 2017:100 Beslag och husrannsakan – ett regelverk för dagens behov, s. 220 och SOU 2021:85 s. 45). Det anförda innebär att behovet av tillgång till elektronisk bevisning också har ökat.

En annan viktig faktor, som vi har berört på flera håll i betänkandet, är de kriminellas riskmedvetenhet. Risken för hemlig avlyssning av elektronisk kommunikation och hemlig dataavläsning har lett till att kriminella många gånger undviker att kommunicera elektroniskt och i stället väljer fysiska möten. Hemlig rumsavlyssning kan då vara den enda framkomliga vägen för att få kunskap om vad som sägs vid dessa möten. För att undvika rumsavlyssning har de kriminella utvecklat strategier som många gånger leder till att en planerad insats, t.ex. en hemlig rumsavlyssning, inte kan verkställas i enlighet med planen eller att myndigheterna avstår från att ansöka om tillstånd eftersom det inte på förhand går att ange var åtgärden kommer att behöva verkställas. I andra fall har domstolarna hanterat situationen genom att tillåta hemlig rumsavlyssning avseende ett större område.

I vissa områden har kriminella grupperingar närmast total kontroll av vem som kommer in i området. Traditionell spaning kan då vara omöjlig. Det kan även vara omöjligt att genom ett fysiskt intrång installera teknisk utrustning för en hemlig kameraövervakning eller hemlig rumsavlyssning. I sådana fall kan hemlig kameraövervak-

[3] Brå, Brottsförebyggande rådet, Bedrägeribrottsligheten i Sverige. Rapport 2016:9.
[4] Jonsson, L. och Svedin, C. G. (2017) Barn utsatta för sexuella övergrepp på nätet. Barnafrid – Nationellt kunskapscentrum. Linköpings universitet.

ning eller hemlig dataavläsning vara de enda möjligheterna att få tillgång till den information som behövs för att föra utredningen framåt.

Även den tekniska utvecklingen har betydelse liksom ändrade kommunikationsmönster. De skäl som låg till grund för införandet av hemlig dataavläsning, bl.a. ökad användning av anonymisering och kryptering (prop. 2019/20:64 avsnitt 7), talar starkt för att möjligheten att använda hemlig dataavläsning bör utökas i motsvarande mån som övriga hemliga tvångsmedel. Vidare har den tekniska utvecklingen inneburit ökade möjligheter att rikta hemlig rumsavlyssning och hemlig kameraövervakning på ett sådant sätt att risken för integritetsintrång mot ovidkommande personer minimeras.

14.5.4 Skyddet för den personliga integriteten är tillräckligt

Bedömningar: Våra sammantagna förslag ger uttryck för en rimlig avvägning av behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet.

Det finns inte något behov av ytterligare rättssäkerhetsgarantier. Det är dock av stor vikt med en effektiv tillsyn.

Skälen för bedömningarna

Vi har i respektive kapitel redovisat våra överväganden i fråga om hur de utökade möjligheterna att använda hemliga tvångsmedel bör begränsas för att de inte ska utgöra ett oproportionerligt ingrepp i enskildas rätt till skydd för sin personliga integritet. Vi har i respektive kapitel gjort bedömningen att våra förslag är proportionerliga vart och ett för sig. Det integritetsintrång som aktualiserats har alltså ansetts stå i proportion till de skäl som talar för den föreslagna ändringen. Med hänsyn till de starka behovsskäl som talar för våra förslag, inte minst med beaktande av att förhållandena har ändrats och vikten av att enskilda ges ett effektivt skydd mot att utsättas för kränkningar från andra enskilda, till de begränsningar som vi föreslår ska gälla för de utökade möjligheterna och till de omfattande rättssäkerhetsgarantier som gäller för hemliga tvångsmedel, gör vi samma bedömning i fråga om förslagen sammantagna. Vi anser alltså att den sammantagna ökningen av integritetsriskerna för enskilda är propor-

tionerlig i förhållande till behovet av de utökade möjligheter vi föreslår. Bedömningen står sig även med beaktande av de straffskärpningar som skett under de senaste åren eller som kan förväntas (se redogörelsen i kapitel 5). I den mån föreslagna straffskärpningar kan påverka våra förslag har vi redovisat det i respektive kapitel.

Sammanfattningsvis gör vi alltså bedömningen att våra sammantagna förslag ger uttryck för en rimlig avvägning av behovet av en effektiv brottsbekämpning och den enskildes rätt till skydd för sin personliga integritet.

Vi anser inte att det behövs några ytterligare rättssäkerhetsgarantier för att förslagen ska leva upp till kraven på hög rättssäkerhet. Som framgått i avsnitt 14.4 har de befintliga rättssäkerhetsgarantierna utvärderats tidigare och i huvudsak ansetts tillräckliga. Våra förslag innebär inte införande av några nya tvångsmedel. Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel har lämnat vissa förslag som fortfarande bereds inom Regeringskansliet. Det finns ingen anledning för oss att i detta läge anlägga några synpunkter på dessa förslag eller att på nytt överväga samma frågor som den utredningen. Det finns dock anledning att särskilt gå in på några av våra förslag ur ett rättssäkerhetsperspektiv.

Vi bedömer att våra förslag i kapitel 10 om en möjlighet att i vissa fall knyta ett tillstånd till bl.a. hemlig rumsavlyssning till den skäligen misstänkte utgör en nödvändig anpassning av regleringen till dagens förhållanden och ett förtydligande av vad som gäller, vilket är en förbättring från rättssäkerhetssynpunkt. Vi har där övervägt om den nya möjligheten bör kombineras med ett krav på efterföljande domstolsprövning av verkställigheten och kommit fram till att något sådant inte är lämpligt. Vi har däremot kommit fram till att tillståndet alltid ska vara förenat med villkor som begränsar integritetsintrånget för enskilda och en skyldighet för åklagaren att lämna förslag till sådana villkor. Därigenom menar vi att risken för onödiga integritetsintrång i tillräcklig mån har begränsats. Förslaget föranleder enligt vår mening inte något behov av ytterligare rättssäkerhetsgarantier.

När möjligheten till interimistiska beslut om bl.a. hemlig avlyssning av elektronisk kommunikation fördes in i rättegångsbalken ansåg lagstiftaren att en ordning med efterföljande obligatorisk domstolsprövning innebar att det saknas skäl att anta att en sådan möjlighet skulle få några negativa konsekvenser för enskildas rättssäkerhet (prop. 2013/14:237 s. 141). För att utökade möjligheter till interimis-

tiska beslut inte skulle få negativa konsekvenser för enskildas rättssäkerhet ansågs det dock även nödvändigt med en begränsningsregel som innebär att man inte till någons nackdel får använda information som kommit fram vid en verkställighet, om domstolen vid sin prövning kommer fram till att det inte funnits skäl för åtgärden. Våra förslag i kapitel 11 och 12 om ökade möjligheter för åklagare att fatta interimistiska beslut bygger på att samma rättssäkerhetsgarantier ska vara tillämpliga som beträffande övriga hemliga tvångsmedel. Dessa bedöms tillräckliga.

Det har tidigare övervägts om det skulle införas ett krav på medverkan av offentliga ombud i ärenden om hemlig övervakning av elektronisk kommunikation (se bl.a. prop. 2013/14:237 s. 120). Ett skäl som skulle kunna tala för det är att åtgärden blir mer ingripande från integritetssynpunkt när man vid hemlig övervakning i syfte att utreda vem som skäligen kan misstänkas tar bort begränsningen till uppgifter om meddelanden som redan skickats. Vår bedömning är dock att denna förändring inte är så betydande att det finns skäl att omvärdera det ställningstagande som tidigare gjorts.

Även om vi alltså kommit fram till att det inte behöver införas några nya rättssäkerhetsgarantier, finns det skäl att framhålla vikten av att de befintliga rättssäkerhetsgarantierna fungerar så som det är tänkt. SIN har vid sina granskningar uppmärksammat att det förekommer brister vid hanteringen av hemliga tvångsmedel (se bl.a. uttalande med beslut 2021-12-15, Granskning av ärenden vid Åklagarmyndigheten i vilka hemlig dataavläsning använts, dnr 92-2020, och uttalande med beslut 2021-06-21, Hanteringen av hemliga tvångsmedel vid åklagarkammaren i Eskilstuna, dnr 136-2019). Det är mycket viktigt för rättssäkerheten och tilltron till systemet att brister upptäcks och uppmärksammas. Det är därför nödvändigt att det finns förutsättningar för en effektiv tillsyn och efterhandskontroll av tillämpningen av hemliga tvångsmedel. SIN har en särskilt viktig roll i detta avseende. Våra förslag innebär att tillämpningsområdet för de hemliga tvångsmedlen ökar, vilket ställer ökade krav på tillsynsverksamheten. Det är därför nödvändigt att SIN har tillräckliga resurser.

Avslutningsvis vill vi också framhålla vikten av kontinuerliga utbildningsinsatser för de personer som deltar i besluten. Åklagare och domare har tillgång till detta i den ordinarie utbildningsverksamhet som finns inom åklagarväsendet och Domstolsakademin. Någon direkt motsvarighet finns emellertid inte för offentliga ombud. Vi har emel-

lertid erfarit att det är möjligt för pensionerade domare att delta i Domstolsakademins utbildning. För advokater har tidigare funnits utbildning i dessa frågor och det är sannolikt att denna utbildning kommer att återupptas. Vi vill understryka vikten av att de offentliga ombuden använder sig av dessa utbildningsmöjligheter.

15 Följdändringar

15.1 Uppdraget

Det ingår i vårt uppdrag att se till att en välfungerande systematik upprätthålls i regelverket om hemliga tvångsmedel. Det innebär att vi även ska överväga behovet av följdändringar i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i det brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen), lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och lagen (1991:572) om särskild utlänningskontroll samt lagen (2020:62) om hemlig dataavläsning. Vi ska även bedöma behovet av följdändringar i lagen (2000:562) om internationell rättslig hjälp i brottmål (LIRB) och lagen (2017:1000) om en europeisk utredningsorder. När det finns behov av det ska vi lämna förslag på författningsändringar. Vi har även övervägt behovet av lagändringar i andra författningar än de som nämns i direktiven.

15.2 Lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

Förslag: Bestämmelserna om interimistiska beslut om hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter i lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. ska upphöra att gälla.

Skälen för förslaget

Enligt 28 § lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. är det vid krig eller krigsfara tillåtet för en åklagare att fatta interimistiska beslut om hemlig rumsavlyssning och hemlig dataavläsning som gäller rumsavlyssningsuppgifter (28 §). När en generell möjlighet till interimistiska åklagarbeslut avseende de angivna åtgärderna införs, vilket vi föreslår i kapitel 11, finns det inte längre skäl att behålla de särskilda bestämmelserna i 28 §. Vi föreslår därför att paragrafen ska upphöra att gälla.

15.3 Lagen om internationell rättslig hjälp i brottmål

Förslag: Åklagare ges en möjlighet att på begäran av en annan stat fatta interimistiskt beslut om hemlig rumsavlyssning av någon i Sverige och om tillträdestillstånd avseende hemlig rumsavlyssning och hemlig kameraövervakning. När ett interimistiskt beslut om hemlig rumsavlyssning har fattats ska återredovisning inte ske förrän rätten har fattat beslut om tvångsmedlet.

Bedömning: Åklagare bör även ha en möjlighet att fatta interimistiskt beslut om hemlig dataavläsning som gäller rumsavlyssningsuppgifter och om tillträdestillstånd för att möjliggöra verkställighet av åtgärden. När ett interimistiskt beslut om hemlig dataavläsning som gäller rumsavlyssningsuppgifter har fattats ska återredovisning inte ske förrän rätten har fattat beslut om tvångsmedlet. Det behövs inga lagändringar för att åstadkomma detta.

Skälen för förslagen och bedömningen

Bestämmelserna

I LIRB finns bestämmelser om rättslig hjälp i brottmål i Sverige och utomlands. Lagen har delvis ersatts av lagen om en europeisk utredningsorder och gäller inte om den lagen är tillämplig (1 kap. 7 a § LIRB). Lagen bygger på principen att Sverige, på begäran av en annan stat, ska kunna vidta en begärd åtgärd om åtgärden hade kunnat vidtas

i ett svenskt förfarande och att svenska åklagare och domstolar ska bistå sina utländska motsvarigheter med olika åtgärder under samma villkor och förutsättningar som motsvarande åtgärder kan genomföras i en svensk förundersökning eller rättegång (prop. 1999/2000:61 s. 97). En översiktlig redogörelse för lagens innehåll finns i avsnitt 4.5.

I 4 kap. 27 § regleras hemlig kameraövervakning av någon i Sverige. En sådan ansökan från en annan stat handläggs av åklagare som genast ska pröva om det finns förutsättningar för åtgärden och i sådant fall ansöka om rättens tillstånd, eller när det får ske enligt 27 kap. 21 a § RB, själv besluta om åtgärden. Tillträdestillstånd omfattas inte av möjligheten till interimistiskt beslut, eftersom tillträdestillstånd i dagsläget bara kan meddelas när även hemlig rumsavlyssning ska ske. Någon möjlighet till interimistiskt beslut om hemlig rumsavlyssning finns inte.

Hemlig rumsavlyssning av någon som befinner sig i Sverige regleras i 4 kap. 28 a § LIRB. Bestämmelsen har motsvarande innehåll som 27 §, med den skillnaden att den inte innehåller någon bestämmelse om interimistiska åklagarbeslut.

Bestämmelser om hemlig dataavläsning finns i 4 kap. 28 c §. Där framgår att en ansökan om hemlig dataavläsning i Sverige handläggs av åklagare och att det av ansökan ska framgå under vilken tid som åtgärden önskas och sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Vidare anges att åklagaren genast ska pröva om det finns förutsättningar för åtgärden och i sådant fall själv ansöka om rättens tillstånd till åtgärden eller, när det får ske enligt 17 § lagen om hemlig dataavläsning, själv besluta om åtgärden.

Överväganden

Vi föreslår i kapitel 11 att åklagaren ska ges möjlighet att fatta interimistiska beslut om hemlig rumsavlyssning och om tillträdestillstånd för installation av tekniska hjälpmedel. Vi föreslår dessutom i kapitel 12 att ett tillträdestillstånd för hemlig kameraövervakning ska kunna meddelas, även interimistiskt, utan att det samtidigt behöver ske en hemlig rumsavlyssning. I likhet med vad som gäller i fråga om övriga tvångsmedel bör åklagarens möjlighet att fatta ett interimistiskt beslut till följd av en ansökan från en annan stat motsvara möjligheten till interimistiskt beslut i en svensk förundersökning.

Bedömningen föranleder ändringar i 4 kap. 27 första stycket och 28 a §§ LIRB.

När åklagaren har fattat ett interimistiskt beslut om hemlig kameraövervakning till följd av en ansökan från en annan stat, ska återredovisning enligt 2 kap. 17 § ske först sedan rätten fattat beslut om hemlig kameraövervakning. Motsvarande bör gälla vid interimistiskt beslut om hemlig rumsavlyssning. Detta kräver ändringar i 4 kap. 28 a §.

Våra förslag i kapitel 11 innebär vidare att det införs en möjlighet för åklagare att fatta interimistiska beslut om hemlig dataavläsning som gäller rumsavlyssningsuppgifter. På de nyss anförda skälen bör motsvarande möjlighet finnas vid rättslig hjälp. Den föreslagna ändringen kommer till följd av hänvisningen till 17 § lagen om hemlig dataavläsning att gälla i 4 kap. 28 c § LIRB utan att det behöver göras någon ändring i paragrafen. När det gäller tillträdestillstånd för installation av tekniska hjälpmedel finns det redan i dag en möjlighet att besluta om tillträdestillstånd även när åtgärden avser enbart kameraövervakningsuppgifter, se 12 § lagen om hemlig dataavläsning. Vidare omfattas tillträdestillstånd – med undantag för rumsavlyssningsuppgifter – redan i dag av åklagarens möjlighet att fatta interimistiskt beslut. Detta sägs inte uttryckligen i lagtexten utan framgår av att åklagarens beslutsbefogenheter enligt 17 § första stycket lagen om hemlig dataavläsning omfattar ”frågor om hemlig dataavläsning”, vilket rymmer även tillträdestillstånd. När hemlig dataavläsning lades till i bestämmelserna om interimistiskt åklagarbeslut i lagen om internationell rättslig hjälp i brottmål kommenterades inte frågan om tillträdestillstånd i förarbetena (jfr prop. 2019/20:64 s. 191 f.). Bestämmelsen måste dock med hänsyn till hänvisningen till 17 § lagen om hemlig dataavläsning förstås så att möjligheten till interimistiskt beslut omfattar även tillträdestillstånd. Det är inte nödvändigt att göra någon författningsändring för att möjligheten ska omfatta även tillträde som syftar till en avläsning av rumsavlyssningsuppgifter.

