# Förenklat förfarande vid vissa beslut om hemlig avlyssning

*Betänkande av Utredningen om regeländringar för vissa hemliga tvångsmedel*

*Stockholm 2018*

STATENS OFFENTLIGA UTREDNINGAR

**SOU 2018:30**

SOU och Ds kan köpas från Norstedts Juridiks kundservice.
Beställningsadress: Norstedts Juridik, Kundservice, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: kundservice@nj.se
Webbadress: www.nj.se/offentligapublikationer

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

Layout: Kommittéservice, Regeringskansliet
Omslag: Elanders Sverige AB
Tryck: Elanders Sverige AB, Stockholm 2018

ISBN 978-91-38-24788-4
ISSN 0375-250X

# Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 12 maj 2016 att tillkalla en särskild utredare med uppdrag att utreda om svenska brottsbekämpande myndigheter ska ges möjlighet att använda hemlig dataavläsning. Samma dag förordnades Petra Lundh, lagman vid Södertörns tingsrätt, att vara särskild utredare. Som sekreterare anställdes från och med den 13 juni 2016 hovrättsassessorn David Caldevik. Utredningen antog namnet Utredningen om hemlig dataavläsning.

Den 19 oktober 2017 beslutade regeringen i tilläggsdirektiv (Dir. 2017:102) att utredningen också skulle analysera och ta ställning till om tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan knytas enbart till den person som åtgärden avser, i stället för till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning, samt föreslå de författningsändringar eller andra åtgärder som behövs. Utredningstiden förlängdes så att uppdraget i den del det avsåg tilläggsdirektiven skulle redovisas senast den 13 april 2018.

Uppdraget som avsåg hemlig dataavläsning redovisades den 16 november 2017 genom delbetänkandet *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet* (SOU 2017:89). Utredningen antog därefter ett nytt namn – Utredningen om regeländringar för vissa hemliga tvångsmedel.

Den 8 juni 2016 förordnades följande personer som experter att biträda utredaren: seniora strategiska rådgivaren Kurt Alavaara och chefsjuristen Per Lagerud vid Säkerhetspolisen, tidigare enhetschefen vid Säkerhets- och integritetsskyddsnämnden numera rådmannen Anna Backman vid Attunda tingsrätt, inspektören och gruppchefen Johan Dahl och it-teknikern Susanne Hedberg vid Nationella opera-

tiva avdelningen (NOA) inom Polismyndigheten, ämnesrådet Mikael Kullberg vid Justitiedepartementet, kammaråklagaren Mats Ljungqvist vid Riksenheten för säkerhetsmål och verksjuristen Lisbeth Tjärnkvist vid Tullverket. Den 22 juni 2016 förordnades ytterligare två experter; vice överåklagaren Bengt Lindholm vid Ekobrottsmyndigheten och generalsekreteraren Anne Ramberg i Sveriges advokatsamfund. Den 16 februari 2017 förordnades kammaråklagaren Hans Harding vid Åklagarmyndighetens Utvecklingscentrum Malmö som expert. Den 30 mars 2017 entledigades Mikael Kullberg från uppdraget som expert. Samma dag förordnades kanslirådet och tillförordnade enhetschefen Frida Göranson vid Justitiedepartementet som expert. Den 17 november 2017 entledigades Kurt Alavaara, Anna Backman, Johan Dahl, Frida Göranson, Susanne Hedberg och Mats Ljungqvist från uppdragen som experter. Samma dag förordnades enhetschefen Cecilia Agnehall vid Säkerhets- och integritetsskyddsnämnden, chefsjuristen Arne Andersson vid Polismyndighetens rättsavdelning och rättssakkunniga Heléne Åberg Benalal vid Justitiedepartementet som experter.

Utredningens experter har ställt sig bakom utredningens överväganden och förslag. Slutbetänkandet har därför skrivits i vi-form.

Härmed överlämnas slutbetänkandet *Förenklat förfarande vid vissa beslut om hemlig avlyssning* (SOU 2018:30). Utredningens uppdrag är härigenom slutfört.

Stockholm i april 2018

Petra Lundh

/David Caldevik

# Innehåll

## Bilagor

# Sammanfattning

## Vårt uppdrag

Vi har haft i uppdrag att analysera och ta ställning till om tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan knytas enbart till den person som åtgärden avser, i stället för till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning, och föreslå de författningsändringar eller andra åtgärder som behövs.

## Problemformulering

I vissa kriminella miljöer förekommer kommunikation via t.ex. flera telefoner med enda syfte att undvika eller försvåra avlyssning och övervakning. Det är särskilt två faktorer som framhållits från de brottsbekämpande myndigheterna som problem kopplade till att kriminella byter eller använder flera telefoner eller nummer som en metod för att undkomma och försvåra avlyssning eller övervakning. Den första är risken för bristande kontinuitet, nämligen att det kan uppstå ett glapp i den tid då avlyssning kan ske. Den andra faktorn är tidsaspekten, ur ett resursanvändningsperspektiv. Varje nytt tillstånd mot en person där det redan meddelats tillstånd till avlyssning innebär en onödig användning av åklagares, och många gånger också andra brottsbekämpande myndigheters tid. Även domstolars och offentliga ombuds tid tas i anspråk till följd av att kriminella sätter i system att byta eller använda flera telefoner eller nummer för att undvika och försvåra avlyssning.

## Tillståndet bör inte knytas enbart till person …

Vi har kommit till slutsatsen att de skäl som tidigare anförts i olika utredningar och propositioner om att domstol bör pröva kopplingen mellan det telefonnummer, den adress eller utrustning som avlyssning eller övervakning ska avse och den person som ska bli föremål för åtgärden fortfarande har starka skäl för sig och att det inte finns tillräckligt tungt vägande skäl för att knyta tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation enbart till person. Utan en sådan ordning skulle nämligen domstolens möjligheter att ta ställning till bland annat proportionaliteten i en begärd åtgärd inte låta sig göras. Det finns därför inte heller nu skäl att gå vidare med ett förslag om att knyta tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation enbart till person, eftersom en sådan ändring, mot bakgrund av hur den svenska regleringen på det hemliga tvångsmedelsområdet ser ut i övrigt, riskerar att få mer långtgående verkningar än att enbart komma till rätta med de problem som uppstår till följd av att vissa kriminella som metod för att försvåra eller undvika avlyssning eller övervakning byter eller använder flera nummer eller utrustningar.

## … däremot bör ett förenklat förfarande i vissa fall få tillämpas för att möta problemet

Sådana förhållandevis enkla motåtgärder från kriminella som att byta eller använda flera olika telefoner eller nummer för att undvika eller försvåra avlyssning utgör ett reellt problem ur effektivitetsperspektiv i den brottsbekämpande verksamheten. Detta eftersom de brottsbekämpande myndigheternas, och domstolarnas, resurser därigenom många gånger får användas vid sammanträden där utfallet knappast kan bli annat än att tillåta avlyssning även mot det nya numret eller den nya utrustningen som upptäckts efter att tidigare beslut om avlyssning börjat verkställas. Vi har därför kommit fram till att ett förenklat förfarande kan införas som innebär att det inte alltid ska ställas krav på sammanträde när frågan om ytterligare tillstånd till hemlig avlyssning av elektronisk kommunikation aktualiseras efter att ett tillstånd redan meddelats.

Det förenklade förfarandet ska bara få tillämpas när rätten redan har meddelat ett tillstånd till hemlig avlyssning av elektronisk kommunikation. Det tidigare tillståndet ska avse samma person och grundas på samma omständigheter som den nya ansökan eller anmälan för att det förenklade förfarandet ska kunna komma ifråga. Om så är fallet men den nya ansökan eller anmälan avser ett annat nummer eller en annan adress eller utrustning än det tidigare tillståndet får domstolen avgöra om det behövs ett sammanträde. Bedömer domstolen att det är utan betydelse med ett sammanträde behöver ett sådant inte hållas utan domstolen kan då fatta sitt beslut på handlingarna. Det grundläggande kravet på att ett offentligt ombud ska utses när en ansökan eller anmälan om hemlig avlyssning av elektronisk kommunikation kommit in till rätten gäller inte när rätten finner att ett sammanträde skulle vara utan betydelse. I stället ska ett offentligt ombud utses när rätten meddelat sitt beslut. På så vis kommer en granskning av rättens beslut till stånd och det är också möjligt för det offentliga ombudet att överklaga rättens beslut. Ett beslut som fattats med tillämpning av det förenklade förfarandet får inte avse annan tid än det tidigare meddelade tillståndet. Därigenom säkerställs både att ansökningar om förlängning av ett tidigare meddelat tillstånd inte blir föremål för prövning genom det förenklade förfarandet och att tillstånd som meddelats med tillämpning av det förenklade förfarandet ställs under rättens prövning vid sammanträde där ett offentligt ombud närvarar om det begärs förlängning av tillståndet.

## Konsekvenser och genomförande

Förslaget om ett förenklat förfarande för tillståndsprövning av ansökan om hemlig avlyssning av elektronisk kommunikation i vissa fall bedöms medföra att resurser inom Ekobrottsmyndigheten och Åklagarmyndigheten som i dag läggs på att åklagare infinner sig i rätten kommer att minska. Även domstolars resursåtgång kopplad till sammanträden bedöms minska. Resurserna som därigenom frigörs kommer därmed att kunna användas på annat håll inom rättsväsendet. Inga andra konsekvenser bedöms uppstå till följd av förslaget.

Den föreslagna lagändringen föreslås träda i kraft den 1 april 2019. Inga särskilda övergångsbestämmelser behövs. Tillämpningen av den föreslagna regleringen bör ingå i regeringens årliga redovisning till riksdagen.

# 1 Författningsförslag

## 1.1 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs i fråga om rättegångsbalken att det ska införas en ny paragraf, 27 kap. 28 a §, av följande lydelse.

**27 kap.**

28 a §

*Om rätten har meddelat tillstånd till hemlig avlyssning av elektronisk kommunikation får en ansökan eller anmälan om ytterligare tillstånd mot samma person och som grundas på samma omständigheter men avser ett annat telefonnummer, en annan adress eller en annan elektronisk kommunikationsutrustning än det tidigare tillståndet prövas utan sammanträde och utan att offentligt ombud utsetts om ett sammanträde skulle vara utan betydelse.*

*Ett tillstånd som har meddelats utan att sammanträde hållits enligt första stycket får inte avse annan tid än det tidigare tillståndet.*

*När rätten prövat en ansökan eller anmälan enligt första stycket ska ett offentligt ombud skyndsamt utses och underrättas om beslutet.*

---

Denna lag träder i kraft den 1 april 2019.

# 2 Utredningens uppdrag och arbete

## 2.1 Utredningsuppdraget

Regeringen beslutade genom tilläggsdirektiv, Dir. 2017:102, den 19 oktober 2017 att förlänga det uppdrag som vi tidigare hade fått genom Dir. 2016:36. I det nya uppdraget ingick att analysera och ta ställning till om tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan knytas enbart till den person som åtgärden avser, i stället för att också knytas till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning, och att föreslå de författningsändringar eller andra åtgärder som behövs. De ursprungliga direktiven och tilläggsdirektiven bifogas som bilaga 1 och 2.

## 2.2 Utredningsarbetet

Uppdraget har, mot bakgrund av direktivens utformning, inrymt överväganden inom en begränsad del av regleringen om hemliga tvångsmedel. Utredningen har haft löpande kontakter med experterna i den expertgrupp som funnits knuten till utredningen, såväl vid sammanträden med hela expertgruppen som vid enskilda möten och genom telefon och e-post. Utredningen har också tagit del av synpunkter från organisationer som inte funnits representerade bland de utsedda experterna, bl.a. Journalistförbundet och den ideella organisationen Dataskydd.net.

Eftersom det uppdrag vi fått genom tilläggsdirektiven saknar annan anknytning till det uppdrag som redovisades den 16 november 2017 med betänkandet *Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet* (SOU 2017:89) än att båda handlar

om hemliga tvångsmedel har vi under utredningsarbetet bytt namn på utredningen, från Utredningen om hemlig dataavläsning till Utredningen om regeländringar för vissa hemliga tvångsmedel.

## 2.3 Tolkning av direktiven och några avgränsningar

Utredningen har funnit anledning att, med utgångspunkt i direktiven, göra några inledande anmärkningar och avgränsningar. För det första är direktiven tydliga med att det som utredningsuppdraget omfattar är om det finns anledning att ändra reglerna om hemlig avlyssning och övervakning av elektronisk kommunikation så att *tillståndet* kan knytas enbart till person i stället för att också knytas till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning. Vi har därför inte ansett det som en del av vårt uppdrag att föreslå ändringar i de bakomliggande reglerna, exempelvis de som reglerar kopplingen mellan den enskilde som tvångsmedlet riktas mot och det telefonnummer, den adress eller den elektroniska kommunikationsutrustning som åtgärden ska avse, se t.ex. 27 kap. 20 § första stycket rättegångsbalken. Frågan har i stället snarast varit om det är domstol eller någon annan (t.ex. åklagaren eller den verkställande myndigheten) som ska göra prövningen av de bakomliggande reglerna.

För det andra anges inte någon begränsning i direktiven till förundersökning. Vår utgångspunkt har därför varit att de lagar som reglerar de nämnda tvångsmedlen, dvs. även de lagar som gäller underrättelseverksamhet, omfattas av vårt uppdrag. Det innebär att vår utredning, utöver att omfatta rättegångsbalkens regelverk, omfattar reglerna i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och lagen (1991:572) om särskild utlänningskontroll (LSU).

För det tredje har vi, utifrån att direktiven ger mandat att föreslå de författningsändringar eller andra åtgärder som behövs, ansett oss oförhindrade att föreslå andra regeländringar än att knyta tillståndet enbart till person, om det inte skulle finnas skäl för en sådan ändring. Vår begränsning såvitt avser möjliga författningsändringar har utgjorts av direktivens problemformulering.

## 2.4 Betänkandets disposition

Vårt författningsförslag har redan presenterats i kapitel 1. Efter det nu aktuella kapitlet följer kapitel 3, som innehåller en redovisning av gällande rätt på relevanta områden, och kapitel 4, där en bakgrund till framväxten av den svenska regleringen redovisas. I kapitel 5 finns sedan en redogörelse för dansk, finsk och norsk rätt på området. Våra överväganden och förslag presenteras i kapitel 6. I kapitel 7 redovisas konsekvenser av vårt förslag. Betänkandet avslutas med författningskommentaren i kapitel 8.

# 3 Gällande rätt

## 3.1 Inledning

Enligt direktiven ska vi analysera och ta ställning till om tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan knytas enbart till den person som åtgärden avser, i stället för att också knytas till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning. För att göra uppdraget mer överskådligt kommer vi i detta kapitel att redogöra övergripande för de generella förutsättningarna för och genomförande av de nämnda tvångsmedlen. Därefter redogör vi mer i detalj för regleringen om kopplingen mellan personen som åtgärden riktas mot och telefonnumret, adressen eller den elektroniska kommunikationsutrustningen som den ska avse, vilken är en helt central reglering för utredningen. Vi kommer också att kort komma in på andra hemliga tvångsmedel. Kapitlet avslutas med en redogörelse för några av de rättssäkerhetsgarantier som finns inbyggda i systemet avseende hemliga tvångsmedel och som är av särskild betydelse för vårt uppdrag.

Det ska dock inledningsvis nämnas att regler om hemliga tvångsmedel finns i fyra olika lagar. När det är fråga om åtgärder i en brottsutredning, dvs. när en förundersökning pågår, regleras användningen av hemliga tvångsmedel i rättegångsbalken. I det följande benämns dessa situationer för förundersökningsfallen. Det är också möjligt för brottsbekämpande myndigheter att under vissa förutsättningar få använda hemliga tvångsmedel för att förebygga eller förhindra brottslighet, dvs. i underrättelseverksamhet. De lagar som reglerar sådan tvångsmedelsanvändning är lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen) och lagen (1991:572) om särskild utlänningskontroll (LSU). Åtgär-

der som sker med stöd av dessa lagar eller någon av dem benämns i det följande underrättelsefallen.

Även i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet finns regler om hemlig tvångsmedelsanvändning. Eftersom varken hemlig avlyssning eller övervakning av elektronisk kommunikation, dvs. de två tvångsmedel som våra direktiv omfattar, regleras i den lagen har vi gjort bedömningen att våra förslag inte omfattar den lagen. Reglerna i den beskrivs eller behandlas därför inte vidare i betänkandet.