Enligt 4 kap. 28 c § tredje stycket gäller vid interimistiska åklagarbeslut att återredovisning enligt 2 kap. 17 § ska ske först när rätten fattat beslut om hemlig dataavläsning. Detta bör gälla även när beslutet gäller rumsavlyssningsuppgifter. Någon författningsändring krävs inte för att detta ska gälla.

15.4 Lagen om en europeisk utredningsorder

Förslag: Åklagare ges en möjlighet att fatta ett interimistiskt beslut om utfärdande av en utredningsorder avseende hemlig rumsavlyssning och om tillträdestillstånd avseende hemlig rumsavlyssning och hemlig kameraövervakning. Åklagare ges också möjlighet att besluta om att interimistiskt erkänna och verkställa hemlig rumsavlyssning och tillträdestillstånd avseende hemlig rumsavlyssning och hemlig kameraövervakning.

Bedömning: Åklagare bör ha en möjlighet att interimistiskt besluta att utfärda, erkänna och verkställa en utredningsorder om hemlig dataavläsning som gäller rumsavlyssningsuppgifter och om tillträdestillstånd för att möjliggöra verkställighet av åtgärden. Det behövs inga lagändringar för att åstadkomma detta.

Skälen för förslagen

Bestämmelserna

Med en europeisk utredningsorder avses ett beslut i Sverige som innebär att en utredningsåtgärd ska vidtas i en annan medlemsstat i syfte att inhämta bevisning som behövs i en svensk förundersökning eller rättegång i brottmål. Vidare avses ett beslut i en annan medlemsstat som innebär att en utredningsåtgärd ska vidtas i Sverige i syfte att inhämta bevisning. (1 kap. 3 § lagen om en europeisk utredningsorder.) I 1 kap. 4 § räknas upp ett antal åtgärder som en utredningsåtgärd enligt lagen ska avse eller motsvara. Där framgår att de hemliga tvångsmedlen kan omfattas av en europeisk utredningsorder. En utredningsorder får utfärdas i Sverige om de förutsättningar som gäller för att vidta utredningsåtgärden under en svensk förundersökning eller rättegång i brottmål och enligt lagen om en europeisk utredningsorder är uppfyllda (2 kap. 3 §). En utredningsorder som gäller hemliga tvångsmedel får erkännas och verkställas endast om den gärning som avses i utredningsordern motsvarar ett brott enligt svensk lag (krav på dubbel straffbarhet) och om övriga förutsättningar som gäller för en motsvarande åtgärd i en svensk förundersökning eller rättegång i brottmål är uppfyllda (3 kap. 4 §). Vad gäller hemlig rums-

avlyssning och hemlig kameraövervakning innebär detta också ett krav på att utredningsordern, i de fall det skulle krävas enligt 27 kap. 25 a § rättegångsbalken, innehåller ett beslut motsvarande ett sådant tillträdestillstånd som kan meddelas enligt nämnda bestämmelse (prop. 2016/17:218 Nya regler om bevisinhämtning inom EU, s. 130). Ett sådant tillstånd kan, beroende på den ordning som gäller enligt den utfärdande statens lagstiftning, antingen anges som ett separat beslut i utredningsordern, t.ex. som ett beslut om husrannsakan, eller omfattas av själva beslutet om hemlig rumsavlyssning eller hemlig kameraövervakning (prop. 2016/17:218 s. 199). När hemlig dataavläsning lades till i förteckningen över hemliga tvångsmedel som kan omfattas av en utredningsorder kommenterades inte frågan om tillträdestillstånd, men samma sak torde gälla vid hemlig dataavläsning.

Enligt 2 kap. 5 § första stycket ska åklagaren, innan en utredningsorder utfärdas på begäran av en annan stat, ansöka om rättens tillstånd i fall då utredningsordern avser bl.a. hemliga tvångsmedel. Enligt andra stycket i paragrafen får åklagaren dock i avvaktan på rättens beslut utfärda en utredningsorder för kvarhållande av försändelse, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig dataavläsning. Ett sådant interimistiskt beslut får fattas under samma förutsättningar som om åtgärden hade vidtagits i en svensk förundersökning, dvs. de förutsättningar som anges i 27 kap. 9 a § och 21 a §§ rättegångsbalken eller 17 § lagen om hemlig dataavläsning.

En bestämmelse om interimistiskt beslut finns även i 3 kap. 10 § som handlar om erkännande och verkställighet i Sverige av en europeisk utredningsorder. Huvudregeln enligt 3 kap. 9 § är att en utredningsorder som avser en utredningsåtgärd som i en svensk förundersökning eller rättegång i brottmål kräver rättens tillstånd ska prövas av domstol. Enligt 3 kap. 10 § får åklagaren dock i avvaktan på rättens beslut, enligt de förutsättningar som anges i rättegångsbalken och lagen om hemlig dataavläsning, besluta att erkänna och verkställa en utredningsorder för kvarhållande av en försändelse eller för hemlig avlyssning eller hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning eller hemlig dataavläsning.

Överväganden

Som nyss nämnts föreslår vi i kapitel 11 att åklagaren ska ges möjlighet att fatta interimistiska beslut om hemlig rumsavlyssning och om tillträdestillstånd för installation av tekniska hjälpmedel. Vi föreslår dessutom i kapitel 12 att ett tillträdestillstånd för hemlig kameraövervakning ska kunna meddelas, även interimistiskt, utan att det samtidigt behöver ske en hemlig rumsavlyssning. Motsvarande möjligheter bör finnas vid en europeisk utredningsorder. Detta kräver ändringar i 2 kap. 5 § andra stycket och 3 kap. 10 § lagen om en europeisk utredningsorder.

Våra förslag i kapitel 11 innebär vidare att det införs en möjlighet för åklagare att fatta interimistiska beslut om hemlig dataavläsning som gäller rumsavlyssningsuppgifter. Den föreslagna ändringen kommer att gälla i lagen om en europeisk utredningsorder utan att det behöver göras någon ändring i den lagen. När det gäller tillträdestillstånd för installation av tekniska hjälpmedel finns det redan i dag en möjlighet att besluta om tillträdestillstånd även när åtgärden avser enbart kameraövervakningsuppgifter, se 12 § lagen om hemlig dataavläsning. Vidare omfattas tillträdestillstånd – med undantag för rumsavlyssningsuppgifter – redan i dag av åklagarens möjlighet att fatta interimistiskt beslut. Detta sägs inte uttryckligen i lagtexten utan framgår av att åklagarens beslutsbefogenheter enligt 17 § första stycket lagen om hemlig dataavläsning omfattar ”frågor om hemlig dataavläsning”, vilket rymmer även tillträdestillstånd. När hemlig dataavläsning lades till i bestämmelserna om interimistiskt åklagarbeslut i lagen om en europeisk utredningsorder kommenterades inte frågan om tillträdestillstånd i förarbetena (jfr prop. 2019/20:64) och SOU 2017:89). Bestämmelsen måste dock med hänsyn till hänvisningen till 17 § lagen om hemlig dataavläsning förstås så att möjligheten till interimistiskt beslut enligt lagen om en europeisk utredningsorder omfattar även tillträdestillstånd. Det är inte nödvändigt att göra någon författningsändring för att möjligheten ska omfatta även tillträde som syftar till en avläsning av rumsavlyssningsuppgifter.

15.5 Inga andra följdändringar krävs

Bedömning: Det behövs inte några andra följdändringar.

Skälen för bedömningen

Platskravet i underrättelseverksamhet

Vi har i kapitel 10 redovisat överväganden om kravet på att hemlig kameraövervakning, hemlig rumsavlyssning och hemlig dataavläsning som avser kameraövervaknings- eller rumsavlyssningsuppgifter knyts till en viss plats och lämnat förslag som innebär att tillstånd till de angivna åtgärderna i vissa fall ska kunna knytas till den skäligen misstänkte. Som vi nämnt i kapitel 10.1 finns det bestämmelser om krav på koppling till en viss plats även i 3 § preventivlagen och 7 § lagen om hemlig dataavläsning. Vi har i det nyss nämnda avsnittet gjort bedömningen att en översyn av dessa bestämmelser sträcker sig längre än vad som följer av vårt uppdrag att föreslå följdändringar och att vi inte heller har möjlighet att ta upp frågan utan att det skulle leda till fördröjningar. Några vidare överväganden om ändringar av 3 § preventivlagen respektive 7 § lagen om hemlig dataavläsning görs därför inte.

Begränsning till uppgifter som avser förfluten tid vid underrättelseverksamhet

Vi föreslår i avsnitt 7.5 att det ska bli tillåtet att vid hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas inhämta uppgift om meddelanden även i realtid. Vi lämnar motsvarande förslag när det gäller hemlig dataavläsning i samma syfte. En begränsning till förfluten tid finns även vid inhämtning av uppgifter om meddelanden i underrättelseverksamhet (1 § första punkten inhämtningslagen och 10 § lagen om hemlig dataavläsning). Med ett undantag omfattar vårt uppdrag i princip inte underrättelseverksamhet. Även om man kan diskutera reglernas inbördes förhållande anser vi att våra förslag när det gäller att utreda vem som skäligen kan misstänkas inte har ett sådant samband med underrättelseverksamhet att det är fråga om en nödvändig följdändring.

Inga ytterligare följdändringar i lagen om hemlig dataavläsning

Eftersom hemlig dataavläsning kan vara en metod för att under en förundersökning få tillgång till samma slags uppgifter som avses med en hemlig övervakning eller hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning eller hemlig rumsavlyssning har vi genomgående i betänkandet övervägt behovet av ändringar i lagen om hemlig dataavläsning såvitt gäller hemlig dataavläsning under en förundersökning. Några ytterligare ändringar av dessa bestämmelser bedöms inte nödvändiga.

Övrigt

Några andra följdändringar bedöms inte nödvändiga.

16 Ikraftträdande

Förslag: Lagändringarna ska träda i kraft den 1 januari 2024.

Bedömning: Det finns inte behov av några övergångsbestämmelser.

Skälen för förslaget och bedömningen

Den nya regleringen bör träda i kraft så snart som möjligt. Med beaktande av den tid som kan beräknas gå åt för remissbehandling och beredning inom Regeringskansliet bedömer vi att detta kan ske tidigast den 1 januari 2024.

Utgångspunkten när det gäller processrättslig lagstiftning är 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 trätt i kraft. Det medför att de brottsbekämpande myndigheterna och domstolarna ska tillämpa de nya bestämmelserna även i förundersökningar och tvångsmedelsärenden som inletts innan de föreslagna bestämmelserna trätt i kraft. Detta är en lämplig ordning. Några övergångsbestämmelser behövs inte för bestämmelser av det slag som vi föreslår (se prop. 2013/14:237 s. 172).

17 Konsekvenser

17.1 Inledning

I 14–16 §§ kommittéförordningen regleras vilka krav som ställs på utredningars redovisning av konsekvenser. Dessa innebär följande.

Om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller regioner, ska kommittén föreslå en finansiering.

Om förslagen i ett betänkande har betydelse för den kommunala självstyrelsen, ska konsekvenserna i det avseendet anges i betänkandet. Detsamma gäller när ett förslag har betydelse för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen.

Eftersom betänkandet innehåller förslag till nya eller ändrade regler, ska förslagens kostnadsmässiga och andra konsekvenser anges i betänkandet. Konsekvenserna ska anges på ett sätt som motsvarar de krav på innehållet i konsekvensutredningar som finns i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning. En konsekvensutredning ska enligt dessa bestämmelser innehålla följande.

1. en beskrivning av problemet och vad man vill uppnå,
2. en beskrivning av vilka alternativa lösningar som finns för det man vill uppnå och vilka effekterna blir om någon reglering inte kommer till stånd,
3. uppgifter om vilka som berörs av regleringen,

4. uppgifter om de bemyndiganden som myndighetens beslutanderätt grundar sig på,
5. uppgifter om vilka kostnadsmässiga och andra konsekvenser regleringen medför och en jämförelse av konsekvenserna för de övervägda regleringsalternativen,
6. en bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen, och
7. en bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser.

Om regleringen kan få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt ska konsekvensutredningen även innehålla vissa ytterligare beskrivningar.

Utöver det angivna följer det av våra direktiv att vi ska föreslå hur eventuella kostnadsökningar för det allmänna ska finansieras. Vidare ska vi beskriva hur förslagen förhåller sig till Sveriges internationella åtaganden om mänskliga rättigheter.

Problembeskrivningar och det som vi önskar uppnå samt alternativa lösningar framgår av respektive övervägandekapitel. Där framgår även våra bedömningar av hur våra förslag förhåller sig till EU-rätten och Sveriges åtaganden när det gäller mänskliga rättigheter. Det som har sagts i de angivna kapitlen upprepas inte här.

17.2 Ekonomiska konsekvenser

Bedömning: Det är synnerligen svårt att beräkna vilket resursbehov som våra förslag kan antas medföra. Det framstår emellertid som uppenbart att ökade resursbehov som inte ryms inom befintlig anslagsram kommer att uppstå hos Polismyndigheten, Åklagarmyndigheten, Ekobrottsmyndigheten, Tullverket och Säkerhets- och integritetsskyddsnämnden. Ett genomförande av våra förslag kräver att det tillskjuts medel till rättsväsendet från andra utgiftsområden.

De ökade resursbehov som kan förväntas uppkomma inom Säkerhetspolisen respektive Sveriges domstolar torde rymmas inom ram.

Skälen för bedömningen

Säkra prognoser kan inte göras

Det måste redan inledningsvis framhållas att det är synnerligen svårt att med någon träffsäkerhet beräkna vilket resursbehov som våra förslag kan antas medföra. Behoven beror på ett antal olika parametrar, däribland brottslighetens utveckling, den tekniska utvecklingen, hur den brottsbekämpande verksamheten organiseras och resurser utnyttjas, m.m. Det är troligt att tillämpningen av de nya reglerna kommer att öka allt eftersom och att detta kommer att medföra ökade resursbehov i framtiden. De utökade möjligheterna att använda hemliga tvångsmedel förväntas leda till att fler brott kan utredas och lagföras. Om möjligheterna innebär att man kan komma framåt i utredningar om brott som man tidigare inte kunnat utreda, t.ex. för att det inte gått att få fram en skäligen misstänkt, kan det innebära en ökad resursåtgång. Samtidigt kan möjligheterna leda till en effektivisering av det brottsutredande arbetet, vilket kan leda till en besparing av andra kostnadsdrivande utredningsresurser.

Det bör vidare framhållas att användningen av hemliga tvångsmedel i hög grad är kopplad till vilka resurser som finns tillgängliga, eftersom det i många fall är resurskrävande att använda hemliga tvångsmedel. Det kan krävas omfattande förberedelser för att hemliga tvångsmedel över huvud taget ska kunna användas effektivt i ett visst ärende. Arbetet med att gå igenom och analysera det material som man får tillgång till kan dessutom vara mycket tidskrävande och kräva särskild kompetens. Av detta följer att en utökning av de rättsliga möjligheterna att använda hemliga tvångsmedel inte automatiskt innebär att den faktiska användningen ökar i motsvarande mån. Detta förutsätter att de brottsbekämpande myndigheterna har tillräckliga resurser för detta. Om rättsväsendet inte ges tillräckliga resurser för att använda de nya möjligheterna kommer de inte att kunna tillämpas fullt ut och då inte heller ge de effekter som är avsedda.

Vi vill framhålla att nedanstående beräkningar, som vi tagit fram med hjälp av respektive myndighet, endast utgör grova uppskattningar av kommande resursbehov. Det är också sannolikt att behovet av resursökningar är något lägre initialt bl.a. eftersom det kan ta viss tid att få de personalförstärkningar som behövs.

Polismyndigheten

Polismyndigheten har uppskattat det ökade resursbehovet på central nivå till 15–20 årsarbetskrafter. Av dessa avser 5 årsarbetskrafter Samordnad teknisk inhämtning (STI) som ansvarar för att samordna inhämtningen av data för att kunna verkställa hemliga tvångsmedel samt administrera avlyssning av elektronisk kommunikation medräknat hemlig dataavläsning. STI servar även Tullverket och Säkerhetspolisen, som även bidrar till finansieringen. I uppskattningen ingår vidare 10–15 årsarbetskrafter som enligt Polismyndigheten behöver tillföras den centrala funktion där viss teknisk verkställighet utförs samt informationen analyseras och förs till utredningsärenden (Spaningssektionen inom Nationella operativa avdelningen).

När det gäller behoven och konsekvenserna i nästa led – alltså för den utredande verksamheten – har Polismyndigheten angett att dessa är betydligt svårare att uppskatta och anfört följande.

Svårigheterna är inte minst kopplade till förslaget om straffvärdeventiler för viss flerfaldig brottslighet, vilket kommer att leda till att vissa brottstyper som i dag sällan eller aldrig kan leda till hemliga tvångsmedel kan komma att omfattas. Ett exempel är systematiska vishingbedrägerier och stölder av stöldligor. Ett annat exempel är internetrelaterade sexualbrott mot barn och barnpornografibrott där vi föreslår nya eller kraftigt utökade möjligheter att använda hemliga tvångsmedel. Mot bakgrund av att förslagen innebär att flera i sammanhanget nya ärendetyper kommer att vara aktuella för användning av hemliga tvångsmedel kommer Polismyndigheten när tvångsmedlen är på plats behöva analysera närmare hur dessa ärendetyper ska allokeras organisatoriskt och även vilken bemanning de förutsätter. De sju polisregionerna kan komma att fördela ärendetyper till olika nivåer i den regionala organisationen. Vissa av förändringarna medför att vissa typer av ärenden bör bli lättare att utreda på ett resurseffektivt sätt medan andra att ärenden som tidigare kanske inte gått att utreda nu kommer kunna utredas och då behöva tilldelas utrednings- och analysresurser. Det faktiska utfallet är beroende av flera olika faktorer såsom

– hur många brott av det slag som enligt förslagen ska kunna leda till hemliga tvångsmedel som faktiskt begås och som kommer till polisens kännedom,
– vilka ärenden som bedöms vara lämpade för hemliga tvångsmedel,

– vilka ärenden som sedan åklagare beslutar att ansöka om hemliga tvångsmedel i,
– hur komplicerade ärendena är,
– vilken kringresurs, utöver utredare, i form av analytiker och spaningspersonal som behövs, och
– hur många personer det finns att misstänka i respektive ärende.

Den beskrivna komplexiteten innebär att det ökade resursbehovet inte kan bedömas med någon precision. Polismyndigheten har mycket grovt uppskattat att myndighetens behov kan förväntas öka med cirka 175–200 årsarbetskrafter. Den årliga kostnaden för flertalet av dessa årsarbetskrafter är cirka 0,7 miljoner kronor per person medan den för omkring 10 personer är något högre. Detta motsvarar ett ökat resursbehov, grovt uppskattat, på 120 till 140 miljoner kronor per år.

Till detta kommer kostnaden för ersättning till teleoperatörer. Under 2021 var kostnaden avseende hemlig övervakning av elektronisk kommunikation, hemlig avlyssning av elektronisk kommunikation som avser historiska uppgifter och inhämtning enligt inhämtningslagen totalt 13,3 miljoner kronor. En ökning kan beräknas till mellan 10 och 20 procent eller cirka 1,3–2,6 miljoner kronor[1]. När det gäller realtidsuppkoppling inom ramen för en hemlig avlyssning av elektronisk kommunikation belastar kostnaden STI. Kostnaden var 30 miljoner kronor för 2021 och den kostnaden kan antas öka mellan 10 och 20 procent eller 3–6 miljoner kronor per år.

Den ökade kostnaden torde inte rymmas inte inom befintlig anslagsram för Polismyndigheten.

Åklagarmyndigheten

Åklagarmyndigheten bedömer att våra lagförslag kommer att leda till fler arbetsuppgifter och därmed ökade behov av både åklagarresurser och administrativa resurser. En del av resursökningen på åklagarsidan kommer att avse den rent administrativa hanteringen av de utökade möjligheterna att använda hemliga tvångsmedel som blir följden av förslagen. I detta ingår att förbereda ansökningar och sammanträden i frågor om tillstånd och ökad hantering av de s.k. efter-

[1] Observera dock att en del av kostnaden avser inhämtningslagen, som vi inte föreslår ändringar i.

processerna. Den hanteringen medför även utökat behov av stöd från den operativa administrativa sidan. Med de nya bestämmelserna ökar komplexiteten i lagstiftningen, vilket kräver mer arbete med frågor om hemliga tvångsmedel generellt, bl.a. i utbildningshänseende för både administratörer och åklagare.

De föreslagna bestämmelserna bedöms skapa nya och bättre förutsättningar i utredningsarbetet. Som exempel kan tas den föreslagna straffvärdeventilen för flerfaldig brottslighet av systematisk eller organiserad art. Som angetts tidigare bedöms den medföra att fler fall av exempelvis stöldligor eller vishingbedrägerier går att utreda, vilket i sin tur kräver att mer tid får läggas av åklagare att leda förundersökningar i dessa ärendetyper och sedan lagföra brotten. Behovet av ökade resurser för detta ytterligare utrednings- och lagföringsarbete är också svårt att beräkna. Ett enda stort ärende som blir möjligt att driva och utreda på grund av de aktuella lagändringarna kan i praktiken ge merarbete för en åklagare under flera månader på heltid.

Åklagarmyndigheten har grovt uppskattat att det ökade resursbehovet motsvarar cirka 10 administratörer och cirka 15–20 åklagare på helårsbasis. Lönekostnaden för en administratör kan beräknas till cirka 0,8 miljoner kronor och för en åklagare cirka 1 miljon kronor. Det innebär en ökad kostnad för Åklagarmyndigheten med uppemot 30 miljoner kronor per år. Denna ökade kostnad bedöms inte rymmas inom befintlig anslagsram.

Ekobrottsmyndigheten

Ekobrottsmyndigheten har i fråga om utredning och lagföring gjort samma bedömning som Åklagarmyndigheten av hur de ökade möjligheterna att använda hemliga tvångsmedel kommer påverka verksamheten. För Ekobrottsmyndighetens del antas det uppstå ett behov av tillkommande resurser motsvarande 3 åklagartjänster, 2 administratörstjänster och 9 utredartjänster. I begreppet utredartjänst ingår it-forensiker och analytiker. Kostnaden per yrkesgrupp kan beräknas till cirka 4 miljoner kronor för åklagare, cirka 1,5 miljoner kronor för administratörer och cirka 8 miljoner kronor för utredare. Till detta kommer kostnader för ny it-utrustning och licenser för programvara. Sammanlagd kostnad uppskattas cirka 15 miljoner kronor per år.

Vad gäller avlyssning och spaning görs bedömningen att lagförslagen kommer innebära en absolut ökning av ärenden om hemliga tvångsmedel, främst vad gäller hemlig avlyssning av elektronisk kommunikation inklusive hemlig dataavläsning. Detta kommer innebära en ökad resursåtgång avseende såväl avlyssningspersonal som spaningspersonal. Här antas ett behov av tillkommande resurser motsvarande tre till fyra tjänster. Även här kommer viss ny it-utrustning krävas samt troligen vissa utbildningsinsatser. Kostnaden för detta kan beräknas till 3 till 4 miljoner kronor.

Totalt uppskattas grovt ett ökat resursbehov för Ekobrottsmyndigheten till uppemot 20 miljoner kronor per år. Denna ökade kostnad bedöms inte rymmas inte inom befintlig anslagsram.

Tullverket

Tullverket har uppskattat att våra förslag föranleder behov av ett tillskott av 4–8 årsarbetskrafter till Tullverkets nationella operativa central för hemliga tvångsmedel och 6–12 årsarbetskrafter till tekniska verkställigheter. På utredningssidan (utredare och analytiker) har Tullverket uppskattat behovet till 21–28 årsarbetskrafter. En årsarbetskraft beräknas till 1,034 miljoner kronor. Vidare gör man likt Polismyndigheten bedömningen att verkställighetskostnaderna kommer att öka med 10 till 20 procent. Tullverkets årliga kostnad är i nuläget cirka 4 miljoner. Det totala ökade resursbehovet uppskattas grovt till uppemot 50 miljoner kronor. Denna ökade kostnad bedöms inte rymmas inom befintlig anslagsram.

Säkerhetspolisen

Säkerhetspolisen har bedömt att de ökade resursbehov som förslagen kan medföra ryms inom befintlig anslagsram.

Ökade kostnader för Säkerhets- och integritetsskyddsnämnden

Våra förslag förväntas leda till fler tillstånd till hemliga tvångsmedel och fler interimistiska åklagarbeslut. Säkerhets- och integritetsskyddsnämnden (SIN) får därför en ökad arbetsbelastning. SIN bedömer

att våra förslag medför behov av en extra årsarbetskraft. Kostnaden för det kan beräknas till 1 miljon kronor. Kostnaden bedöms inte rymmas inom anslagsramen.

Ökade kostnader för Sveriges domstolar och anslaget Rättsliga biträden m.m.

Ärenden om hemliga tvångsmedel under en förundersökning ska alltid prövas av domstol. Våra förslag förväntas medföra en ökning av antalet ärenden hos de allmänna domstolarna. Det är inte möjligt att göra någon säker prognos av hur stor ökningen av antalet ärenden kan komma att bli, men vi uppskattar grovt att det kan bli fråga om en total ökning av antalet ärenden med 10–20 procent. Det är dock förenat med betydande svårigheter att omsätta detta i siffror, eftersom det inte förs någon statistik över vare sig antalet ärenden, tidsåtgång, antal sammanträden eller kostnaden för offentliga ombud.

Uppgifter från domstolar ger vid handen att det vid de domstolar som hanterar flest ärenden om hemliga tvångsmedel krävs omkring en halv årsarbetskraft för en domare och detsamma för en domstolshandläggare för denna handläggning. För flertalet domstolar är arbetskraftsbehovet för ifrågavarande ärenden väsentligt lägre. Den ökning av antalet ärenden som kan antas uppkomma om våra förslag genomförs innebär inte någon väsentlig ökning av arbetskraftsbehovet för själva handläggningen av ärendena. Det bör dock framhållas att en ökning av antalet ärenden medför ytterligare svårigheter i planeringen av domstolarnas verksamhet. Detta kan i sig skapa ytterligare resursbehov.

Våra förslag medför vidare att offentliga ombud kommer att tas i anspråk i fler ärenden än i dag. Det har inte varit möjligt att få fram någon siffra för storleken av denna kostnad i dag men vi utgår från att våra förslag inte medför någon betydande kostnadsökning för anslaget Rättsliga biträden m.m.

Mot bakgrund av den information vi har fått om det ekonomiska läget för Sveriges Domstolar utgår vi från att det ökade resursbehovet för närvarande kan rymmas inom den befintliga anslagsramen och likaså att utgifterna för offentliga ombud ryms inom anslaget för Rättsliga biträden m.m.

Inga ökade kostnader för företag som medverkar vid verkställighet

Våra förslag kan förväntas innebära en ökad arbetsbörda för de företag som på olika sätt är skyldiga att medverka vid verkställighet av hemliga tvångsmedel. Den som är skyldig att lagra uppgifter enligt 16 a § LEK har enligt 16 e och 22 § rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna. Närmare bestämmelser finns i Post- och telestyrelsens föreskrifter om ersättning vid utlämnande av uppgifter som lagras eller bevaras för brottsbekämpande ändamål (PTSFS 2021:5). Där anges bl.a. vilka belopp som ska betalas vid utlämnande av olika kategorier av uppgifter.

En skyldighet för operatörer att medverka vid verkställighet följer även av 24 § lagen om hemlig dataavläsning. Aktörerna är även i dessa fall berättigade till ersättning av den verkställande myndigheten för kostnader som uppstår till följd av medverkan. Närmare bestämmelser finns i Post- och telestyrelsens föreskrifter om ersättning vid medverkan i samband med verkställighet av hemlig dataavläsning (PTSFS 2021:6).

Med hänsyn till myndigheternas ersättningsskyldighet bedöms förslagen vara kostnadsneutrala för operatörerna. Däremot uppstår ökade kostnader för den brottsbekämpande myndighet som ska betala operatören. Dessa kostnader ingår i den bedömning som nämns ovan beträffande de brottsbekämpande myndigheterna.

Kriminalvården

Våra förslag förväntas leda till en ökad lagföring avseende allvarlig brottslighet. Detta kommer att innebära en ökad belastning för Kriminalvården. Det är i dagsläget inte möjligt att göra någon bedömning av vilken resursökning som kan bli aktuell.

Finansiering

Som framgått kommer i vart fall Polismyndigheten, Åklagarmyndigheten, Tullverket och Ekobrottsmyndigheten samt SIN att behöva ökade resurser om våra förslag ska få genomslag. Ett genomförande av våra förslag kräver därför att det tillskjuts medel till rättsväsendet från andra utgiftsområden.

17.3 Konsekvenserna för brottsligheten och det brottsförebyggande arbetet

Bedömning: Förslagen kommer att bidra till att fler brott kommer att kunna utredas och till effektivare utredningar. Därigenom kommer fler personer att kunna lagföras för brott. Detta förväntas bidra till att färre brott begås.

Skälen för bedömningen

Vi bedömer att våra förslag både sedda för sig och sammantagna kommer att medföra påtagliga förbättringar när det gäller möjligheterna att utreda allvarlig brottslighet och få till stånd en lagföring.

Förslagen bedöms vidare ge bättre förutsättningar för internationellt rättsligt samarbete, inte minst när det gäller cyberbrott.

Till stor del syftar förslagen till att möta utmaningar som uppstått till följd av brottslighetens utveckling, den tekniska utvecklingen, minskad vilja hos allmänheten att medverka i brottsutredningar och riskmedvetet beteende hos kriminella. Förbättrade utredningsmöjligheter innebär att risken för den enskilde brottslingen att bli avslöjad och lagförd ökar. Detta kan också bidra till att färre brott begås.

17.4 Övriga konsekvenser enligt kommittéförordningen

Bedömning: Våra förslag medför inte några av de övriga konsekvenser som ska redovisas enligt kommittéförordningen, bl.a. för sysselsättningen eller för jämställdheten mellan kvinnor och män.

Skälen för bedömningen

Vår bedömning är att det inte kan förväntas uppstå några andra konsekvenser av det slag som avses i kommittéförordningen.

18 Författningskommentar

Inledning

I den mån lagändringar har föreslagits i prop. 2021/22:119 Modernare regler för användningen av tvångsmedel eller prop. 2021/22:133 En samlad straffrättslig terrorismlagstiftning utgår våra förslag från den lydelse som föreslås i respektive proposition.

18.1 Förslaget till lag om ändring i rättegångsbalken

27 kap.

18 §

Paragrafen innehåller en definition av tvångsmedlet hemlig avlyssning av elektronisk kommunikation och anger när tvångsmedlet får användas under en förundersökning.

I *andra stycket* görs ett tillägg som upplyser om den nya bestämmelsen i 18 a § som begränsar möjligheterna att använda hemlig avlyssning av elektronisk information i syfte att utreda vem som skäligen kan misstänkas för brottet. Genom införande av *punkterna 2–4, 7–9, 12 och 13 i andra stycket* införs en möjlighet att använda hemlig avlyssning av elektronisk kommunikation vid utredning av vissa ytterligare brott, som räknas upp i punkterna. Förslaget har behandlats i avsnitt 7.4. Införande av de nya punkterna föranleder en ändrad numrering i punktlistan.

Andra stycket sextonde punkten, som har behandlats i avsnitt 7.4, motsvarar i huvudsak åttonde punkten enligt lydelsen i prop. 2021/22:119 Modernare regler för användningen av tvångsmedel. Bestämmelsen innebär att hemlig avlyssning kan ske även vid misstanke om försök,

förberedelse eller stämpling till något av brotten i paragrafens brottskatalog förutsatt att gärningen är straffbelagd.

Genom en ny *artonde punkt i andra stycket* införs en ny straffvärdeventil för viss flerfaldig brottslighet. Förslaget har behandlats i avsnitt 6.5–6.7 och 6.10–6.14. Bestämmelsen innebär att det kan fattas ett beslut om hemlig avlyssning av elektronisk kommunikation även vid förundersökningar om viss flerfaldig brottslighet, fastän de brott som ingår i den misstänkta brottsligheten inte vart och ett för sig kan föranleda ett sådant beslut. En grundförutsättning för att bestämmelsen ska kunna tillämpas är att det samlade straffvärdet för brottsligheten kan antas överstiga fängelse i två år. Bedömningen av det samlade straffvärdet ska avse den brottslighet som ligger till grund för förundersökningen. De sammanlagda brottsmisstankarna ska avse den skäligen misstänkte. Det är alltså inte tillåtet att lägga samman brottsmisstankar mot flera personer och lägga dessa till grund för ett beslut om hemlig avlyssning, även om personerna skulle ingå i samma kriminella organisation (se vidare nedan om kravet på att det ska kunna antas att brottsligheten ska ha utövats i organiserad form eller systematiskt).