### 3.1.1 Grundläggande principer

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

### 3.1.2 Skyddet för den personliga integriteten

Utöver de nyss nämnda principerna måste också de grundläggande bestämmelser som har betydelse för det allmännas ansvar att skydda enskildas privatliv och integritet beskrivas i ett sammanhang som det förevarande. Sådana bestämmelser finns i bl.a. regeringsformen. Av målsättningsstadgandet i 1 kap. 2 § regeringsformen framgår att den offentliga makten ska utövas med respekt för alla människors lika värde och för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv.

Enligt 2 kap. 6 § första stycket regeringsformen gäller vidare att var och en gentemot det allmänna är skyddad mot bl.a. husrannsakan och liknande intrång, undersökning av brev eller annan förtrolig

försändelse samt hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Därtill gäller enligt paragrafens andra stycke ett skydd mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Skyddet enligt 2 kap. 6 § regeringsformen kan begränsas endast genom lag. Begränsningen får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar (2 kap. 20 och 21 §§ regeringsformen).

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

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

Konventionsrättigheterna får enligt artikel 8.2 Europakonventionen inte inskränkas annat än med stöd av lag och om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller för andra personers fri- och rättigheter. Det innebär att en inskränkning måste ha stöd i inhemsk lag som i sin tur uppfyller rimliga anspråk på rättssäkerhet, såsom att skydda mot godtycke, vara tillgänglig för allmänheten och förutsebar. Att inskränkningen måste vara nödvändig i ett demokratiskt samhälle för något av de i artikeln skyddade intressena innebär i huvudsak att det ska finnas ett angeläget samhälleligt behov av åtgärden och att den måste stå i rimlig proportion till det syfte som ska tillgodoses (Danelius s. 369 f.).

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

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

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

Europadomstolen har också slagit fast att nationell lagstiftning om dolda spaningsåtgärder eller hemliga tvångsmedel måste innehålla kontrollmekanismer för att skydda mot missbruk av den prövningsrätt som finns. Vad som krävs i det avseendet beror på omständigheter som åtgärdernas karaktär, räckvidd och varaktighet, vilka motiv som krävs för att besluta, utföra och övervaka dem samt vilken typ

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

av rättsmedel som finns i den nationella lagstiftningen. Beträffande telefonavlyssning har Europadomstolen ansett att beslutet normalt sett ska kontrolleras av domstol, åtminstone i sista instans.

Även i EU:s rättighetsstadga[2] finns en bestämmelse om rätt till respekt för bl.a. privatlivet, artikel 7. Av artikel 52.3 i stadgan följer att i den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen ska de ha samma innebörd och räckvidd som enligt konventionen.

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

## 3.2 Hemlig avlyssning av elektronisk kommunikation

Hemlig avlyssning av elektronisk kommunikation innebär att meddelanden, som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av innehållet i meddelandet. Åtgärden får under vissa i rättegångsbalken angivna förutsättningar tillåtas under förundersökning men kan, när förutsättningarna enligt preventivlagen eller LSU är uppfyllda, också få användas i underrättelseverksamhet.

Definitionen av begreppet elektroniskt kommunikationsnät finns i 1 kap. 7 § lagen om elektronisk kommunikation och förklaras där som ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs. Såvitt avser uttrycket adress framgår av förarbetena att det i begreppet ingår olika typer av nummer, t.ex. telefonnummer och andra identifikationsnummer och

[2] Europeiska unionens stadga om de grundläggande rättigheterna av den 7 december 2000, anpassad den 12 december 2007 i Strasbourg.

adresser, såsom e-postadresser (prop. 2011/2012:55 s. 62). Tvångsmedlet kan tillämpas på alla former av kommunikation genom elektroniska kommunikationsnät och är tillämpligt på muntlig och skriftlig kommunikation, liksom på datakommunikation.

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

1. Brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år.
2. Sabotage eller grovt sabotage enligt 13 kap. 4 eller 5 § brottsbalken.
3. Mordbrand, grov mordbrand, allmänfarlig ödeläggelse, kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 1, 2, 3, 5 a eller 5 b § brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel.
4. Uppror, väpnat hot mot laglig ordning eller brott mot medborgerlig frihet enligt 18 kap. 1, 3 eller 5 § brottsbalken.
5. Högförräderi, krigsanstiftan, spionerі, grovt spionerі, obehörig befattning med hemlig uppgift, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 1, 2, 5, 6, 7, 8, 10, 10 a eller 10 b § brottsbalken.
6. Företagsspionerі enligt 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att gärningen har begåtts på uppdrag av eller har understötts av en främmande makt eller av någon som har agerat för en främmande makts räkning.
7. Terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott, brott enligt 3 eller 3 a § lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller brott enligt lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.
8. Försök, förberedelse eller stämpling till något av de nu angivna brotten, om en sådan gärning är belagd med straff.

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

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

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

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

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

Tillstånd till hemlig avlyssning av elektronisk kommunikation enligt preventivlagen får också meddelas om det finns en påtaglig

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

Enligt 19–20 §§ LSU kan hemlig avlyssning av elektronisk kommunikation (som även i detta fall har samma innebörd som enligt rättegångsbalken) tillåtas om det är av betydelse för att utreda om en utlänning eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott och det finns synnerliga skäl.

## 3.3 Hemlig övervakning av elektronisk kommunikation

Hemlig övervakning av elektronisk kommunikation innebär enligt 27 kap. 19 § rättegångsbalken att uppgifter i hemlighet hämtas in om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress, vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Genom hemlig övervakning av elektronisk kommunikation får meddelanden även hindras från att nå fram. Tvångsmedlet ger, till skillnad från hemlig avlyssning av elektronisk kommunikation, inte tillgång till uppgifter om innehållet i meddelanden. Det som kan hämtas in är i stället trafikuppgifter och lokaliseringsuppgifter. Åtgärden får under vissa i rättegångsbalken angivna förutsättningar tillåtas under förundersökning men kan också tillåtas i underrättelseverksamhet enligt bestämmelserna i preventivlagen och LSU.

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

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

narkotikabrott enligt 1 § narkotikastrafflagen (1968:64) och narkotikasmuggling enligt 6 § första stycket lagen (2000:1225) om straff för smuggling.

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

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

När det gäller underrättelsefallen (enligt preventivlagen och LSU) gäller samma förutsättningar för tillstånd till hemlig övervakning av elektronisk kommunikation som för hemlig avlyssning enligt de lagarna, avseende såväl vilken brottslighet som kan aktualisera åtgärden som de övriga närmare förutsättningarna, se avsnitt 3.2.

## 3.4 Kopplingen mellan person och adress eller elektronisk kommunikationsutrustning

I samtliga de lagar som reglerar hemlig avlyssning och övervakning av elektronisk kommunikation finns regler som tar sikte på kopplingen mellan den person som ska bli föremål för tvångsmedelsanvändningen och det telefonnummer, den adress eller den elektroniska kommunikationsutrustning som tillståndet till tvångsmedelsanvändningen avser. I väsentliga delar överensstämmer regleringen mellan de olika lagarna men eftersom detta är en av nyckelfrågorna i betänkandet har vi valt att särredovisa vad som gäller enligt respektive lag.

### 3.4.1 Rättegångsbalken

Enligt 27 kap. 20 § första stycket 1 rättegångsbalken får hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation avse endast ett telefonnummer eller annan adress eller viss elektronisk kommunikationsutrustning som, under den tid som tillståndet gäller, innehas eller har innehafts av den misstänkte eller som annars kan antas ha använts eller komma att användas av denne. Åtgärden får emellertid också, enligt 27 kap. 20 § första stycket 2 rättegångsbalken, avse ett telefonnummer eller en annan adress eller viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att den misstänkte, under den tid som tillståndet avser, har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta. I 27 kap. 20 § andra stycket rättegångsbalken framgår vidare att hemlig övervakning av elektronisk kommunikation också får ske i syfte att utreda vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen. I de fallen uppställs inget krav på koppling mellan person och den adress eller utrustning åtgärden ska avse.

Av 27 kap. 21 § tredje stycket rättegångsbalken följer att det alltid i ett tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation ska anges vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område tillståndet avser. Den bestämmelsen gäller även när det enligt 27 kap. 20 § andra stycket rättegångsbalken inte krävs en viss koppling mellan den som ska bli föremål för åtgärden och den adress eller utrustning åtgärden ska avse.

### 3.4.2 Preventivlagen

Preventivlagen är beträffande kopplingen uppbyggd på i praktiken samma sätt som rättegångsbalken, dock med den skillnaden att det inte är till en misstänkt person som kopplingen ska föreligga utan i stället till en sådan person som kan bli föremål för åtgärd enligt den lagen (dvs. person som anges i 1 § preventivlagen). Således gäller enligt 2 § första stycket 1 preventivlagen att hemlig avlyssning eller övervakning av elektronisk kommunikation enligt den lagen endast får avse antingen ett telefonnummer eller annan adress

eller en viss elektronisk kommunikationsutrustning som under den tid tillståndet avser innehas eller har innehafts av den person som avses i 1 § preventivlagen eller annars kan antas ha använts eller komma att användas av honom eller henne. Liksom i förundersökningsfallen finns, enligt 2 § första stycket 2 preventivlagen, också möjlighet att låta tillståndet avse ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som det finns synnerlig anledning att anta att den person som avses i 1 § preventivlagen under den tid tillståndet avser har kontaktat eller kommer att kontakta. Någon möjlighet till motsvarande hemlig övervakning av elektronisk kommunikation som den som finns enligt rättegångsbalken för att ta reda på vem som är skäligen misstänkt föreligger inte enligt preventivlagen. Enligt 8 § andra stycket preventivlagen gäller att det i beslutet om tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation bl.a. ska anges vilket telefonnummer eller annan adress eller vilken elektronisk kommunikationsutrustning tillståndet avser.

### 3.4.3 LSU

Reglerna i LSU knyter an till rättegångsbalkens bestämmelser genom att det i 20 § första stycket LSU anges att rätten enligt 27 kap. rättegångsbalken kan meddela tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation. Vad som ovan sagts om balkens bestämmelser gäller således även enligt LSU, dock med den skillnaden att i stället för misstänkt person så ska kopplingen föreligga till en utlänning som kan bli föremål för åtgärd enligt LSU.

## 3.5 Något om andra hemliga tvångsmedel

### 3.5.1 Hemlig kameraövervakning

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

under vissa i rättegångsbalken angivna förutsättningar tillåtas under förundersökning men kan också tillåtas i underrättelseverksamhet enligt bestämmelserna i preventivlagen.

Enligt 27 kap. 20 a § andra stycket rättegångsbalken kan tillstånd till hemlig kameraövervakning lämnas vid förundersökning som rör de brott som kan aktualisera hemlig avlyssning av elektronisk kommunikation. Övervakningen får som huvudregel, i likhet med vad som gäller för hemlig avlyssning och övervakning av elektronisk kommunikation, användas endast om någon är skäligen misstänkt för brottet. Åtgärden får avse sådan plats där den skäligen misstänkte kan antas komma att uppehålla sig, 27 kap. 20 b § rättegångsbalken. Om det inte finns någon skäligen misstänkt för brottet får hemlig kameraövervakning användas för att övervaka den plats där brottet har begåtts eller en nära omgivning till denna plats, dock endast om syftet är att fastställa vem som skäligen kan misstänkas för brottet, 27 kap. 20 c § rättegångsbalken. Platsen ska anges i tillståndet, 27 kap. 21 § fjärde stycket rättegångsbalken.

När det gäller hemlig kameraövervakning enligt preventivlagen gäller samma förutsättningar för tillstånd till hemlig kameraövervakning som för hemlig avlyssning av elektronisk kommunikation avseende vilken (möjlig) brottslighet som kan aktualisera åtgärden, 1 § preventivlagen. Hemlig kameraövervakning enligt preventivlagen får endast avse en plats där den för tvångsmedlet aktuella personen kan antas komma att uppehålla sig eller en plats där den brottsliga verksamheten kan antas komma att utövas eller en nära omgivning till denna plats, 3 § preventivlagen. Platsen ska, liksom i förundersökningsfallen, anges i tillståndet, 8 § tredje stycket preventivlagen.

### 3.5.2 Hemlig rumsavlyssning

Hemlig rumsavlyssning innebär avlyssning eller upptagning som görs i hemlighet, och med ett tekniskt hjälpmedel som är avsett att återge ljud, och avser tal i enrum, samtal mellan andra eller förhandlingar vid sammanträden eller andra sammankomster som allmänheten inte har tillträde till. Tvångsmedlet får inte användas i underrättelseverksamhet utan endast, enligt 27 kap. 20 d § rättegångsbalken, vid en förundersökning om vissa i bestämmelsen angivna brott. De

brotten är som utgångspunkt allvarligare brott än de som kan föranleda användning av andra hemliga tvångsmedel.

Tvångsmedlet får användas endast när någon är skäligen misstänkt för ett angivet brott. Därtill gäller att åtgärden endast får avse en plats där det finns särskild anledning att anta att den misstänkte kommer att uppehålla sig. Avser åtgärden någon annan stadigvarande bostad än den misstänktes, får hemlig rumsavlyssning användas endast om det finns synnerlig anledning att anta att den misstänkte kommer att uppehålla sig där. Vissa platser får dessutom aldrig avlyssnas, 27 kap. 20 e § rättegångsbalken. Liksom vid hemlig kameraövervakning gäller att platsen ska anges i tillståndet enligt 27 kap. 21 § fjärde stycket rättegångsbalken.

## 3.6 Vissa rättssäkerhetsgarantier

Utöver de materiella förutsättningarna för tillstånd till de olika tvångsmedlen som presenterats i avsnitt 3.2–3.5 finns en rad bestämmelser som har till syfte att begränsa integritetsintrång och att garantera rättssäkerheten när hemliga tvångsmedel ska användas. Dessa bestämmelser har arbetats fram utifrån bl.a. de krav som enligt Europadomstolens praxis gäller enligt Europakonventionen och är av olika karaktär och avser olika områden. Mot bakgrund av hur våra direktiv är utformade har vi funnit anledning att här begränsa framställningen avseende bestämmelserna till sådana som vi bedömt vara av omedelbar relevans för uppdraget. En mer fullständig beskrivning av integritetsskyddsregler och rättssäkerhetsgarantier vid hemlig tvångsmedelsanvändning finns t.ex. i vårt delbetänkande Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89), avsnitt 3.5.

### 3.6.1 Domstolsprövning

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

Även i underrättelsefallen enligt preventivlagen och LSU gäller att det är domstol som prövar frågor om tillstånd till hemliga tvångsmedel. Enligt preventivlagen sker ansökan av åklagaren (6 § preventivlagen) medan yrkande enligt LSU framställs av Säkerhetspolisen eller Polismyndigheten (21 § LSU).

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

Enligt 6 a § preventivlagen finns en i huvudsak motsvarande möjlighet som i förundersökningsfallen till interimistiskt åklagarbeslut. Betydelsen av olägenheten av att inhämta rättens tillstånd är emellertid i den bestämmelsen knuten till möjligheterna att förhindra den brottsliga verksamheten i stället för, som i förundersökningsfallen, utredningen.

Vid prövningen av om det finns skäl att tillåta tvångsmedlet i fråga har domstolen (och, i förekommande fall, åklagaren), utöver prövningen av om de materiella och formella förutsättningarna är uppfyllda, alltid att avgöra om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse. Proportionalitetsprincipen finns kodifierad bl.a. i 27 kap. rättegångsbalken och 5 § preventivlagen men gäller, som redan nämnts, vid tillämpningen av all tvångsmedelslagstiftning. Det följer också direkt av lagtext att rätten, när det finns skäl till detta, ska ange villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan, se t.ex. 27 kap. 21 § sjätte stycket rättegångsbalken och 8 § fjärde stycket preventivlagen.

För att hemliga tvångsmedel ska få tillåtas ställs också upp vissa kvalificerande krav som tar sikte på behovet av åtgärden i det enskilda fallet. Således krävs att åtgärden är av synnerlig vikt för utredningen (rättegångsbalken), av synnerlig vikt för att förhindra brottslighet (preventivlagen) alternativt att det ska föreligga synnerliga skäl för åtgärden (LSU).

### 3.6.2 Offentliga ombud

Offentliga ombud ska bevaka enskildas integritetsintressen i ärenden hos domstol om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning. Samma regler om offentliga ombud gäller för förundersökningsfallen som för underrättelsefallen, i de senare genom hänvisning till rättegångsbalkens regler, 6 § preventivlagen och 21 § LSU. Däremot finns inte regler om offentligt ombud beträffande hemlig övervakning av elektronisk kommunikation.

Regeringen förordnar för tre år i sänder personer som får tjänstgöra som offentliga ombud. Ett offentligt ombud ska vara svensk medborgare och vara eller ha varit advokat alternativt ha varit ordinarie domare. Regeringen ska inhämta förslag på lämpliga kandidater från Sveriges advokatsamfund och Domarnämnden (27 kap. 27 § rättegångsbalken).