Det samlade straffvärdet bedöms i enlighet med de principer som utvecklats i praxis, se bl.a. NJA 2008 s. 359. Faktorer som inverkar höjande eller sänkande på straffvärdet ska beaktas i den mån de är kända. Däremot beaktas inte sådana faktorer som särskilt beaktas vid straffmätningen, såsom att den misstänkte tidigare gjort sig skyldig till brott eller inte har fyllt 21 år. Liksom när det gäller den hittills gällande straffvärdeventilen får det bedömas om de omständigheter som föreligger är tillräckliga för ett antagande om att det samlade straffvärdet överstiger fängelse i två år. Varje eventuell osäkerhet, t.ex. vid bedömningen av straffvärdet för något av de brott som ingår i sammanläggningen, ska tillgodoräknas den misstänkte. Vid beräkningen av det samlade straffvärdet får man endast beakta brott för vilka det är föreskrivet fängelse i ett år eller däröver, dvs. häktningsgrundande brott. Om ett häktningsgrundande brott inte fullbordats kan dock även försök, förberedelse eller stämpling till brottet räknas in förutsatt att en sådan gärning är straffbelagd.

För att den nya straffvärdeventilen ska kunna tillämpas krävs vidare att det kan antas att brottsligheten har utövats systematiskt eller i organiserad form. Med brottslighet som utövats i organiserad form avses brottslighet som har begåtts inom ramen för en struktur där

flera personer har samverkat under en inte helt obetydlig tid för att begå brott. Det är inte tillräckligt att det aktuella brottet har skett i samverkan. Personerna ska kunna antas ha ingått i en sammanslutning eller ett nätverk av viss kontinuitet vars syfte att begå brott sträckt sig längre än till enbart det ifrågavarande brottet. Det är inte nödvändigt att den misstänkte är den person som organiserat brottsligheten. Straffvärdeventilen kan alltså tillämpas även mot personer längre ner i den kriminella organisationen, förutsatt att villkoren i fråga om det samlade straffvärdet och de ingående brottens straffskala är uppfyllda. Uttrycket ”kan antas” betyder att det ska föreligga en mindre sannolikhetsöversikt för att antagandet är riktigt.

För att en brottslighet ska anses ha utövats systematiskt krävs att ett visst tillvägagångssätt har upprepats ett flertal gånger av antingen en ensam gärningsman eller av flera personer i samförstånd. Ett exempel kan vara att man upprepade gånger kontaktar enskilda i syfte att få tillgång till personens BankID och använder uppgifterna för att tillgodogöra sig medel på personens bankkonto. Ett annat exempel kan vara att man upprepade gånger smugglar in varor i landet eller begår punktskattebrott med ett liknande tillvägagångssätt. Förutsatt att tillvägagångssättet är likartat från gång till annan kan brottsligheten i ett sådant fall anses ha utövats systematiskt. Inget hindrar att brott med olika rubricering läggs samman, förutsatt att de ingår i den systematiska brottsligheten. Ett exempel kan vara ett förfarande som består i systematiska skattebrott och bokföringsbrott, eller systematiskt bedrägeri som begås med hjälp av olovlig identitetsanvändning

De brott som omfattas av sammanläggningen ska kunna antas ha utgjort ett led i den organiserade eller systematiska brottsligheten, vilket innebär att det kan antas att varje ingående brott ska ha haft ett naturligt samband med brottsligheten. Om en person misstänks för dels flera brott som utövats systematiskt eller i organiserad form, dels något brott som inte ingår i den brottsligheten, ska det sistnämnda brottet inte räknas in i sammanläggningen. Däremot hindrar ingenting att hemlig avlyssning används i fråga om det brottet förutsatt att detta är tillåtet på någon annan grund, t.ex. för att det har ett minimistraff på två års fängelse eller däröver.

En särskild situation kan uppstå om det i en systematisk eller organiserad brottslighet ingår dels brott som i sig själva kan leda till hemlig avlyssning, antingen på grund av att de har ett minimistraff på lägst två års fängelse eller ett straffvärde som överstiger två års

fängelse, dels andra brott. I dessa fall får alla de angivna brotten räknas in i sammanläggningen, förutsatt att villkoren för detta i övrigt är uppfyllda.

Eftersom det är fråga om användning av ett mycket integritetskänsligt tvångsmedel bör även den nya straffvärdeventilen tillämpas restriktivt (jfr prop. 2002/03:74 s. 48).

Övriga ändringar i paragrafen är endast redaktionella.

18 a §

I paragrafen, som är ny, finns bestämmelser som begränsar tillämpningsområdet för möjligheten enligt 20 § tredje stycket att vidta hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet. Övervägandena finns i avsnitt 9.10.2–9.10.4.

Av *första stycket första punkten* framgår utgångspunkten att hemlig avlyssning i de angivna fallen endast får användas för brott eller brottslighet som kan leda till hemlig rumsavlyssning. Det följer av bestämmelsen i 20 d andra stycket att hemlig rumsavlyssning kan förekomma även vid försök, förberedelse eller stämpling. Huvudregeln kompletteras med en brottskatalog i *andra till åttonde punkterna.* Brotten i första styckets brottskatalog är sådana som kan leda till hemlig avlyssning av elektronisk kommunikation antingen på den grunden att straffskalan börjar på lägst två års fängelse eller att de räknas upp i brottskatalogen i 18 § andra stycket. Det finns här en viss överlappning när det gäller spionerі, som regleras både i 20 d § andra stycket 2 och i 18 § andra stycket 11 och även när det gäller företagsspionerі enligt 26 § lagen (2018:558) om företagshemligheter. Av *nionde punkten* följer att hemlig avlyssning i det nu aktuella syftet får användas även vid försök, förberedelse eller stämpling avseende brotten i andra till åttonde punkten, förutsatt att en sådan gärning är straffbelagd.

Av *andra stycket* följer att hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas kan användas även i fråga om vissa brott som inte har ett minimistraff på fängelse i två år eller mer och som inte heller räknas upp i brottskatalogen i 18 § andra stycket. Brotten räknas upp i en brottskatalog i *första till tredje punkterna.* För att hemlig avlyssning ska kunna användas för dessa brott krävs det att någon av straffvärdeventilerna

i 18 § andra stycket är tillämpliga. Om det är fråga om ett enstaka brott innebär detta krav att straffvärdet ska kunna antas överstiga två års fängelse (18 § andra stycket 17). Vid flerfaldig brottslighet kan hemlig avlyssning användas om den samlade brottsligheten kan antas ha ett sammanlagt straffvärde överstigande fängelse i två år, och övriga förutsättningar för tillämpning av straffvärdeventilen i 18 § andra stycket 18 är uppfyllda. Det är inte nödvändigt att alla de sammanlagda brotten finns med i katalogen, utan det är tillräckligt att något av dem räknas upp och att brottsligheten sammantagen är sådan att hemlig avlyssning av elektronisk kommunikation hade varit tillåten om det hade funnits en skäligen misstänkt. När det gäller grovt bedrägeri, som anges i *andra punkten*, är tillämpningen begränsad till fall då bedrägeriet begåtts med hjälp av elektronisk kommunikation. Innebörden är att elektronisk kommunikation ska ha varit ett verktyg för att begå brottet eller att elektronisk kommunikation har använts för att understödja brottet. Ett exempel kan vara att en okänd gärningsperson ringer upp ett antal målsägande i syfte att förmå dem att lämna ut sitt digitala BankID, för att sedan med hjälp av detta kunna få tillgång till medel på målsägandens bankkonto. En annan situation kan vara att en första kontakt tas med en målsägande per telefon och att gärningspersonen sedan vid ett fysiskt möte fullbordar brottet genom att exempelvis lura till sig målsägandens bankomatkort. Enligt *fjärde punkten* krävs det inte att brottet har fullbordats utan det är tillräckligt att det är fråga om försök, förberedelse eller stämpling, förutsatt att en sådan gärning är straffbelagd.

Som framgått av kommentaren till 18 § andra stycket ska brottsmisstankarna avse en viss person, i den bemärkelsen att man inte kan lägga ihop brottsmisstankar som riktar sig mot flera. Det sagda innebär inte att det krävs att det är visat att en och samma person begått gärningarna. Det som krävs är att det finns konkreta omständigheter som talar för att brotten begås av en person eller av flera personer gemensamt och i samförstånd.

19 §

Paragrafen innehåller en definition av tvångsmedlet hemlig övervakning av elektronisk kommunikation och anger när tvångsmedlet får användas under en förundersökning. Övervägandena finns i avsnitt 6.15 och 7.4.

I *tredje stycket* görs ett tillägg som upplyser om den nya bestämmelsen i 19 a § som delvis motsvarar tidigare 19 § fjärde stycket. Brottskatalogen i *tredje stycket andra punkten* ändras på så sätt att barnpornografibrottet tas bort till följd av att brottet lagts till i brottskatalogen för hemlig avlyssning av elektronisk kommunikation i 18 §. I *tredje punkten* görs tillägg som klargör att alla brott och all brottslighet som enligt 18 § andra stycket 2–18 kan leda till hemlig avlyssning av elektronisk kommunikation även kan leda till hemlig övervakning av elektronisk kommunikation. Härigenom klargörs det att ett beslut om hemlig övervakning alltid kan fattas i fråga om sådana brott och sådan brottslighet oberoende av om det samtidigt fattas ett beslut om hemlig avlyssning.

Bestämmelsen i *fjärde stycket* flyttas till en ny 19 a §.

19 a §

Paragrafen, som är ny, motsvarar delvis tidigare 19 § fjärde stycket. Förslaget har behandlats i avsnitt 6.5–6.7 och 6.9–6.14.

Bestämmelsen skiljer sig från 19 § fjärde stycket genom ett tillägg som klargör att hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet får ske inte bara när det enstaka brottet är sådant att det kan leda till hemlig avlyssning av elektronisk kommunikation utan även när den samlade brottsligheten kan föranleda beslut om hemlig avlyssning med stöd av den nya straffvärdeventilen för flerfaldig brottslighet i 18 § andra stycket 18. Som framgått av kommentaren till 18 § andra stycket ska brottsmisstankarna avse en viss person, i den bemärkelsen att man inte kan lägga ihop brottsmisstankar som riktar sig mot flera. Det sagda innebär inte att det krävs att det är visat att en och samma person begått gärningarna. Det som krävs är att det finns konkreta omständigheter som talar för att brotten begås av en person eller av flera personer gemensamt och i samförstånd.

20 §

I paragrafen anges när hemlig avlyssning och hemlig övervakning av elektronisk kommunikation får ske under en förundersökning och vilka telefonnummer, andra adresser eller kommunikationsutrustningar som åtgärden får avse.

Huvudregeln är att hemlig avlyssning och hemlig övervakning av elektronisk kommunikation endast får ske när det finns en skäligen misstänkt, och då enbart i förhållande till telefonnummer, andra adresser eller kommunikationsadresser som på visst angivet sätt har en koppling till den skäligen misstänkte. Undantag görs från denna huvudregel i andra stycket och en ny bestämmelse i tredje stycket. *Första stycket* ändras endast på så sätt att det förs in en hänvisning till den nya bestämmelsen i tredje stycket.

I *andra stycket* finns bestämmelser som gör det möjligt att i vissa fall använda hemlig övervakning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet. Bestämmelsen är, med hänsyn till syftet med den, inte begränsad till någon viss personkrets. Användningsområdet begränsas i stället genom kravet på att åtgärden ska vara av synnerlig vikt för utredningen i det konkreta fallet. Ändringen i stycket innebär att det blir tillåtet att hämta in uppgifter om meddelanden i realtid även när syftet är att utreda vem som skäligen kan misstänkas. Övervägandena till denna ändring finns i avsnitt 7.5 och 8.5, 8.7 och 8.8.

I *tredje stycket* införs en möjlighet att tillgripa även hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet. Övervägandena finns i avsnitt 9.4–9.6 och 9.8–9.10. I likhet med vad som gäller i fråga om hemlig övervakning enligt andra stycket krävs det att åtgärden är av synnerlig vikt för utredningen. Vidare krävs att brottet eller brottsligheten är sådan som avses i 18 a §. Till skillnad från vad som gäller i fråga om hemlig övervakning enligt andra stycket är åtgärden begränsad till att avse de telefonnummer, andra adresser eller kommunikationsutrustningar som närmare anges i stycket.

Enligt *första punkten* får åtgärden endast avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som under den tid som tillståndet avser kan antas innehas eller ha innehafts av någon som kan misstänkas ha begått eller annars medverkat till brottet eller annars kan antas ha använts eller kan komma

att användas av en sådan person. Uttrycket ”kan misstänkas” innebär ett krav på en låg misstankegrad. Det krävs inte att personen är identifierad, utan endast att det kan antas att det nummer, den adress eller den kommunikationsutrustning som avlyssnas kan antas ha koppling av det angivna slaget till någon person som kan misstänkas för inblandning i brottet. Ett exempel kan vara en utredning om människorov där det är känt att kidnapparna kontaktar den frihetsberövades anhöriga från ett visst telefonnummer. Ett annat exempel kan vara att utredningen ger vid handen att brott begås med hjälp av en viss elektronisk kommunikationsutrustning, men att den person som använder eller innehar utrustningen inte är identifierad. Bestämmelsen omfattar inte bara den som kan misstänkas vara gärningsman, utan även någon som kan misstänkas för någon annan form av medverkan.

Av *andra punkten* följer att hemlig avlyssning i det nu aktuella syftet även får avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att någon som kan misstänkas ha begått eller medverkat till brottet har kontaktat eller kommer att kontakta under den tid som tillståndet avser. Uttrycket ”någon som kan misstänkas ha begått eller annars medverkat till brottet” har här samma innebörd som i första punkten. Innebörden av kravet på ”synnerlig anledning att anta” är densamma som enligt första stycket andra punkten.

Det kan många gånger finnas anledning att förena ett tillstånd till hemlig avlyssning enligt tredje stycket med villkor som syftar till att begränsa integritetsintrånget. Detta gäller i synnerhet tillstånd enligt andra punkten. Eftersom personen i fråga är okänd och tillståndet därför inte kan begränsas till enbart samtal där han eller hon deltar, behöver beslutsfattaren noga överväga hur sådana villkor kan ges en lämplig utformning.

Det följer av 23 § att åklagaren eller rätten är skyldig att omedelbart upphäva ett beslut om exempelvis hemlig avlyssning av elektronisk kommunikation om det inte längre finns skäl för beslutet. Av detta får anses följa en skyldighet att upphäva ett beslut om hemlig avlyssning av elektronisk kommunikation när ändamålet med åtgärden, dvs. att få fram vem eller vilka som skäligen kan misstänkas för brottet, är uppfyllt.

Övriga ändringar är endast redaktionella.

20 a §

Paragrafen innehåller en definition av tvångsmedlet hemlig kameraövervakning och anger när tvångsmedlet får användas under en förundersökning.

I *andra stycket andra punkten* görs en ändring som innebär att den utvidgning av brottskatalogen för hemlig avlyssning av elektronisk kommunikation som görs i 18 § andra stycket gäller även för hemlig kameraövervakning. Övervägandena finns i avsnitt 7.6.

Genom en ny *femte punkt i andra stycket* införs en ny straffvärdeventil för viss flerfaldig brottslighet. Förslaget har behandlats i avsnitt 6.5–6.7 och 6.9–6.14. Straffvärdeventilen har samma innebörd som i 18 § andra stycket 18, se vidare kommentaren till den bestämmelsen.

Eftersom det är fråga om användning av ett mycket integritetskänsligt tvångsmedel bör den nya straffvärdeventilen tillämpas restriktivt.

Hemlig kameraövervakning kan i vissa fall användas även om det inte finns någon som är skäligen misstänkt för brottet (20 c §). Det som sagts i kommentaren till 18 a § om principer för sammanläggning av flera brottsmisstankar gäller även i fråga om hemlig kameraövervakning.

Övriga ändringar i paragrafen är endast redaktionella.

20 b §

Paragrafen innehåller bestämmelser om förutsättningarna för att använda hemlig kameraövervakning.

Andra stycket ändras endast på så sätt att det införs en hänvisning till det nya tredje stycket.