Ett offentligt ombud har rätt att ta del av vad som förekommer i ärendet, yttra sig i ärendet och överklaga rättens beslut (27 kap. 26 § rättegångsbalken). När en ansökan eller anmälan om hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning eller hemlig rumsavlyssning har kommit in till rätten ska rätten så snart som möjligt utse ett offentligt ombud i ärendet och hålla ett sammanträde. Vid sammanträdet ska åklagaren och det offentliga ombudet närvara (27 kap. 28 § rättegångsbalken). Vid hemlig övervakning av elektronisk kommunikation uppställs inget krav på sammanträde – vilket sammanhänger med att offentligt ombud inte ska utses vid ansökningar om det tvångsmedlet.

### 3.6.3 Säkerhets- och integritetsskyddsnämnden

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

Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan författning avhjälps (1 och 2 §§). Nämnden är också skyldig att på begäran av en enskild kontrollera om han eller hon har utsatts för hemliga tvångsmedel, samt om användningen av tvångsmedlen och därmed sammanhängande verksamhet har skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde om att kontrollen har utförts (3 §).

I vissa fall ska Säkerhets- och integritetsskyddsnämnden få underrättelse från åklagaren om vidtagna tvångsmedelsåtgärder. När underrättelse i efterhand till enskild om tvångsmedelsanvändningen har underlåtits på grund av sekretess, ska nämnden underrättas om detta.

# 4 Framväxten av dagens svenska reglering

I avsnitt 3.4 har vi redovisat hur regleringen ser ut beträffande kopplingen mellan den som ska bli föremål för hemlig avlyssning eller övervakning av elektronisk kommunikation och det telefonnummer eller annan adress eller den elektroniska kommunikationsutrustning som tillståndet avser samt vad tillståndet ska innehålla i detta avseende. Mot bakgrund av att dessa regler är helt centrala för denna utrednings vidkommande har vi funnit skäl att här redogöra för de bakomliggande skälen till bestämmelserna.

Regler om hemlig avlyssning av elektronisk kommunikation (tidigare benämnt hemlig telefonavlyssning och hemlig teleavlyssning) har funnits i rättegångsbalken sedan den infördes. Redan då krävdes att det fanns en koppling mellan den som skulle avlyssnas och, som det då hette, telefonapparaten.[1] I förarbetena till den ursprungliga bestämmelsen anfördes bl.a. att det med hänsyn till den stora betydelsen av telefonhemlighetens bevarande borde ställas upp stränga regler för ett ingrepp i denna. Processlagsberedningen anförde att rätt att besluta om sådan åtgärd uteslutande borde tillkomma rätten och att beslutet borde innefatta tillstånd till avhörande av samtal till och från telefonapparat som innehas av den misstänkte eller eljest kan antas komma att begagnas av honom. Det angavs särskilt att det i beslutet *bör angivas nummer eller annan beteckning å telefonapparat, som tillståndet skall avse*.[2] Några ytterligare skäl för att rättens beslut borde innefatta dessa uppgifter, som ju i praktiken utgör en koppling mellan den misstänkte och utrustningen, anfördes inte.

[1] Bestämmelsen om telefonavlyssning fanns vid balkens införande i 27 kap. 16 §.
[2] Se NJA II 1943 s. 367.

Regleringen om telefonavlyssning fanns, väsentligen oförändrad, kvar på samma plats i rättegångsbalken fram till år 1989. Då moderniserades bestämmelsen och flyttades till 27 kap. 18 § rättegångsbalken. Dessutom ändrades då benämningen från telefonavlyssning till hemlig teleavlyssning. I samma lagstiftningsärende infördes också det då nya hemliga tvångsmedlet hemlig teleövervakning. Gemensamma bestämmelser för de båda hemliga tvångsmedlen, bl.a. beträffande kopplingen mellan misstänkt och utrustning, infördes också. Enligt dåvarande 27 kap. 20 § rättegångsbalken gällde att avlyssningen eller övervakningen endast fick avse telefonapparat eller annan teleanläggning som innehades eller annars kunde antas komma att användas av den misstänkte. Detta var således något som domstolen skulle pröva innan tillstånd meddelades. I dåvarande 27 kap. 21 § rättegångsbalken angavs att tillstånd skulle meddelas att gälla för *viss tid och anläggning*.[3]

År 1995 infördes ändringar i rättegångsbalken som tog sikte på de bestämmelser som här diskuteras. Orden *telefonapparat* och *annan teleanläggning* ersattes i 27 kap. 20 § rättegångsbalken med begreppet *teleadress*. I 27 kap. 21 § rättegångsbalken föreskrevs att rätten i ett beslut att tillåta hemlig teleavlyssning eller teleövervakning skulle ange vilken adress tillståndet gällde. Regeringen konstaterade i förarbetena till lagändringarna att den dittillsvarande tekniska utvecklingen på teleområdet, främst framväxten av it, hade inneburit ett behov av förändringar, så att de närmast fysiska avgränsningarna (teleanläggning) skulle ersättas med mer neutrala begrepp för att bibehålla möjligheterna att verkställa hemliga tvångsmedel. I sammanhanget uttalade regeringen också att det inte var möjligt att reglera tillämpningsområdet för hemlig teleavlyssning och hemlig teleövervakning genom att endast låta åtgärden avse telemeddelanden med viss anknytning till den misstänkte och anförde i det sammanhanget följande.

> 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 teleavlyssning eller hemlig

[3] Se prop. 1988/89:124 s. 7.

> teleövervakning kan konkretiseras. I annat fall blir beslutet inte praktiskt verkställbart.[4]

Därefter konstaterade regeringen att genom att knyta tillståndet till en teleadress i stället för till en anläggning skulle man både undvika den fysiska begränsningen som gällde med tidigare uttryckssätt (som man alltså ville komma ifrån på grund av den tekniska utvecklingen) och uppnå det krav på konkretion som krävs från såväl integritetssynpunkt som verkställbarhetsperspektiv.

Frågan om kopplingen mellan person och tvångsmedel var också uppe i det lagstiftningsärende som föregick lagen (1995:1506) om hemlig kameraövervakning.[5] I det fallet gällde frågan om tillstånd till det nya tvångsmedlet skulle lämnas beträffande den person som skulle övervakas eller beträffande viss plats. Den dåvarande regeringen gjorde i det sammanhanget några mer uttryckliga uttalanden än vad som gjorts beträffande kopplingen mellan viss utrustning (eller adress) och person i förarbetena till reglerna om ”teletvångsmedlen”. Eftersom dessa uttalanden emellertid knyter an till de för all tvångsmedelsanvändning grundläggande principerna är de av intresse även i förevarande sammanhang.

> Frågan huruvida ett tillstånd till hemlig kameraövervakning skall 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 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. Vid en förundersökning som avser ett [visst] brott skulle, beroende på omständigheterna, övervakning av en allmän plats kanske anses vara godtagbar medan övervakning av en enskild plats, t.ex. genom att kameran riktades mot ett bostadsfönster, inte skulle kunna komma i fråga.[6]

Beredningen för rättsväsendets utveckling (BRU) föreslog år 2005 att kravet på att det i tillståndet ska anges vilket telefonnummer eller annan teleadress som hemlig avlyssning eller övervakning får avse skulle tas bort. BRU menade att den oerhört snabba tekniska utvecklingen och de metoder som de kriminella personerna använ-

[4] Prop. 1994/95:227 s. 20 f.
[5] Lagen om hemlig kameraövervakning är upphävd och reglerna har i allt väsentligt arbetats in i rättegångsbalkens bestämmelser om hemliga tvångsmedel.
[6] Prop. 1995/96:85 s. 29.

der för att undgå tvångsmedlen hade gjort att regeringens tidigare uttalanden om integritet och verkställighet behövde omprövas. Det var enligt BRU:s mening fullt tillräckligt att undersökningsledaren, efter domstolens beslut om att tillåta tvångsmedlen i förundersökningen fick avgöra utifrån vad lagstiftningen tillåter, t.ex. vilka identifierade enskilda telefonnummer eller e-postadresser som skulle omfattas av verkställigheten. Verkställighet av tvångsmedelsbeslutet kunde enligt BRU därefter begäras hos operatören. Med en sådan lösning menade beredningen att domstolarna inför beslut om tvångsmedlen skulle få all nödvändig information från åklagaren och, i förekommande fall, från det offentliga ombudet. Därigenom skulle det vara möjligt att göra en fullödig bedömning i tillståndsfrågan, bl.a. avseende det integritetsintrång som skulle uppkomma om tillstånd ges. BRU menade också att de villkor som domstolen ställer upp skulle kunna röra vissa typer av tekniska hjälpmedel och vissa särskilt identifierade hjälpmedel[7], som att avlyssning får avse en viss telefon enbart under viss tid. BRU erinrade också om att de brottsutredande myndigheterna genom proportionalitetsprincipen har en skyldighet att under hela verkställigheten se till att tvångsåtgärderna står i rimlig proportion till vad som står att vinna med dessa.[8]

Frågan om att knyta tillståndet enbart till person var också uppe till diskussion i betänkandet Hemliga tvångsmedel mot allvarliga brott. Det framfördes under den utredningens gång från brottsbekämpande myndigheter att det är ett betydande effektivitetshinder att en viss teleadress eller plats alltid måste anges i beslut om de olika formerna av hemlig avlyssning eller övervakning. Kravet att ange teleadress skapade enligt myndigheterna problem bl.a. eftersom bruket av anonyma sim-kort ökat och personer i kriminella kretsar ofta byter både kort och telefon för att undvika avlyssning. Myndigheterna ansåg att det borde vara tillräckligt att tillståndet knyts till en misstänkt person och att en behovs- och proportionalitetsbedömning sedan skulle få avgöra var åtgärden ska verkställas, med de begränsningar vad gäller bl.a. platsen som i övrigt följer av lag. Utredningen ansåg att det fanns ett behov av att effektivisera regleringen för att bättre hantera situationer när nya platser

[7] Beredningen föreslog att begreppet teleadress skulle utmönstras till förmån för *tekniska hjälpmedel.*
[8] Se SOU 2005:38 s. 199 f. BRU:s förslag i denna del ledde inte till lagstiftning.

eller teleadresser blir aktuella efter ett initialt domstolsbeslut om avlyssning eller övervakning. Utredningen delade emellertid den uppfattning som lagstiftaren tidigare uttryckt om att det är nödvändigt, inte minst från integritetssynpunkt, att lagstiftningen är utformad så att beslutsfattaren kan ta ställning till den konkreta åtgärd som avses vid tillståndsgivningen. Delar av den initiala tillståndsprövningen – till exempel tillämpningen av proportionalitetsprincipen – skulle enligt utredningen vara omöjlig, om beslutet inte var bestämt till plats, teleadress eller liknande. Däremot föreslog utredningen vissa förändringar av beslutsordningen (bl.a. avseende interimistiska beslut), vilka antogs huvudsakligen kunna tillgodose det aktuella behovet av effektivisering.[9]

Den dåvarande regeringen delade i prop. 2013/14:237 den bedömning som gjordes i det nyss angivna betänkandet och uttalade därvid bl.a. följande.

> Enligt de brottsbekämpande myndigheterna utgör kravet på att viss adress, utrustning eller plats ska anges i beslutet ett betydande effektivitetshinder i myndigheternas verksamhet. Till exempel har de pekat på det omfattande bruket av anonyma SIM-kort i kriminell verksamhet, där personer byter både kort och telefon ofta i syfte att undvika avlyssning eller övervakning. Den omständigheten att ett nytt beslut måste inhämtas vid varje sådant byte tar enligt Rikspolisstyrelsen tid och resurser i anspråk och innebär att möjligheterna att använda tvångsmedel fördröjs eller omöjliggörs. Säkerhetspolisen har också påtalat att teknikutvecklingen radikalt har förändrat förutsättningarna för bestämmelserna och ansett att det finns en uppenbar risk för att användningen av tvångsmedel kommer att minska eller helt upphöra på grund av att bestämmelserna inte är anpassade till de förutsättningar som den nya tekniken ger. Som exempel har angetts kommunikation som sker via IP-adresser, vilka i vissa fall byts ut för varje ny uppkoppling. Både Rikspolisstyrelsen och Säkerhetspolisen har också påpekat att en möjlighet att knyta ett tillstånd enbart till en viss person skulle kunna bidra till att säkerställa att det är rätt person som avlyssnas eller övervakas.
>
> Regeringen har förståelse för de synpunkter som de brottsbekämpande myndigheterna har framfört. Utredningens kartläggning visar att polisen i ett inte obetydligt antal fall med kort varsel får reda på t.ex. platsen för ett viktigt möte. Det innebär i vissa fall att ett domstolsbeslut om tvångsmedel inte kan inhämtas i tid. Ett stort antal av de tillstånd som meddelats till hemlig avlyssning av elektronisk kom-

[9] Se SOU 2012:44 s. 574 ff. och 581 f., jfr också synpunkter från Säkerhetspolisen angående den tekniska utvecklingen som skäl för att knyta tillstånd till person, s. 769 f.

munikation och hemlig övervakning av elektronisk kommunikation i sådana ärenden som utredningens kartläggning omfattar är också, bortsett från teleadressen, identiska med redan löpande tillstånd. Enligt utredningen meddelas dessa beslut inte sällan i mycket nära tidsmässig anslutning till varandra.

Det finns alltså en del som talar för att regleringen bör ändras för att bättre hantera situationer där nya platser eller adresser blir aktuella efter ett initialt domstolsbeslut om avlyssning eller övervakning. Samtidigt anser regeringen att integritets- och rättssäkerhetsskäl alltjämt talar för att lagstiftningen bör 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 försämras om åtgärden inte var bestämd till viss adress, plats eller liknande. Beslutsfattarens möjligheter att bedöma i vilken mån ett tillstånd behöver förenas med villkor för att tillgodose intresset av att enskildas integritet inte kränks i onödan skulle sannolikt också minska. Regeringen är därför nu inte beredd att ta bort kravet på att viss adress, utrustning eller plats ska anges i tvångsmedelsbeslutet.[10]

Regeringen menade i det aktuella lagstiftningsarbetet, liksom utredningen, att de ändringar som gjorts i beslutsordningen, bl.a. avseende möjligheten till interimistiska åklagarbeslut när ändamålet med åtgärden kunde gå förlorat i avvaktan på rättens beslut, torde kunna avhjälpa en del av den problematik som hade skisserats.

Det bör också i sammanhanget nämnas att en lagändring skedde avseende regleringen i 27 kap. 20 § första stycket rättegångsbalken år 2012 då begreppet teleadress utmönstrades och ersattes med den nuvarande lydelsen *telefonnummer eller annan adress eller viss elektronisk kommunikationsutrustning*.

När det gäller regleringen i preventivlagen och LSU har inga särskilda uttalanden gjorts beträffande kopplingen mellan den som utsätts för åtgärder (hemlig avlyssning eller övervakning av elektronisk kommunikation) och telefonnumret, adressen eller kommunikationsutrustningen. Detta trots att motsvarande bestämmelser som enligt rättegångsbalken gäller – dvs. det ska föreligga en sådan koppling och telefonnumret, adressen eller kommunikationsutrustningen ska anges i tillståndsbeslutet.

[10] Prop. 2013/14:237 s. 97.

# 5 Nordisk utblick

## 5.1 Danmark

Regler som motsvarar de svenska tvångsmedlen hemlig avlyssning och övervakning av elektronisk kommunikation (telefonaflytning och teleoplysning) finns i den danska retsplejelovens 71 kap. Enligt första stycket första punkten i § 780 retsplejeloven kan polisen, på de villkor som framgår av lagens 71 kapitel avlyssna ”telefonsamtaler eller anden tilsvarende telekommunikation (telefonaflytning)”. Enligt tredje punkten i samma stycke kan polisen inhämta upplysning om ”hvilke telefoner eller andre tilsvarende kommunikationsapparater der sættes i forbindelse med en bestemt telefon eller andet kommunikationsapparat, selv om indehaveren af dette ikke har meddelt tilladelse hertil (teleoplysning)”. För tillgång till avlyssning krävs att det ”er bestemte grunde til at antage, at der på den pågældende måde gives meddelelser eller foretages forsendelser til eller fra en mistænkt” och att åtgärden ”må antages at være af afgørende betydning for efterforskningen”, se första stycket punkterna 1 och 2 i § 781. De brott som kan föranleda åtgärden är enligt tredje punkten i nyss nämnda lagrum sådana som kan bestraffas med fängelse i sex år eller mer och vissa andra, i lagen angivna, brott. Ett tillstånd till telefonaflytning avser inte bara telefonsamtal, utan också ”anden tilsvarende telekommunikation”, som e-post och sms. Åtgärden kan dock endast riktas mot meddelanden som är under transport mellan avsändare och mottagare.