Tredje stycket är nytt. Övervägandena finns i avsnitt 10.4–10.9. Genom bestämmelsen i stycket införs en möjlighet att knyta ett tillstånd till hemlig kameraövervakning till den skäligen misstänkte i stället för till en viss plats. Innebörden av den nya möjligheten är att det inte i beslutet måste anges en viss plats där åtgärden ska ske och att det ska anges att övervakningen avser den skäligen misstänkte. Bestämmelsen får tillämpas endast om det finns särskilda skäl. Sådana skäl föreligger om det saknas rimliga förutsättningar att få tillgång till de uppgifter som behövs i utredningen genom en hemlig kameraövervakning avseende en viss plats. Ett exempel på en sådan situation kan vara att den misstänkte är i rörelse på platser där det

inte är möjligt att bedriva fysisk spaning utan upptäckt, men att man kan följa den misstänkte med hjälp av kameror.

Inget hindrar att man vid samma tillfälle meddelar tillstånd till övervakning av såväl en viss plats som övervakning som avser den skäligen misstänkte, om det även finns förutsättningar för det. Man kan t.ex. tänka sig att tillstånd ges för dels kameraövervakning i den misstänktes trapphus för att man ska kunna se vem som besöker dennes bostad, dels för att man ska kunna följa den misstänkte med kameror när denne rör sig utomhus.

Åtgärden får endast verkställas på så sätt att den riktas mot en plats där den misstänkte kan antas komma att uppehålla sig. Med uttrycket ”riktas mot” avses den plats som avbildas med hjälp av kamerorna. Kravet på att det kan antas att den misstänkte kommer att uppehålla sig på platsen har samma innebörd som i andra stycket.

Av sista meningen framgår att de tekniska hjälpmedel som används vid övervakningen inte får placeras på en plats som skyddas mot intrång. Med detta avses samma slags intrångsskyddade platser som avses i 25 a §. Om inte något annat följer av de villkor som gäller för tillståndet och det bedöms proportionerligt är det dock tillåtet att rikta övervakningen mot en intrångsskyddad plats. Det är alltså möjligt att från luften eller med en kamera som anbringas på en allmän plats kameraövervaka det som sker på exempelvis en intrångsskyddad tomt eller i en bostad.

När ett tillstånd meddelas med stöd av tredje stycket är det obligatoriskt att meddela villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Eftersom tillståndet inte är begränsat till en viss plats måste det ställas höga krav på villkorens utformning. Dessa bör vara formulerade så att kameraövervakningen är proportionerlig och i övrigt godtagbar oavsett var åtgärden sedermera kommer att verkställas. I normalfallet bör det i villkoren ges någon form av platsangivelse, låt vara att den kan vara brett formulerad. Om det t.ex. är känt att den misstänkte kommer att sammanträffa med en medmisstänkt någonstans inom en viss stadsdel bör det alltså anges. Andra villkor kan vara exempelvis att kameraövervakning bara får ske när det genom spaning eller på annat sätt kan konstateras att den misstänkte är på plats, agerar på ett visst sätt eller sammanträffar med någon viss person. I vissa fall kan det finnas skäl att föreskriva att utomstående inte får avbildas på ett sådant sätt att de kan identifieras. Se vidare i kommentaren till 21 §.

20 d §

Paragrafen innehåller en definition av tvångsmedlet hemlig rumsavlyssning och anger när tvångsmedlet får användas under en förundersökning.

Brottskatalogen i *andra stycket fjärde punkten* avskaffas. Ändringen innebär att straffvärdeventilen kan tillämpas oavsett brottsrubricering, förutsatt att brottet kan antas ha ett straffvärde som överstiger fängelse i fyra år. Övervägandena finns i avsnitt 6.9.

Genom en ny *femte punkt i andra stycket* införs en ny straffvärdeventil för viss flerfaldig brottslighet. Förslaget har behandlats i avsnitt 6.8–6.14. Bestämmelsen innebär att det kan fattas ett beslut om hemlig rumsavlyssning även vid förundersökningar om viss flerfaldig brottslighet, fastän de brott som ingår i den misstänkta brottsligheten inte vart och ett för sig kan föranleda ett sådant beslut. En grundförutsättning för att bestämmelsen ska kunna tillämpas är att det samlade straffvärdet för brottsligheten kan antas överstiga fängelse i fyra år. Bedömningen ska då avse den brottslighet som ligger till grund för förundersökningen. Det är inte tillåtet att lägga samman brottsmisstankar mot flera personer och lägga dessa till grund för ett beslut om hemlig rumsavlyssning, även om personerna skulle ingå i samma kriminella organisation (se vidare nedan om kravet på att brottsligheten ska ha utövats i organiserad form eller systematiskt).

Det samlade straffvärdet bedöms i enlighet med de principer som utvecklats i praxis, se bl.a. NJA 2008 s. 359. Faktorer som inverkar höjande eller sänkande på straffvärdet ska beaktas i den mån de är kända. Däremot beaktas inte sådana faktorer som särskilt beaktas vid straffmätningen, såsom att den misstänkte tidigare gjort sig skyldig till brott eller inte har fyllt 21 år. Liksom när det gäller den hittills gällande straffvärdeventilen får det bedömas om de omständigheter som föreligger är tillräckliga för ett antagande om att det samlade straffvärdet överstiger fängelse i fyra år. Varje eventuell osäkerhet, t.ex. vid bedömningen av straffvärdet för något av de brott som ingår i sammanläggningen, ska tillgodoräknas den misstänkte. Vid beräkningen av det samlade straffvärdet får man endast beakta brott med ett minimistraff i straffskalan om sex månaders fängelse eller mer. Om ett sådant brott inte fullbordats kan dock även försök, förberedelse eller stämpling till brottet räknas in, förutsatt att en sådan gärning är straffbelagd. I praktiken kan det dock förväntas vara relativt

sällsynt att osjälvständiga brottsformer har ett så högt straffvärde att de ger något större utslag vid sammanläggningen.

För att bestämmelsen ska kunna tillämpas krävs vidare att de ingående brotten kan antas vara ett led i en brottslighet som kan antas ha utövats systematiskt eller i organiserad form, se vidare i kommentaren till 18 § andra stycket 18.

Eftersom det är fråga om användning av ett mycket integritetskänsligt tvångsmedel bör den nya straffvärdeventilen tillämpas restriktivt.

Bestämmelsen i tidigare *sjätte punkten* utgår till följd av att brottskatalogen i fjärde punkten avskaffas. Osjälvständiga brottsformer omfattas utan att det behöver föreskrivas särskilt, under förutsättning att brottets straffvärde överstiger fängelse i fyra år och gärningen är straffbelagd.

Övriga ändringar i paragrafen är endast redaktionella.

20 e §

Paragrafen innehåller bestämmelser om förutsättningarna för att använda hemlig rumsavlyssning. Paragrafen ändras endast på så sätt att det i *andra stycket* tas in en hänvisning till den nya 20 f §. Övervägandena finns i avsnitt 10.4–10.9.

20 f §

Genom paragrafen, som är ny, införs en möjlighet att knyta ett tillstånd till hemlig rumsavlyssning till den skäligen misstänkte i stället för till en viss plats. Övervägandena finns i avsnitt 10.4–10.9.

Innebörden av den nya möjligheten är att det inte i beslutet måste anges en viss plats där åtgärden ska ske och att det ska anges att avlyssningen avser den skäligen misstänkte. Bestämmelsen får tillämpas endast om det finns särskilda skäl. Sådana skäl föreligger om det saknas rimliga förutsättningar att få tillgång till de uppgifter som behövs i utredningen genom en hemlig rumsavlyssning avseende en viss plats. Ett exempel kan vara att den misstänkte undviker att föra för utredningen intressanta samtal på sådana platser som kan avlyssnas, och i stället samtalar under promenader på olika platser. Inget hindrar att man vid samma tillfälle meddelar tillstånd till rumsavlyssning av såväl en viss plats som rumsavlyssning som avser den skäli-

gen misstänkte, om det även finns förutsättningar för det. Man kan t.ex. tänka sig att tillstånd ges för dels rumsavlyssning i den misstänktes bostad, dels för att man ska kunna avlyssna den misstänkte när denne rör sig utomhus.

Det gäller ett krav på att åtgärden endast får verkställas på så sätt att avlyssningen riktas mot en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Med orden ”riktas mot” avses den plats varifrån ljud fångas upp. Kravet på att det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig på platsen har samma innebörd som i 20 e § andra stycket. Ytterligare en begränsning gäller för att avlyssningen ska få riktas mot någon annan stadigvarande bostad än den misstänktes. I det fallet krävs att det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. Även detta krav har samma innebörd som i 20 e § andra stycket. Det är inte tillåtet att rikta avlyssningen mot sådana platser som avses i 20 e § tredje stycket.

Bestämmelsen innehåller även en begränsning när det gäller den plats där de tekniska hjälpmedel som används vid rumsavlyssningen får placeras. Av den framgår nämligen att de tekniska hjälpmedel som används vid övervakningen inte får placeras på en plats som skyddas mot intrång, dvs. sådana intrångsskyddade platser som avses i 25 a §. Om inte något annat följer av de villkor som gäller för tillståndet och det bedöms proportionerligt är det dock tillåtet att rikta avlyssningen mot en intrångsskyddad plats. Det är alltså tillåtet att med en avlyssningsutrustning som anbringas på en allmän plats avlyssna det som sker på exempelvis en intrångsskyddad tomt. De tekniska hjälpmedlen får aldrig placeras på en sådan plats som avses i 20 e § tredje stycket.

När ett tillstånd meddelas med stöd av paragrafen är det obligatoriskt att meddela villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Eftersom tillståndet inte är begränsat till en viss plats måste det ställas höga krav på villkorens utformning. Dessa bör vara formulerade så att rumsavlyssningen är proportionerlig och i övrigt godtagbar oavsett var åtgärden sedermera kommer att verkställas. I normalfallet bör det i villkoren ges någon form av platsangivelse, låt vara att den kan vara brett formulerad. Andra villkor kan vara exempelvis att rumsavlyssning bara får ske när det genom spaning eller på annat sätt kan konstateras att den misstänkte är på plats eller att ett visst möte äger rum.

21 §

Paragrafen innehåller bestämmelser dels om vem som ansöker om och fattar beslut om hemliga tvångsmedel enligt 27 kap., dels vad beslutet om att tillåta åtgärden ska innehålla.

Genom tillägget i f*örsta stycket* införs ett nytt åliggande för åklagaren i vissa fall. I de fall då beslutet knyts till den skäligen misstänkte i stället för en viss plats är åklagaren enligt bestämmelsen skyldig att i samband med ansökan till rätten föreslå de villkor som tillståndet ska förenas med. Förslaget kan tas in i själva ansökan eller i den promemoria som ges in till rätten. Övervägandena finns i avsnitt 10.7 och 10.9.

Fjärde stycket innehåller särskilda bestämmelser om innehållet i ett tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning. Genom tilläggen klargörs att kravet på angivande av en viss plats inte gäller om beslutet har fattats med stöd av 20 b § tredje stycket eller 20 f §. Vidare klargörs att det i sådana fall ska framgå av beslutet att tillståndet avser den skäligen misstänkte.

Tillägget i *sjätte stycket* innebär att det är obligatoriskt att förena ett tillstånd till hemlig kameraövervakning eller hemlig rumsavlyssning med villkor när beslutet har meddelats med stöd av 20 b § tredje stycket eller 20 f §.

21 a §

Paragrafen reglerar åklagarens möjligheter att meddela interimistiska beslut om hemliga tvångsmedel och tillträdestillstånd. Paragrafen innehåller också bestämmelser om förfarandet när ett sådant beslut har meddelats.

Ändringen i *första stycket* innebär att en interimistisk beslutanderätt – motsvarande den som gäller för bl.a. hemlig avlyssning av elektronisk kommunikation – införs även för hemlig rumsavlyssning och tillstånd för att installera utrustning för hemlig rumsavlyssning eller hemlig kameraövervakning (se vidare kommentaren till 25 a §). Övervägandena finns i avsnitt 11.5, 12.4 och 12.5.

Möjligheten till interimistiska beslut är avsedd att tillämpas endast i undantagsfall. Den bör framför allt användas vid de tidpunkter då det inte är möjligt med en domstolsprövning inom domstolarnas ordinarie öppettider eller inom jourdomstolssystemet. Emellertid kan

det även under domstolarnas öppettider finnas situationer där ett beslut behöver kunna fattas med sådan skyndsamhet att det kan befaras att ändamålet med åtgärden går förlorat om man inväntar domstolsprövning. Bestämmelsen är tänkt att kunna tillämpas även i sådana fall. Exempel på sådana situationer är att de brottsbekämpande myndigheterna med kort varsel får kännedom om ett möte som det är av synnerlig vikt för utredningen att kunna avlyssna.

25 a §

Paragrafen innehåller bestämmelser om tillträdestillstånd.

Ändringarna i *andra stycket* innebär att det införs en möjlighet att meddela tillträdestillstånd för enbart hemlig kameraövervakning. Kravet på att platsen även ska vara föremål för hemlig rumsavlyssning tas alltså bort. Övervägandena finns i avsnitt 12.4.

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

28 §

Paragrafen upphävs till följd av att det i rättegångsbalken införs en möjlighet till interimistiskt beslut om hemlig rumsavlyssning och hemlig dataavläsning avseende rumsavlyssningsuppgifter. Övervägandena finns i avsnitt 11.5 och 15.2.

18.3 Förslaget till lag om ändring i lagen (2000:562) om internationell rättslig hjälp i brottmål

4 kap.

27 §

Paragrafen innehåller bestämmelser om hemlig kameraövervakning av någon som befinner sig i Sverige.

Av bestämmelsen i *första stycket* följer att en åklagare kan fatta ett interimistiskt beslut om hemlig kameraövervakning under de förutsättningar som anges i 27 kap. 21 a § rättegångsbalken. Tillägget klargör att åklagaren då även får besluta om tillträdestillstånd, om ansökan innehåller en sådan begäran och förutsättningar finns för åtgärden. Övervägandena finns i avsnitt 12.4, 12.5 och 15.3.

28 a §

Paragrafen innehåller bestämmelser om hemlig rumsavlyssning av någon som befinner sig i Sverige.

Genom tillägget i *första stycket* införs det en möjlighet för åklagare att fatta ett interimistiskt beslut om hemlig rumsavlyssning under de förutsättningar som anges i 27 kap. 21 a § rättegångsbalken. Vidare klargörs att åklagaren då även får besluta om tillträdestillstånd, om ansökan innehåller en sådan begäran och förutsättningar finns för åtgärden.

Tillägget i *tredje stycket* innebär att de uppgifter som insamlats till följd av ett interimistiskt beslut om hemlig rumsavlyssning inte får lämnas över till den ansökande staten innan rätten har fattat beslut om tvångsmedlet. Detta överensstämmer med vad som gäller i fråga om interimistiska beslut om hemlig övervakning och hemlig avlyssning av elektronisk kommunikation samt hemlig kameraövervakning.

Övervägandena finns i avsnitt 11.5 och 15.4.

18.4 Förslaget till lag om ändring i lagen (2017:1000) om en europeisk utredningsorder

2 kap.

5 §

Paragrafen innehåller bestämmelser om förfarandet vid utfärdande av en utredningsorder.

Ändringen i *andra stycket* innebär att det införs en möjlighet för åklagare att fatta interimistiskt beslut om hemlig rumsavlyssning. Eftersom alla tvångsmedel i första stycket första och andra punkten kommer att omfattas av en möjlighet till interimistiskt åklagarbeslut slopas uppräkningen och ersätts med en hänvisning till de angivna bestämmelserna. Övervägandena finns i avsnitt 11.5, 12.4, 12.5 och 15.4.

3 kap.

10 §

Paragrafen innehåller bestämmelser om åklagares möjlighet att interimistiskt besluta att erkänna och verkställa en utredningsorder.

Det införs en möjlighet för åklagare att fatta interimistiskt beslut om hemlig rumsavlyssning och om tillträdestillstånd avseende hemlig kameraövervakning och hemlig rumsavlyssning. Vidare klargörs att åklagaren i en utgående utredningsorder även får besluta interimistiskt om tillträdestillstånd, om ansökan innehåller en sådan begäran och förutsättningar finns för åtgärden. Övervägandena finns i avsnitt 11.5, 12.4, 12.5 och 15.4.

18.5 Förslaget till lag om ändring i lagen (2020:62) om hemlig dataavläsning

4 §

Paragrafen reglerar under vilka förutsättningar tillstånd till hemlig dataavläsning får beviljas under en förundersökning.