Beträffande frågan om vad som ska anges i tillståndet gäller enligt första stycket i § 783 retsplejeloven som huvudregel att det i rättens tillstånd ska anges de ”telefonnumre, lokaliteter, adressater eller forsendelser, som indgrebet angår”. I paragrafens andra stycke anges dock ett antal brott för vilka undantag från huvudregeln gäller vid telefonaflytning och teleoplysning. Det är fråga om mycket

allvarlig brottslighet, bl.a. brott mot statens självständighet och säkerhet, brott mot statsförfattningen och de översta statsmyndigheterna, terrorism m.m. När det är fråga om sådana brott kan rätten, utöver bestämda telefonnummer, i tillståndet ange den person som ”indgrebet angår (den mistænkte)”. När ett tillstånd meddelats mot en person kan polisen under tillståndstiden löpande verkställa avlyssning eller övervakning av de kommunikationsmedel som det finns bestämd grund att anta att den misstänkte använder, utan ytterligare domstolstillstånd (kendelser). Om rätten meddelar tillstånd mot person ska polisen snarast möjligt efter att den tid då åtgärden får vidtas underrätta rätten om det telefonnummer som åtgärden har riktats mot, vilka inte angetts i tillståndet. Talar särskilda skäl (særlige forhold) för det ska sådan underrättelse ske senast 24 timmar efter åtgärdens igångsättande. En underrättelse till rätten ska innehålla de grunder som det finns att anta att det från det aktuella telefonnumret sänds meddelanden till eller från den misstänkte. Rätten ska i sin tur underrätta den ”beskikkede advokat”, som därefter kan begära att rätten prövar lagligheten av åtgärden. Om åtgärden enligt rättens bedömning inte borde ha företagits ska rätten informera det danska Justitieministeriet.

De danska reglerna om koppling till person infördes år 2006 och kom till efter rapporten *Det danske samfunds indsats og beredskab mod terror* av D*en tværministerielle arbejdsgruppe om terrorbekæmpelse*. I rapportens anbefaling nr 26 angavs att det skulle möjliggöras att rättens beslut om ingrepp i meddelelseshemmeligheden kan vara riktat mot personen och inte kommunikationsmedlen. De skäl som anfördes för ändringen var följande (översättning av utredningen).

> Erfarenheten visar att en del misstänkta försöker dölja sina handlingar genom att använda flera olika kommunikationsmedel eller kommunikationsanläggningar. Det kan exempelvis vara olika telefoner eller simkort som byts ut löpande. Det erinras i det avseendet om att den tekniska utvecklingen under de senare åren har inneburit att såväl antalet som tillgängligheten av de till buds stående kommunikationsmedlen har ökat betydligt. Om en misstänkt använder flera olika kommunikationsmedel krävs att det inhämtas ett beslut av rätten för varje kommunikationsmedel. Det medför att det ska hållas ett sammanträde varje gång, som involverar domare och försvarare samt att polisen ska förbereda saken inför sammanträdet. Om det skapas möjlighet för att rättens beslut får gälla personen och inte kommunikationsmedlet kommer det att kunna sparas resurser hos både domstol och polisen, vilket också erfarenheter från utlandet har visat. Det förutsätts att

polisen inför rätten bevisar att den person som ingreppet riktas mot använder ett flertal kommunikationsmedel och att rätten i efterhand informeras om vilka kommunikationsmedel personen som beslutet avser har använt.[1]

## 5.2 Finland

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

Regler om hemliga tvångsmedel finns i 10 kap. tvångsmedelslagen (förundersökning) och 5 kap. polislagen (förebyggande eller förhindrande av brott). I allt väsentligt motsvarar bestämmelserna varandra och fortsättningsvis presenteras endast det som gäller enligt tvångsmedelslagen. De tvångsmedel som i Finland motsvarar de svenska tvångsmedlen hemlig avlyssning och övervakning av elektronisk kommunikation kallas där teleavlyssning och teleövervakning.[2] Med teleavlyssning avses enligt 10 kap. 3 § tvångsmedelslagen att ett meddelande som tas emot av eller sänds från en viss teleadress eller teleterminalutrustning genom ett allmänt kommunikationsnät eller ett därtill anslutet kommunikationsnät avlyssnas, upptas eller behandlas på något annat sätt för utredning av innehållet i meddelandet och de identifieringsuppgifter i anslutning till det som avses i reglerna om teleövervakning. Teleavlyssning får riktas endast mot meddelanden från eller meddelanden avsedda för en person som är misstänkt för brott. Förundersökningsmyndigheten kan ges tillstånd att rikta teleavlyssning mot en teleadress eller teleterminalutrustning som en misstänkt innehar eller annars kan antas använda,

[1] Se Det danske samfunds indsats og beredskab mod terror, Den tværministerielle arbejdsgruppe om terrorbekæmpelse, oktober 2005, s. 76.
[2] Till skillnad från i Sverige där inhämtning av lokaliseringsuppgifter är en del av hemlig övervakning av elektronisk kommunikation finns det i Finland dock särskilda bestämmelser om inhämtande av lägesuppgifter och inhämtande av basstationsuppgifter i 10 kap. 8 och 10 §§ tvångsmedelslagen.

om den misstänkte är skäligen misstänkt för vissa i lagen särskilt angivna allvarliga brott.

Med teleövervakning avses enligt 10 kap. 6 § tvångsmedelslagen att identifieringsuppgifter inhämtas om ett meddelande som har sänts från en teleadress eller teleterminalutrustning som är kopplad till ett kommunikationsnät som avses i 3 § eller som har mottagits till en sådan adress eller sådan utrustning och att uppgifter om en teleadress eller teleterminalutrustnings läge inhämtas eller att det tillfälligt förhindras att adressen eller utrustningen används. Förundersökningsmyndigheten kan ges tillstånd att rikta teleövervakning mot en teleadress eller teleterminalutrustning som en misstänkt innehar eller annars kan antas använda, om den misstänkte är skäligen misstänkt för vissa i lagen angivna brott av visst allvar.

För såväl teleavlyssning som teleövervakning gäller att rätten i beslut om att tillåta åtgärderna ska ange *den teleadress eller teleterminalutrustning som åtgärden riktas mot*, se 10 kap. 5 § tredje stycket 5 och 10 kap. 9 § fjärde stycket 6 tvångsmedelslagen. Ett yrkande som gäller hemliga tvångsmedel ska enligt 10 kap. 43 § andra stycket tvångsmedelslagen utan dröjsmål tas upp till behandling i domstol i närvaro av den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman som är insatt i ärendet. Som ett undantag från detta krav gäller enligt tredje stycket i den nämnda paragrafen emellertid att om domstolen har beviljat tillstånd till teleavlyssning eller teleövervakning, får den pröva och avgöra ett ärende som gäller beviljande av tillstånd i fråga om en ny teleadress eller teleterminalutrustning utan att den tjänsteman som framställt yrkandet eller en av denne förordnad tjänsteman är närvarande, om det har förflutit mindre än en månad från den muntliga förhandlingen i ett tillståndsärende som gäller samma misstänkta person och samma misstanke om brott.

Beträffande den sistnämnda regleringen, som ju ligger i linje med det vi har att utreda, uttalade den finska regeringen följande vid införandet av den.

> I praktiken begränsas en ändamålsenlig och effektiv användning av både förundersökningsmyndighetens och domstolens resurser av att alla ärenden som gäller byte av teleadresser och teleterminalutrustning ska behandlas i sammanträde. Problemen accentueras när en brottsmisstänkt avsiktligen byter teleadresser eller teleterminalutrustning mycket ofta. Användningen av dylikt förenklat förfarande ska kunna prövas av domstolen och det ska kunna användas endast när tillståndet

är i kraft. Tillståndsärendet ska alltså behandlas minst en gång i månaden i närvaro av den tjänsteman som ser till att yrkandet framställs. En ytterligare förutsättning för förenklat förfarande ska vara att det är fråga om samma brottsmisstänkta person och samma brottsmisstanke som i det tidigare beviljade tillståndet.[3]

## 5.3 Norge

I Norge regleras hemliga tvångsmedel i straffeprosessloven. Tvångsmedel som motsvarar hemlig avlyssning och övervakning av elektronisk kommunikation benämns gemensamt som kommunikasjonskontroll och finns i straffeprosesslovens kapitel 16 a. I § 216 a straffeprosessloven föreskrivs att rätten genom beslut kan ge polisen tillåtelse att företa kommunikasjonsavlytting när någon med skjellig grunn misstänks för en handling eller försök till handling som enligt lagen kan bestraffas med fängelse i tio år eller mer samt för vissa andra i lagen angivna allvarliga brott. Kommunikasjonsavlytting kan bestå i att avlyssna samtal eller annan kommunikation till och från *bestemte* telefoner, datorer eller andra anläggningar för elektronisk kommunikation som den misstänkte besitter eller kan antas använda.