I *första stycket* införs en hänvisning till den nya 5 a §. Vidare görs i *andra punkten* en ändring som innebär att den utvidgning av brottskatalogen för hemlig avlyssning av elektronisk kommunikation som görs i 18 § andra stycket rättegångsbalken gäller även för hemlig dataavläsning. Förslaget har behandlats i avsnitt 7.4 och 7.6.

Genom en ny *femte punkt i första stycket* införs en ny straffvärdeventil för viss flerfaldig brottslighet. Förslaget har behandlats i avsnitt 6.5–6.7 och 6.10–6.14. Bestämmelsen innebär att det kan fattas ett beslut om hemlig dataavläsning även vid förundersökningar om viss flerfaldig brottslighet, fastän de brott som ingår i den misstänkta brottsligheten inte vart och ett för sig kan föranleda ett sådant beslut. Möjligheten gäller samtliga uppgiftstyper som räknas upp i 2 § första stycket, med undantag för rumsavlyssningsuppgifter. Sådana uppgifter regleras i stället i 6 §. Straffvärdeventilen har samma innebörd som i 18 § andra stycket 18 rättegångsbalken, se vidare kommentaren till den bestämmelsen.

Eftersom det är fråga om användning av ett mycket integritetskänsligt tvångsmedel bör den nya straffvärdeventilen tillämpas restriktivt.

I *andra och tredje styckena* regleras vilka informationssystem som åtgärden får avse. Genom tillägg i respektive stycke ges en upplysning om att det finns särbestämmelser om detta i den nya 5 a §.

I *fjärde stycket* regleras vilka platser tillståndet får avse. Stycket ändras endast på så sätt att det klargörs att begränsningarna av själva tillståndet till en viss plats inte gäller när den nya 4 a § är tillämplig. Övervägandena finns i avsnitt 10.4–10.6.

Övriga ändringar i paragrafen är endast redaktionella.

4 a §

Genom paragrafen, som är ny, införs en möjlighet att knyta ett tillstånd till hemlig dataavläsning som gäller kameraövervakningsuppgifter till den skäligen misstänkte i stället för, som enligt 4 §, en viss plats. Övervägandena finns i avsnitt 10.4–10.9.

Innebörden av den nya möjligheten är att det inte i beslutet måste anges en viss plats där åtgärden ska ske och att det ska anges att åtgärden avser den skäligen misstänkte. När beslutet på detta sätt knyts till den skäligen misstänkte, får de villkor som enligt 18 § första stycket 4 alltid ska tas in i tillståndet för att tillgodose skyddet av den personliga integriteten en särskilt stor betydelse. Dessa villkor bör vara utformade på ett sådant sätt att den hemliga dataavläsningen är proportionerlig och i övrigt godtagbar oavsett var den sedermera kommer att verkställas. Inget hindrar att man vid samma tillfälle meddelar tillstånd till hemlig dataavläsning av såväl en viss plats som avläsning som avser den skäligen misstänkte, om det även finns förutsättningar för det.

Bestämmelsen får tillämpas endast om det finns särskilda skäl. Sådana skäl föreligger om det saknas rimliga förutsättningar att få tillgång till de uppgifter som behövs i utredningen genom en hemlig kameraövervakning eller en hemlig dataavläsning som avser kameraövervakningsuppgifter avseende en viss plats. Det kan t.ex. gälla kartläggning av hur den misstänkte rör sig på platser som är svåra att bedriva fysisk spaning på utan att riskera upptäckt, såsom mötesplatser med andra misstänkt kriminella personer eller gömmor för narkotika eller vapen.

Det gäller ett krav på att åtgärden endast får användas på en plats där den misstänkte kan antas komma att uppehålla sig. Med ordet användas avses här att åtgärden verkställs. Skrivningen innebär alltså inte någon begränsning när det gäller tillståndets utformning. Kravet på att det kan antas att den misstänkte kommer att uppehålla sig på platsen har samma innebörd som i 4 § fjärde stycket. Av sista meningen framgår att åtgärden aldrig får användas i någons stadigvarande bostad. Motsvarande begränsning gäller när åtgärden vidtas enligt 4 § fjärde stycket.

5 §

I paragrafen regleras att tillstånd till hemlig dataavläsning i vissa fall får beviljas för att utreda vem som skäligen kan misstänkas för brott och under vilka förhållanden en sådan åtgärd får vidtas.

Tillägget i *första stycket* har behandlats i avsnitt 6.5–6.7 och 6.10–6.14 och innebär att hemlig dataavläsning avseende kommunikationsövervaknings- och platsuppgifter i syfte att utreda vem som skäligen kan misstänkas för brottet får användas även med tillämpning av den nya straffvärdeventilen för viss flerfaldig brottslighet. Begränsningen till historiska kommunikationsövervakningsuppgifter slopas. Övervägandena i den delen finns i avsnitt 7.5.

5 a §

I paragrafen, som är ny, regleras att tillstånd till hemlig dataavläsning avseende kommunikationsavlyssningsuppgifter i vissa fall får beviljas för att utreda vem som skäligen kan misstänkas för brott och under vilka förhållanden en sådan åtgärd får vidtas. Övervägandena finns i avsnitt 9.5 och 9.7–9.10.

Genom paragrafen införs en möjlighet att meddela tillstånd till hemlig dataavläsning i syfte att utreda vem som skäligen kan misstänkas för brottet även avseende kommunikationsavlyssningsuppgifter. Möjligheten är dock enligt *första stycket* begränsad till de brott och den brottslighet som kan leda till hemlig avlyssning av elektronisk kommunikation i samma syfte. Se vidare kommentaren till 27 kap. 18 a § rättegångsbalken.

I *andra stycket* regleras vilka avläsningsbara informationssystem som får omfattas av åtgärden. Bestämmelsen motsvarar med ett undantag från vad som gäller i fråga om hemlig avlyssning av elektronisk kommunikation i syfte att utreda vem som skäligen kan misstänkas för brottet (27 kap. 20 § tredje stycket rättegångsbalken), nämligen på det sättet att endast användning och inte innehav av ett visst informationssystem kan vara en sådan koppling som kan läggas till grund för ett tillstånd till tvångsmedlet. Med uttrycket ”kontakta” avses samma sak som i 4 § fjärde stycket. I övrigt hänvisas till kommentaren till 27 kap. 20 § tredje stycket rättegångsbalken.

6 §

I paragrafen regleras förutsättningarna för ett tillstånd till hemlig dataavläsning som gäller rumsavlyssningsuppgifter.

Tillägget i *första stycket*, som har behandlats i avsnitt 6.8–6.14, innebär att hemlig dataavläsning som gäller rumsavlyssningsuppgifter, utöver vad som tidigare gällt, även får användas i fall där den nya straffvärdeventilen avseende viss flerfaldig brottslighet för hemlig rumsavlyssning är tillämplig, se vidare kommentaren till ändringarna i 27 kap. 20 d § rättegångsbalken.

Ändringen i andra stycket har endast ett förtydligande syfte. Någon ändring i sak är inte avsedd.

Tredje stycket är nytt. Övervägandena finns i avsnitt 10.4–10.9. Genom bestämmelsen införs en möjlighet att knyta ett tillstånd till hemlig dataavläsning som gäller rumsavlyssningsuppgifter till den skäligen misstänkte i stället för till en viss plats. Innebörden av den nya möjligheten är att det inte i beslutet måste anges en viss plats där åtgärden ska ske och att det ska anges att dataavläsningen avser den skäligen misstänkte. Bestämmelsen får tillämpas endast om det finns särskilda skäl. Sådana skäl föreligger om det saknas rimliga förutsättningar att få tillgång till de uppgifter som behövs i utredningen genom en hemlig rumsavlyssning eller hemlig dataavläsning som gäller rumsavlyssningsuppgifter avseende en viss plats. Ett exempel kan vara att den misstänkte undviker att föra för utredningen intressanta samtal på sådana platser som kan avlyssnas, och i stället samtalar under promenader på olika platser. Inget hindrar att man vid samma tillfälle meddelar tillstånd till hemlig dataavläsning av såväl en viss plats som avläsning som avser den skäligen misstänkte, om det även finns förutsättningar för det. Man kan t.ex. tänka sig att tillstånd dels ges med stöd av andra stycket för dataavläsning i den misstänktes bostad, dels med stöd av detta stycke för att man ska kunna avlyssna den misstänkte när denne rör sig utomhus.

Det gäller ett krav på att åtgärden endast får användas på en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Kravet på att det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig på platsen har samma innebörd som i andra stycket. Ytterligare en begränsning gäller för att dataavläsningen ska få riktas mot någon annan stadigvarande bostad än den misstänktes. I det fallet krävs att det finns synnerlig an-

ledning att anta att den misstänkte kommer att uppehålla sig där. Även detta krav har samma innebörd som i andra stycket. Förbudet mot hemlig dataavläsning på vissa platser gäller även i de fall som avses i tredje stycket.

När ett tillstånd till hemlig dataavläsning meddelas är det obligatoriskt att meddela villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. Eftersom tillståndet inte är begränsat till en viss plats måste det ställas särskilt höga krav på villkorens utformning. Dessa bör vara formulerade så att dataavläsningen är proportionerlig och i övrigt godtagbar oavsett var åtgärden sedermera kommer att verkställas. I normalfallet bör det i villkoren ges någon form av platsangivelse, låt vara att denna kan vara brett formulerad. Andra villkor kan vara exempelvis att dataavläsning bara får ske när det genom spaning eller på annat sätt kan konstateras att den misstänkte är på plats eller att ett visst möte äger rum.

Övriga ändringar är endast redaktionella.

14 §

I paragrafen finns regler om att rätten prövar ansökan om hemlig dataavläsning och om vem som ska göra ansökan.

Det införs ett nytt *andra stycke* som innebär ett nytt åliggande för åklagaren. I de fall då beslutet knyts till den skäligen misstänkte är åklagaren enligt bestämmelsen skyldig att i samband med ansökan till rätten föreslå de villkor som tillståndet ska förenas med. Förslaget kan tas in i själva ansökan eller i den promemoria som ges in till rätten. Övervägandena finns i avsnitt 11.7 och 11.9.

15 §

Paragrafen innehåller bestämmelser om behörig domstol vid beslut om hemlig dataavläsning. Hänvisningen till 27 kap. 18 § andra stycket ändras till följd av den ändrade punktindelningen i den paragrafen. Någon ändring i sak är inte avsedd.

17 §

Paragrafen innehåller bestämmelser om en möjlighet för åklagaren att i avvaktan på rättens prövning fatta beslut om hemlig dataavläsning. Ändringen i *första stycket* innebär att det blir tillåtet med sådana beslut även i fråga om rumsavlyssningsuppgifter. Övervägandena finns i avsnitt 11.5.

18 §

Paragrafen innehåller bestämmelser om innehållet i ett beslut om hemlig dataavläsning.

I paragrafen tas det in ett nytt *andra stycke* med särskilda bestämmelser om innehållet i beslutet när tillståndet med stöd av 4 a § eller 6 § tredje stycket har kopplats till den skäligen misstänkte. Övervägandena finns i avsnitt 10.7 och 10.9.

Övriga ändringar är endast redaktionella.

Kommittédirektiv 2020:104

Utökade möjligheter att använda hemliga tvångsmedel

Beslut vid regeringssammanträde den 14 oktober 2020

Sammanfattning

En särskild utredare ska se över delar av regleringen om hemliga tvångsmedel. Syftet är att ta ställning till hur hemliga tvångsmedel ska kunna användas i en större utsträckning för att bekämpa allvarlig brottslighet. Brott som begås i kriminella miljöer kan av olika skäl vara särskilt svåra att utreda. De brottsbekämpande myndigheterna måste ha tillgång till ändamålsenliga och verkningsfulla verktyg för att effektivt kunna bekämpa sådana brott. Utredaren ska noga väga behovet av en effektiv brottsbekämpning mot den enskildes rätt till skydd för sin personliga integritet. En sådan avvägning ska göras för varje förslag för sig och även när det gäller förslagen sammantaget. Förslagen ska även uppfylla högt ställda krav på rättssäkerhet.

Utredaren ska bl.a.

- ta ställning till om det bör införas en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning vid misstanke om flera brott vars samlade straffvärde kan antas överstiga ett visst straff,
- ta ställning till i vilka situationer och vid vilka straffvärden en sådan möjlighet bör kunna tillämpas,
- ta ställning till om åklagare bör få möjlighet att fatta interimistiska beslut om hemlig rumsavlyssning inklusive tillträde för att installera utrustningen,

- ta ställning till om den verkställande myndigheten bör kunna få tillstånd att i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång för att verkställa ett beslut om enbart hemlig kameraövervakning,
- ta ställning till om åklagare bör få möjlighet att interimistiskt besluta om sådant tillträde,
- ta ställning till om skyddet för den personliga integriteten bör stärkas, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Uppdraget ska redovisas senast den 14 april 2022.

Uppdraget att utöka möjligheterna att använda hemliga tvångsmedel

Behovet av åtgärder

De brottsbekämpande myndigheterna måste ha tillgång till ändamålsenliga och verkningsfulla verktyg för att kunna lagföra dem som begår brott. Förändringar i brottsligheten och av misstänkta personers beteenden samt den tekniska utvecklingen har inneburit att det finns ett ökat behov av att kunna använda hemliga tvångsmedel. Detta behov är påtagligt när det gäller den grova våldsbrottslighet och förmögenhetsbrottslighet som begås i kriminella miljöer. Många kriminella nätverk i Sverige är i dag löst sammansatta. Samtidigt ökar samverkan mellan kriminella aktörer med kompetens inom ekonomi och kriminella aktörer med våldskapital. För att uppnå ekonomisk vinning söker kriminella aktörer efter olika konstellationer och samverkansformer. Formerna för dessa kan variera beroende på typ av brottsupplägg, men generellt sett följs graden av organisering och komplexiteten i ett brottsupplägg åt. De kriminella aktörerna blir också mer tekniskt sofistikerade (Nationellt underrättelsecentrums rapport Myndighetsgemensam lägesbild om organiserad brottslighet 2018–2019 s. 4). Brott som begås inom ramen för kriminella nätverk är ofta särskilt svåra att utreda eftersom brottsoffer och vittnen av olika anledningar kan vara obenägna att lämna information till polisen. Det finns därför skäl att se över om de brottsbekämpande myndigheterna ska ges utökade möjligheter att använda hemliga tvångsmedel.

Dagens reglering av hemliga tvångsmedel

De hemliga tvångsmedlen utgörs av hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning. Även ett förordnande enligt 27 kap. 9 § rättegångsbalken (RB) om kvarhållande (och kontroll) av en försändelse samt inhämtning enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, förkortad inhämtningslagen, är hemliga tvångsmedel.

Regeringen beslutade den 11 december 2019 propositionen Hemlig dataavläsning (prop. 2019/20:64). I propositionen föreslår regeringen att de brottsbekämpande myndigheterna ska få möjlighet att använda ett nytt hemligt tvångsmedel, som ska kallas hemlig dataavläsning. Det nya tvångsmedlet ska enligt propositionen kunna användas under en förundersökning, i underrättelseverksamhet och vid särskild utlänningskontroll. Den nya lagstiftningen trädde i kraft den 1 april 2020.

Hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation får användas både under en förundersökning och innan en förundersökning inletts. Dessa tvångsmedel regleras i rättegångsbalken, lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, förkortad preventivlagen, och lagen (1991:572) om särskild utlänningskontroll. I lagen om särskild utlänningskontroll regleras förutsättningarna för Säkerhetspolisen att använda vissa hemliga tvångsmedel när ett utvisningsbeslut enligt lagen inte kan verkställas. Lagen om särskild utlänningskontroll är för närvarande föremål för en översyn och utredningen om utlänningsärenden med säkerhetsaspekter redovisade sitt uppdrag i betänkandet Ett effektivare regelverk för utlänningsärenden med säkerhetsaspekter (SOU 2020:16) i mars 2020. Betänkandet har remitterats och bereds för närvarande inom Regeringskansliet. Inhämtningslagen reglerar förutsättningarna för Polismyndigheten, Säkerhetspolisen och Tullverket att i underrättelseverksamhet hämta in övervakningsuppgifter om elektronisk kommunikation. Möjligheterna att använda hemliga kameraövervakning regleras i rättegångsbalken och preventivlagen. Hemlig rumsavlyssning, som endast får användas under förundersökning, regleras i rättegångsbalken.

Hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning kan också aktualiseras inom ramen för Sveriges internationella samarbete enligt lagen (2017:1000) om en europeisk utredningsorder och lagen (2000:562) om internationell rättslig hjälp i brottmål.

Utredaren bör väga behovet av brottsbekämpning mot den personliga integriteten och rättssäkerheten

Regleringen om hemliga tvångsmedel har utformats efter en avvägning mellan å ena sidan samhällets behov av en effektiv brottsbekämpning till skydd för medborgarna och å andra sidan den enskildes rätt till integritet och rättssäkerhet i förhållande till staten.

Regeringsformen (RF) garanterar den enskilde ett skydd gentemot det allmänna mot bl.a. husrannsakan och liknande intrång, hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Skyddet omfattar även betydande intrång i den personliga integriteten, om det sker utan samtycke och genom övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § RF). Dessa grundläggande fri- och rättigheter får begränsas endast genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt eller utgöra ett hot mot den fria åsiktsbildningen (2 kap. 20 och 21 §§ RF).

Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) är inkorporerad i svensk lag. Enligt artikel 8.1 i Europakonventionen har var och en rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens, vilket bl.a. omfattar skydd mot övervakning i olika former och mot telefonavlyssning. Tvångsmedel som innefattar ingrepp i området som artikel 8 skyddar, kan enligt konventionen endast godtas om de har stöd i lag och omfattas av de undantag som anges i artikel 8.2. Undantagen avser t.ex. åtgärder som i ett demokratiskt samhälle är nödvändiga för att upprätthålla den allmänna säkerheten och för att förebygga brott. Europadomstolen har i sin praxis också uppställt en minimistandard för de krav som bör ställas på lagstiftning om dolda spaningsåtgärder eller hemliga tvångsmedel till undvikande av missbruk.

Sverige har ratificerat Internationella konventionen om medborgerliga och politiska rättigheter (ICCPR). Enligt artikel 17 i konventionen får ingen utsättas för godtyckligt eller olagligt ingripande med avseende på privatliv, hem eller korrespondens. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp. Ett ingripande med avseende på privatliv enligt ICCPR måste således ha stöd i lag.

EU:s stadga om de grundläggande rättigheterna ska tillämpas när unionsrätten tillämpas. Enligt artikel 7 i stadgan har var och en rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer. Vidare stadgas i artikel 8 att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

För all tvångsmedelsanvändning gäller ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Ändamålsprincipen innebär att en myndighets befogenhet att använda ett tvångsmedel ska vara bundet till det ändamål för vilket tvångsmedlet har beslutats. Enligt behovsprincipen får en myndighet använda ett tvångsmedel bara när det finns ett påtagligt behov av det och en mindre ingripande åtgärd inte är tillräcklig. Proportionalitetsprincipen innebär att ett tvångsmedel får användas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller något annat motstående intresse.

Regelverket om hemliga tvångsmedel innehåller även flera rättssäkerhetsgarantier. Förhandsprövning av domstol är en sådan. Huvudregeln är att rätten prövar frågor om hemliga tvångsmedel innan de får användas och rätten har dessutom möjlighet att ange närmare villkor för tvångsmedelsanvändningen i syfte att säkerställa att enskildas personliga integritet inte kränks i onödan. Då rätten prövar frågor om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning har dessutom ett offentligt ombud till uppgift att bevaka enskildas integritetsintressen. Förutom den föregående prövningen av domstol finns en efterföljande tillsyn. De brottsbekämpande myndigheternas användning av hemliga tvångsmedel är nämligen föremål för tillsyn av Säkerhets- och integritetsskyddsnämnden.

De brottsbekämpande myndigheternas befogenheter att med stöd av hemliga tvångsmedel bereda sig tillgång till information om en enskild innebär ett ingrepp i dennes personliga integritet. Utredaren bör i sina ställningstaganden beakta att möjligheterna till att

använda hemliga tvångsmedel har utökats genom flertalet straffskärpningar under de senaste åren. Utredaren bör noga väga behovet av en effektiv brottsbekämpning mot den enskildes rätt till skydd för sin personliga integritet. En sådan avvägning ska göras för varje förslag för sig och även när det gäller förslagen sammantaget. Utredaren ska även ta ställning till om skyddet för den personliga integriteten bör stärkas och vid behov lämna sådana förslag. Vidare ska förslagen uppfylla högt ställda krav på rättssäkerhet.

Frågan om att införa en ny straffvärdeventil för hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning

Bestämmelserna som anger för vilka brott hemliga tvångsmedel får användas innehåller en eller flera av följande komponenter. Antingen anges ett krav på ett visst lägsta föreskrivet straff, en uppräkning av vissa brottstyper eller en s.k. straffvärdeventil som anger att det hemliga tvångsmedlet får användas för ett brott vars straffvärde i det enskilda fallet kan antas överstiga ett visst fängelsestraff.

Det krävs misstanke om ett konkret brott vars straffvärde kan antas överstiga två års fängelse för att hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning ska få användas under en förundersökning (27 kap. 18 och 20 a §§ RB). Det är emellertid inte möjligt att använda tvångsmedlen vid misstanke om flera brott där det sammanlagda straffvärdet kan antas vara högt, men där samtliga ingående enskilda brott kan betraktas som mindre allvarliga. Som en konsekvens av hur dagens regler är utformade kan således i normalfallet misstankar om systematisk brottslighet bestående av t.ex. flera skattebrott, stölder eller bedrägerier falla utanför tillämpningsområdet för dessa hemliga tvångsmedel. Detta samtidigt som de ovan angivna brottstyperna utgör exempel på vad som kan vara viktiga inkomstkällor för kriminella, enligt Brottsförebyggande rådets (Brå) rapport Kriminella nätverk och grupperingar – Polisers bild av maktstrukturer och marknader (rapport 2016:12 s. 87, 99–102 och 114–119). När det gäller den ekonomiska brottsligheten är det vanligt med brottsupplägg som omfattar flera olika brott. Det kan t.ex. handla om brott som begås i ett och samma bolag eller en individ som begår samma brott i flera olika bolag. Dessa typer av brott, som sedda för sig inte alltid är särskilt allvarliga, utgör således en

inkomstkälla för nätverk som ägnar sig åt betydligt allvarligare brottslighet än så.

Frågan om att införa en straffvärdeventil vid seriebrottslighet har tidigare övervägts i propositionen Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering, och regeringen ansåg då att en sådan inte skulle införas med hänsyn till det integritetsintrång som användandet av hemliga tvångsmedel innebär (prop. 2002/03:74 s. 34). Även om detta argument fortfarande är giltigt finns det mot bakgrund av brottsutvecklingen skäl att på nytt överväga en sådan straffvärdeventil.

Straffvärdeventilen i bestämmelsen om hemlig rumsavlyssning är utformad på så sätt att det krävs att brottets straffvärde kan antas överstiga fängelse i fyra år och att det dessutom är fråga om ett brott som räknas upp i paragrafen (27 kap. 20 d § RB). Det bör i sammanhanget även ses över om denna straffvärdeventil ska förändras på motsvarande sätt samt om brottskatalogen ska tas bort för att straffvärdeventilen vid hemlig rumsavlyssning ska kunna tillämpas oavsett vilket brott som utreds.

Utredaren ska därför

- ta ställning till om det bör införas en möjlighet att använda hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning vid misstanke om flera brott vars samlade straffvärde kan antas överstiga ett visst straff,
- ta ställning till i vilka situationer och vid vilka straffvärden en sådan möjlighet bör kunna tillämpas,
- ta ställning till om straffvärdeventilen i fråga om hemlig rumsavlyssning bör få tillämpas oavsett brott, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Frågan om fler brott ska ingå i brottskatalogerna i bestämmelserna om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation

Att den som utsatts för eller bevittnat ett brott av olika skäl inte vill lämna upplysningar om brottet är ett problem. Brå har på regeringens uppdrag i rapporten Tystnadskulturer – En studie om tystnad mot rättsväsendet (rapport 2019:10) studerat tystnadskulturer och

övergrepp i rättssak. Enligt rapporten kan de kriminella tystnadskulturerna ha spridningseffekter till personer utanför miljön genom medierapportering eller ryktesspridning som förmedlar grupperingarnas skrämselkapital. Konsekvensen kan bli att personer utanför den kriminella miljön inte vågar anmäla brott eller vittna om de har skäl att tro att gärningspersonen tillhör ett kriminellt nätverk (s. 11–12).

Vissa brottstyper är enligt Åklagarmyndigheten särskilt svårutredda eftersom de typiskt sett begås i en miljö där det råder en tystnadskultur. Myndigheten anger i skrivelsen Framställning om ändringar i lagstiftningen om hemliga tvångsmedel i 27 kap. rättegångsbalken (Ju2019/03572/Å s. 5) att utpressning, övergrepp i rättssak, mened och skyddande av brottsling kan vara sådana brott. Det är av största vikt att samhället tar tydlig ställning mot beteenden som påverkar möjligheterna att upprätthålla straffsystemets effektivitet. Det bör därför undersökas om dessa brott ska ingå i brottskatalogerna i bestämmelserna om hemlig avlyssning av elektronisk kommunikation (27 kap. 18 § RB) och hemlig övervakning av elektronisk kommunikation (27 kap. 19 § RB).

Utredaren ska därför

- ta ställning till om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation bör få användas vid fler brott, t.ex. utpressning, övergrepp i rättssak, mened och skyddande av brottsling, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Frågan om hemlig övervakning av elektronisk kommunikation ska få användas för att lokalisera skäligen misstänkta

Hemlig övervakning av elektronisk kommunikation får användas om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen (27 kap. 20 § första stycket RB).

Säkerhets- och integritetsskyddsnämnden har i ett uttalande med beslut om hanteringen av hemliga tvångsmedel vid Norrorts åklagarkammare (dnr 132-2018 [Ju2019/03048/Å]) uppmärksammat att hemlig övervakning av elektronisk kommunikation har använts i realtid för att lokalisera var skäligen misstänkta, som också var anhållna i sin frånvaro, befann sig i syfte att anhållandet skulle kunna verkställas. Nämnden ifrågasätter om kravet som ställs upp i 27 kap. 20 §

första stycket RB på att åtgärden ska vara av synnerlig vikt för utredningen är uppfyllt i dessa ärenden, eftersom nämnden anser att syftet med den hemliga övervakning som använts i ärendena inte varit att tillföra nya uppgifter till utredningen. Även Justitieombudsmannen har uttryckt tveksamhet till en sådan tillämpning av tvångsmedlet (JO 2011/12 s. 71–76 och JO 1994/95 s. 34–43).

Åklagarmyndigheten har anfört att domstolarna ger tillstånd till hemlig övervakning av elektronisk kommunikation i realtid för att verkställa ett frihetsberövande när även andra åtgärder, som bedöms vara av synnerlig vikt för utredningen, ska vidtas. Det kan t.ex. handla om att spår ska säkras från den misstänktes kläder eller kropp (Ju2019/03572/Å s. 16).

Regeringen anser att utrymmet för att använda hemlig övervakning av elektronisk kommunikation för att lokalisera en misstänkt bör ses över.

Utredaren ska därför

- ta ställning till i vilka situationer hemlig övervakning av elektronisk kommunikation bör få användas för att lokalisera skäligen misstänkta, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Frågan om hemlig övervakning av elektronisk kommunikation ska få användas mot målsäganden för att utreda vem som skäligen kan misstänkas för brottet

Hemlig övervakning av elektronisk kommunikation får användas i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen (27 kap. 20 § andra stycket RB). Lagtexten innehåller inga begränsningar om vem tvångsmedlet får riktas mot.

Säkerhets- och integritetsskyddsnämnden har i ett uttalande med beslut om hanteringen av hemliga tvångsmedel vid Norrorts åklagarkammare (dnr 132-2018) uppmärksammat att hemlig övervakning av elektronisk kommunikation använts mot målsäganden i två fall. Nämnden ifrågasätter om det är rimligt att brottsbekämpande myndigheters intresse av övervakningsuppgifter tillåts urholka målsägandens integritetsskydd på detta sätt. Åklagarmyndigheten har i sin tur uppgett att domstolarna brukar ge tillstånd till hemlig övervakning

av elektronisk kommunikation i dessa fall. Om möjligheten till detta skulle inskränkas får det enligt myndigheten allvarliga negativa konsekvenser för möjligheterna att utreda brott och det skulle innebära ett steg tillbaka i kampen mot tystnadskulturen (Ju2019/03572/Å s. 13–16). Några särskilda överväganden om åtgärden ska kunna riktas mot målsäganden har inte gjorts i tidigare lagstiftningsarbeten. Det finns därför skäl att se över denna frågeställning.

Utredaren ska därför

- ta ställning till om det bör vara tillåtet med hemlig övervakning av elektronisk kommunikation mot målsäganden i syfte att utreda vem som skäligen kan misstänkas för brottet och i så fall i vilka situationer, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Frågan om hemlig avlyssning av elektronisk kommunikation ska få användas för att utreda vem som skäligen kan misstänkas för brottet

Det är inte tillåtet att använda hemlig avlyssning av elektronisk kommunikation för att utreda vem som skäligen kan misstänkas för brottet. Åklagarmyndigheten har uppgett att det i vissa fall inte är tillräckligt att använda hemlig övervakning av elektronisk kommunikation för att utreda vem som skäligen kan misstänkas för brottet. En möjlighet till hemlig avlyssning av elektronisk kommunikation i fall som handlar om t.ex. människorov skulle kunna leda till att gärningsmännen identifieras fortare än i dag. Hemlig avlyssning av elektronisk kommunikation skulle kunna användas när det gäller sådana nummer som målsäganden varit i kontakt med innan försvinnandet eller sådana nummer som använts i kontakter med anhöriga för att pressa dem på pengar (Ju2019/03572/Å s. 14).

En närliggande fråga kan uppstå när den som misstänks för ett brott har avlidit. Hemlig avlyssning av elektronisk kommunikation för att utreda vem som skäligen kan misstänkas för brottet i detta fall skulle utgöra en viktig informationskälla för de brottsbekämpande myndigheterna och därigenom underlätta undersökningen av om det finns eventuella medgärningsmän som är i livet. Det skulle t.ex. kunna röra sig om ett terroristbrott där en gärningsperson dör i samband med attentatet.

Det finns således skäl ur brottsbekämpningsperspektiv att tillåta hemlig avlyssning av elektronisk kommunikation för att utreda vem som skäligen kan misstänkas för brottet. Samtidigt är hemlig avlyssning av elektronisk kommunikation ett ingripande tvångsmedel, varför det finns anledning att se restriktivt på i vilka fall det ska få användas. Utredaren ska bedöma om hemlig avlyssning av elektronisk kommunikation bör tillåtas för att utreda vem som skäligen kan misstänkas för brottet. Därtill måste det även övervägas vem åtgärden ska få riktas mot, t.ex. om den ska få riktas mot målsäganden eller den som har avlidit.

Utredaren ska därför

- ta ställning till om hemlig avlyssning av elektronisk kommunikation bör få användas i syfte att utreda vem som skäligen kan misstänkas för brottet och i så fall i vilka situationer tvångsmedlet bör få användas samt vem åtgärden bör få riktas mot, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Frågan om beslut om hemlig rumsavlyssning och hemlig kameraövervakning ska knytas till en person

Tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning måste enligt dagens regler alltid knytas till en viss plats. Åklagarmyndigheten har väckt frågan om tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning ska få knytas till person (Ju2019/03572/Å s. 7–13).

Frågan om anknytning mellan person och tvångsmedel har varit föremål för överväganden i flera tidigare lagstiftningsarbeten (se t.ex. prop. 1994/95:227 s. 20–22, prop. 1995/96:85 s. 30–32 och prop. 2013/14:237 s. 96–97). I det lagstiftningsärende som föregick lagen (1995:1506) om hemlig kameraövervakning övervägde regeringen om tillståndet skulle knytas till en plats eller en person. Regeringen bedömde då att det skulle medföra svårigheter att tillämpa ändamåls-, behovs- och proportionalitetsprinciperna om tillståndet skulle knytas till en person (prop. 1995/96:85 s. 30). I propositionen Hemlig dataavläsning har regeringen återigen gjort samma principiella bedömning om hemlig dataavläsning och föreslagit att en verkställighet genom hemlig dataavläsning också ska vara underkastad ett platskrav (prop. 2019/20:64 s. 118–120). Detta ställnings-

tagande ligger även i linje med den slutsats som dras i propositionen Ett förenklat förfarande vid vissa beslut om hemlig avlyssning, nämligen att det inte finns tillräckliga skäl att knyta tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation till en person. Skälen till detta är bl.a. att det är viktigt att domstolen i sin proportionalitetsprövning kan ta ställning till den konkreta avlyssnings- eller övervakningsåtgärd som ska utföras (prop. 2019/20:145 s. 14).

Åklagarmyndigheten uppger att grovt kriminella personer är ytterst säkerhetsmedvetna. Det har gjort att det blivit vanligt att misstänkta personer träffas på allmänna platser där de känner sig säkra på att kunna tala utan risk för att bli avlyssnade. Den tekniska utvecklingen har gjort att utrustningen för att verkställa hemlig rumsavlyssning och hemlig kameraövervakning kan anpassas efter de misstänkta personerna snabbare än tidigare med minskade risker för att utomstående personer drabbas av tvångsmedlet (Ju2019/03572/Å s. 7–8 och 12).

Det finns alltjämt starka betänkligheter mot att knyta ett tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning till en person i stället för en viss plats. Mot bakgrund av förändringen av de brottsaktiva personernas beteende och den ovan beskrivna tekniska utvecklingen finns det dock tillräckliga skäl att i detta sammanhang återigen analysera frågan.

Utredaren ska därför

- ta ställning till om tillstånd till hemlig rumsavlyssning och hemlig kameraövervakning bör kunna knytas till en person, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Frågan om det bör införas möjlighet för åklagare att fatta interimistiska beslut om hemlig rumsavlyssning

Åklagare får fatta interimistiska beslut om hemlig rumsavlyssning endast om landet är i krig eller om liknande extraordinära omständigheter råder (2 och 28 §§ lagen [1988:97] om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.). Frågan om att låta åklagare fatta interimistiska beslut om hemlig rumsavlyssning även i fredstid har tidigare varit föremål för regeringens överväganden i propositionen Hemliga tvångs-

medel mot allvarliga brott (prop. 2013/14:237). Regeringen gjorde då bedömningen att någon sådan möjlighet inte skulle införas med hänsyn till att hemlig rumsavlyssning typiskt sett är det tvångsmedel som leder till det största intrånget i enskildas personliga integritet varför särskild försiktighet ansågs påkallad (s. 142).

Åklagare har möjlighet att under förundersökning fatta interimistiska beslut om hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning (27 kap. 21 a § RB och 2 kap. 5 § andra stycket lagen om en europeisk utredningsorder). En sådan möjlighet finns även när någon av dessa åtgärder ska vidtas i Sverige på begäran av en annan stat (4 kap. 25 och 27 §§ lagen om internationell rättslig hjälp i brottmål och 3 kap. 10 § lagen om en europeisk utredningsorder). Varje år redovisar regeringen användningen av hemliga tvångsmedel till riksdagen. Av det underlag som myndigheterna gett in för tvångsmedelsanvändningen under 2019 framgår det att domstol endast har upphävt en handfull interimistiska beslut (Redovisning av användningen av vissa hemliga tvångsmedel under 2019 [Ju2020/02045/Å] s. 10–11, 21, 27 och 40). Bilden är densamma föregående år. Det kan därför ifrågasättas om en särskild försiktighet verkligen är påkallad när det gäller möjligheten att fatta interimistiska beslut om hemlig rumsavlyssning. Härtill kommer det förhållandet att kriminella byter platser för sina möten med kort varsel, vilket gör att det finns ett behov av ett snabbt beslutsfattande. Ny teknik möjliggör dessutom att hemlig rumsavlyssning kan verkställas snabbare än tidigare.

Vidare kan det även finnas skäl att anta att en möjlighet till interimistiskt beslutsfattande kan leda till ökad effektivitet när det rör sig om internationellt samarbete mot gränsöverskridande brottslighet där ett snabbt beslutsfattande är viktigt.

Utredaren ska därför

- ta ställning till om åklagare bör få möjlighet att fatta interimistiska beslut om hemlig rumsavlyssning inklusive tillträde för att installera utrustningen, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Frågan om tillträdestillstånd för att verkställa enbart hemlig kameraövervakning

Ett tillträdestillstånd för hemlig kameraövervakning kan endast fås för att samtidigt verkställa ett beslut om hemlig rumsavlyssning (27 kap. 25 a § RB). När regeln infördes ansågs den medföra att möjligheten till tillträdestillstånd för hemlig kameraövervakning skulle begränsas till de mycket allvarliga och samhällsfarliga brotten (prop. 2013/14:237 s. 154).

Åklagarmyndigheten har uppgett att ett tillträde för enbart hemlig kameraövervakning ofta fås genom att samtycke inhämtas från den som förfogar över platsen. Det kan dock finnas fall där sådant samtycke inte lämnas eller där det inte är lämpligt att inhämta ett sådant samtycke, t.ex. om den som kan lämna samtycke är misstänkt för inblandning i brottsligheten (Ju2019/03572/Å s. 13).

I propositionen Hemlig dataavläsning föreslår regeringen att den verkställande myndigheten, efter särskilt tillstånd, i hemlighet ska få skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång. Det ska även vara möjligt för åklagare att under vissa förutsättningar fatta sådana interimistiska beslut (prop. 2019/20:64 s. 142 och 154). I linje med detta anser regeringen att frågan om införande av en möjlighet till tillträdestillstånd för enbart hemlig kameraövervakning bör övervägas. Det bör även övervägas om åklagare bör få möjlighet att fatta interimistiska tillträdesbeslut.

Utredaren ska därför

- ta ställning till om den verkställande myndigheten bör kunna få tillstånd att i hemlighet skaffa sig tillträde till och installera tekniska hjälpmedel på en plats som annars skyddas mot intrång för att verkställa ett beslut om enbart hemlig kameraövervakning,
- ta ställning till om åklagare bör få möjlighet att interimistiskt besluta om sådant tillträde, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Frågan om införande av en straffvärdeventil i inhämtningslagen

Inhämtningslagen reglerar de brottsbekämpande myndigheternas möjligheter att i underrättelseverksamhet inhämta uppgifter om elektronisk kommunikation. Tillstånd till sådan inhämtning kan ges antingen för brott för vilket det inte är föreskrivet lindrigare straff än fängelse två år eller för vissa särskilt angivna samhällsfarliga brott. Det saknas en straffvärdeventil i inhämtningslagen, vilket således innebär att även om viss brottslighet i det enskilda fallet kan antas ha ett straffvärde på över två år får inte tillstånd till inhämtning enligt lagen beviljas.

Frågan om att införa en straffvärdeventil i inhämtningslagen har väckts vid flera tillfällen. Framför allt har Ekobrottsmyndigheten påtalat behovet av att införa en sådan, eftersom myndigheten i princip inte handlägger några brott med ett minimistraff om fängelse i två år, enligt Slutredovisning av regeringsuppdrag till Tullverket, Polismyndigheten, Ekobrottsmyndigheten och Skatteverket om illegal hantering av punktskattepliktiga varor – Fi 2015/05353/S3 (Ju2018/02964/Å s. 16). Frågan har även tagits upp i olika utredningar där det har påtalats att frågan om straffvärdeventil i inhämtningslagen bör utredas, bl.a. i Datalagring och integritet (SOU 2015:31 s. 314–316) och i Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra (SOU 2017:37 s. 418–421). Regeringen har uttalat att frågan bör utredas, dels i propositionen Vissa kontrollfrågor och andra frågor på punktskatteområdet (prop. 2017/18:294 s. 70), dels i propositionen Datalagring vid brottsbekämpning (prop. 2018/19:86 s. 91). Det finns därför skäl att se över frågan.

När man tar ställning till om en straffvärdeventil ska införas i inhämtningslagen måste det särskilt beaktas att en sådan ventil är svårtillämpad i underrättelseskedet eftersom bristen på konkretion av brottsmisstanken i det skedet medför svårigheter att göra den straffvärdebedömning som krävs.

Det måste dessutom tas hänsyn till internationell praxis på området. EUdomstolen har i den s.k. Tele2-domen (dom av den 21 december 2016 i de förenade målen C-203/15 och C-698/15) gjort uttalanden i fråga om personkrets och brottets allvar när det gäller i vilka fall som brottsbekämpande myndigheter får ges tillgång till trafikuppgifter. En eventuell utvidgning av tillämpningsområdet för inhämtningslagen måste vara förenlig med internationell praxis.

Utredaren ska därför

- ta ställning till om en straffvärdeventil bör införas i inhämtningslagen, och
- lämna förslag på de författningsändringar som bedöms nödvändiga.

Konsekvensbeskrivningar

Utredaren ska bedöma hur förslagen förhåller sig till Sveriges internationella åtaganden om mänskliga rättigheter. Om förslagen förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Kontakter och redovisning av uppdraget

Utredaren ska föra dialog med och inhämta upplysningar från Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden, Post- och telestyrelsen och Sveriges advokatsamfund men även andra myndigheter och berörda aktörer, såsom telekomoperatörer, i den utsträckning som utredaren finner lämpligt. Utredaren ska också hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet, och om relevant arbete inom utredningsväsendet. Förslagen som utredaren lämnar ska vara förenliga med Sveriges internationella åtaganden.

Utredaren ska säkerställa att en välfungerande systematik i regelverket om hemliga tvångsmedel upprätthålls. Det innebär att utredaren även ska bedöma behovet av följdändringar i lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet, lagen om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen om särskild utlänningskontroll samt lagen (2020:62) om hemlig dataavläsning. Utredaren ska även bedöma behovet av följdändringar i lagen om internationell rättslig hjälp i brottmål och lagen om en europeisk utredningsorder. När det finns behov av det ska utredaren lämna förslag på författningsändringar. Utredaren har även möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska utredas under förutsättning att uppdraget ändå kan redovisas i tid.

Uppdraget ska redovisas senast den 14 april 2022.

(Justitiedepartementet)

Kommittédirektiv 2022:13

Tilläggsdirektiv till Utredningen om utökade möjligheter att använda hemliga tvångsmedel (Ju 2020:20)

Beslut vid regeringssammanträde den 17 mars 2022

Utvidgning av och förlängd tid för uppdraget

Regeringen beslutade den 14 oktober 2020 kommittédirektiv om utökade möjligheter att använda hemliga tvångsmedel (dir. 2020:104). Enligt direktiven ska en särskild utredare se över delar av regleringen om hemliga tvångsmedel. Syftet är att ta ställning till hur hemliga tvångsmedel ska kunna användas i större utsträckning för att bekämpa allvarlig brottslighet. I uppdraget ingår bl.a. att ta ställning till i vilka situationer hemlig övervakning av elektronisk kommunikation bör få användas för att lokalisera skäligen misstänkta. Utredaren ska även ta ställning till om skyddet för den personliga integriteten bör stärkas och vid behov lämna sådana förslag.

Utredaren får nu, utöver vad som framgår av de ursprungliga direktiven, även i uppdrag att

- särskilt bedöma om det finns ett behov av att ändra reglerna om underrättelse till enskild om användning av hemliga tvångsmedel,
- ta ställning till om och i så fall i vilka situationer hemlig övervakning av elektronisk kommunikation bör få användas för att lokalisera personer som är häktade i sin frånvaro efter att en förundersökning har avslutats eller som har uteblivit eller avvikit från verkställighet av påföljder, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Enligt direktiven skulle uppdraget redovisas senast den 14 april 2022. Utredningstiden ligger fast för större delen av det ursprungliga uppdraget som ska redovisas i ett delbetänkande. Utredningstiden ska dock förlängas för frågan i de ursprungliga direktiven om i vilka situationer hemlig övervakning av elektronisk kommunikation bör få användas för att lokalisera skäligen misstänkta. Den frågan ska, tillsammans med den del av uppdraget som omfattas av dessa tilläggsdirektiv, slutredovisas senast den 14 oktober 2022.

Frågan om reglerna om underrättelse till enskild om användning av hemliga tvångsmedel ska ändras

Säkerhets- och integritetsskyddsnämnden (SIN) inkom den 3 maj 2021 med en framställning om åtgärder för att förbättra enskildas rättssäkerhet i fråga om underrättelser om användning av hemliga tvångsmedel (Ju2021/01982). I framställningen anges bl.a. att det finns brister i dagens reglering som bör åtgärdas.

Mot bakgrund av SIN:s framställning får utredaren i uppdrag att

- särskilt bedöma om det finns ett behov av att ändra reglerna om underrättelse till enskild om användning av hemliga tvångsmedel, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Vid framtagandet av förslagen ska utredaren ta hänsyn till intresset av att undvika onödig regelbörda och administration.

Frågan om hemlig övervakning av elektronisk kommunikation ska få användas för att lokalisera personer som är häktade i sin frånvaro efter att en förundersökning har avslutats eller som har uteblivit eller avvikit från verkställighet av påföljder

Polismyndigheten inkom den 2 december 2019 med en framställning om lagändringar som förbättrar myndighetens möjligheter att eftersöka personer som är anhållna eller häktade i sin frånvaro eller som uteblivit eller avvikit från verkställighet av fängelsestraff eller rättspsykiatrisk vård (Ju2019/04054). Myndigheten efterfrågar en utökad tillgång till uppgifter, bl.a. om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

Utredaren ska enligt de ursprungliga direktiven bl.a. ta ställning till i vilka situationer hemlig övervakning av elektronisk kommunikation bör få användas för att lokalisera skäligen misstänkta och lämna förslag på de författningsändringar som bedöms nödvändiga. I uppdraget ingår därmed redan att överväga lagändringar som förbättrar möjligheterna att lokalisera personer som är anhållna eller häktade i sin frånvaro inom ramen för en förundersökning.

Mot bakgrund av Polismyndighetens framställning får utredaren även i uppdrag att

- ta ställning till om och i så fall i vilka situationer hemlig övervakning av elektronisk kommunikation bör få användas för att lokalisera personer som är häktade i sin frånvaro efter att en förundersökning har avslutats eller som har uteblivit eller avvikit från verkställighet av påföljder, och
- lämna förslag till författningsändringar som bedöms nödvändiga.

Det står utredaren fritt att föreslå att tillgång till sådana uppgifter som Polismyndigheten efterfrågar ska ges på något annat sätt än genom hemlig övervakning av elektronisk kommunikation. Utredaren ska säkerställa att en välfungerande systematik i regelverket om hemliga tvångsmedel upprätthålls i stort och i synnerhet i förhållande till förslag om att lokalisera skäligen misstänkta med hjälp av hemlig övervakning av elektronisk kommunikation. Utredaren ska vidare bedöma behovet av följdändringar i tillämplig lagstiftning om internationellt straffrättsligt samarbete.

Redovisning av uppdraget

Utredningstiden ligger fast för större delen av det ursprungliga uppdraget som ska redovisas i ett delbetänkande senast den 14 april 2022. Utredningstiden ska dock förlängas för frågan i de ursprungliga direktiven om i vilka situationer hemlig övervakning av elektronisk kommunikation bör få användas för att lokalisera skäligen misstänkta. Den frågan ska, tillsammans med den del av uppdraget som omfattas av dessa tilläggsdirektiv, slutredovisas senast den 14 oktober 2022.

(Justitiedepartementet)

Statens offentliga utredningar 2022

Kronologisk förteckning

1. Förbättrade åtgärder när barn misstänks för brott. Ju.
2. En skärpt syn på brott mot journalister och utövare av vissa samhällsnyttiga funktioner. Ju.
3. Sveriges tillgång till vaccin mot covid-19 – framgång genom samarbete och helgardering. S.
4. Minska gapet. Åtgärder för jämställda livsinkomster. A.
5. Innehållsvillkor för public service på internet – och ordningen för beslut vid förhandsprövning. Ku.
6. Hälso- och sjukvårdens beredskap – struktur för ökad förmåga. Del 1 och 2. S.
7. Kunskapsläget på kärnavfallsområdet 2022. Samhället, tekniken och etiken. M.
8. Rätt och rimligt för statligt anställda. Fi.
9. Avfallsbeskattning – En fråga om undantag? Fi.
10. Sverige under pandemin. Volym 1 Samhällets, företagens och enskildas ekonomi. Volym 2 Förutsättningar, vägval och utvärdering. S.
11. Handlingsplan för en långsiktig utveckling av tolktjänsten för döva, hörselskadade och personer med dövblindhet. S.
12. Startlån till förstagångsköpare av bostad. Fi.
13. Godstransporter på väg – vissa frågeställningar kring ett nytt miljöstyrande system. Fi.
14. Sänk tröskeln till en god bostad. Fi.
15. Sveriges globala klimatavtryck. M.
16. Ett förstärkt lagstöd för utlämnande av sekretesskyddade uppgifter till utlandet. Fö.
17. En modell för att mäta och belöna progression inom sfi. U.
18. EU:s förordning om terrorisminnehåll på internet – kompletteringar och ändringar i svensk rätt. Ju.
19. Utökade möjligheter att använda hemliga tvångsmedel. Ju.

Statens offentliga utredningar 2022

Systematisk förteckning