I § 216 b straffeprosessloven regleras vad som kan liknas vid hemlig övervakning av elektronisk kommunikation, benämnt annen kontroll av kommunikasjonsanlegg. Den åtgärden får efter rättens beslut användas när någon med skjellig grunn misstänks för en handling eller försök till handling som enligt lagen kan bestraffas med fängelse i fem år eller mer samt för vissa särskilt angivna brott. Även beträffande det här angivna tvångsmedlet gäller kravet på *bestemte* telefoner, datorer eller andra anläggningar för elektronisk kommunikation som den misstänkte besitter eller kan antas använda.

I formuleringen *bestemte* ligger ett krav på att anläggningen som ska avlyssnas eller kontrolleras måste identifieras i rättens tillstånd, se den norska propositionen Prop. 68 L (2015–2016) s. 118 p. 7.5.1 och där angivna hänvisningar. Det är således inte möjligt att i Norge knyta tillståndet enbart till den person som ska avlyssnas eller kontrolleras. Frågan om att ändra på dessa bestämmelser var uppe till prövning i den angivna norska propositionen.[4] Den ut-

[3] RP 222/2010 s. 364.
[4] Följande är hämtat från den norska propositionen Prop. 68 L (2015–2016) avsnitt 7.5 (s. 118 ff.).

redning (Metodekontrollutvalget) som hade behandlat frågan fann att en sådan ordning skulle ge polisen för stor befogenhet och att möjligheterna till kontroll av tvångsmedelsanvändningen i allt för hög grad skulle försvagas om tillståndet knöts till person. Metodekontrollutvalget behandlade också frågan om att införa en regel liknande den som gäller i dansk rätt enligt 783 § andra stycket retsplejeloven (se avsnitt 5.4.1). Utredningen framhöll att en sådan lösning i och för sig på ett bättre sätt än om tillståndet knöts endast till person skulle tillvarata rättssäkerhetsaspekter, genom att information om avlyssnade telefonnummer förmedlades via domstolen till den utsedde advokaten. Den danska lösningen hade dock enligt Metodekontrollutvalget klara svagheter. Genom att domaren ska vidarebefordra relevanta upplysningar till den utsedda advokaten sätts domaren i en, enligt norsk rätt, okänd sits eftersom denne då lämnar sin sedvanliga roll som enbart kontrollfunktion. Enligt utredningens mening skulle den danska ordningen dessutom lägga för stor kontrollfunktion hos den utsedda advokaten, vilket ansågs stå i motsättning till det norska systemet där åklagarmyndigheten framställer en begäran till domstolen som denna tar ställning till efter att ha hört advokatens inställning.

Metodekontrollutvalget ifrågasatte i och för sig inte att det är resurskrävande att framställa nya begäranden om kommunikasjonskontroll varje gång en misstänkt byter telefon eller sim-kort. Enligt utvalgets mening kunde emellertid möjligheten till interimistiska åklagarbeslut användas för att utredningen inte skulle bli lidande av ett sådant agerande av kriminella. I det sammanhanget utvärderade Metodekontrollutvalget också om det kunde vara lämpligt att ”samla upp” flera tillkommande anläggningar som beslutats interimistiskt av åklagaren till en samlad framställning till rätten efter en viss tidsperiod. Utvalgets konklusion av en sådan lösning blev emellertid att den i allt för hög grad skulle minska domstolens efterföljande kontroll av åklagarmyndighetens användning av sin interimistiska beslutanderätt.

Den norska regeringen anslöt sig till det som Metodekontrollutvalget framhållit och konstaterade bl.a. att flera remissinstanser på polis- och åklagarsidan instämde i, eller hade förståelse för, utredningens slutsatser. Regeringen anförde också att resurshänsyn inte ensamt kan läggas till grund för en ändring och att det, även om det inte finns anledning att tro att polisen skulle missbruka en

utvidgad befogenhet, finns skäl att sträva efter ett system som i så hög grad som möjligt förhindrar missbruk.

# 6 Förslag

## 6.1 Problemformulering

Som framkommit av tidigare text krävs domstolens tillstånd för varje telefonnummer, annan adress eller elektronisk kommunikationsutrustning som hemlig avlyssning eller övervakning av elektronisk kommunikation ska avse. Det är ett välkänt faktum att det i vissa kriminella miljöer förekommer kommunikation via t.ex. flera telefoner med enda syfte att undvika eller försvåra avlyssning och övervakning. I olika sammanhang har det från brottsbekämpande myndigheter framhållits att frekventa byten eller användning av flera sim-kort eller telefoner utgör problem för de myndigheter som ska verkställa hemliga tvångsmedel eftersom varje ny telefon eller varje nytt nummer fordrar dels att en adress identifieras, vilket kan vara tidsödande, dels ett nytt beslut.

Det är särskilt två faktorer som framhållits från de brottsbekämpande myndigheterna som problem kopplade till att kriminella byter eller använder flera telefoner eller nummer som en metod för att undkomma och försvåra avlyssning eller övervakning. Den första är risken för bristande kontinuitet, nämligen att det kan uppstå ett glapp i den tid då avlyssning kan ske. Detta glapp är dels den tid det tar i anspråk att identifiera ett nytt nummer och knyta det till den misstänkte, dels den tid det tar från att sådan identifiering skett tills ett nytt tillstånd finns på plats och inkoppling av den nya avlyssningen eller övervakningen kan ske. Inom ramen för denna utredning är det den första delen av det andra ledet av denna problematik, dvs. möjligheterna att få ett nytt tillstånd på plats, som är föremål för överväganden.

Den andra faktorn som de brottsbekämpande myndigheterna framhållit som problematisk är tidsaspekten, ur ett resursanvändningsperspektiv. Varje nytt tillstånd mot en person där det redan

meddelats tillstånd till avlyssning innebär, enligt myndigheterna, att åklagares, och många gånger också andra brottsbekämpande myndigheters resurser används i onödan. Även domstolars och offentliga ombuds tid används till följd av att kriminella sätter i system att byta eller använda flera telefoner eller nummer för att undvika och försvåra avlyssning. Anledningen till att resursanvändningen anses onödig är enligt de brottsbekämpande myndigheterna att det i många fall knappast utgör ett större integritetsintrång att rikta avlyssning eller övervakning mot ett nytt nummer, en ny adress eller en ny utrustning i de fall det redan finns ett tidigare tillstånd mot samma person.

## 6.2 Omfattning av problemen

När det gäller omfattningen av den redovisade problematiken går det att dra vissa slutsatser av den årliga redovisningen från regeringen till riksdagen om användningen av hemliga tvångsmedel. Sedan år 2013 finns i den uppgifter om såväl antalet tillstånd till tvångsmedlen, dvs. antalet telefonnummer, andra adresser eller utrustningar som åtgärderna får avse, som antalet personer det meddelats tillstånd att rikta avlyssning eller övervakning mot. I tabellen nedan framgår hur utvecklingen beträffande hemlig avlyssning av elektronisk kommunikation i det avseendet har sett ut sedan den redovisningen inleddes.[1]

**Tabell 6.1 Genomsnittligt antal tillstånd till hemlig avlyssning av elektronisk kommunikation per avlyssnad person**

| | 2012 | 2013 | 2014 | 2015 | 2016 |
|---|---|---|---|---|---|
| Antal personer | 1 268 | 1 251 | 1 235 | 1 158 | 1 253 |
| Antal tillstånd | 3 432 | 3 384 | 3 564 | 3 465 | 3 456 |
| **Antal tillstånd per person** | **2,71** | **2,71** | **2,89** | **2,99** | **2,75** |

[1] Uppgifterna är hämtade från regeringens skrivelser med redovisning om användningen av hemliga tvångsmedel för år 2013–2016, Skr 2014/15:36, 2015/16:49, 2016/17:69 och 2017/18:69 och avser hemlig avlyssning av elektronisk kommunikation i Ekobrottsmyndighetens, Polismyndighetens och Tullverkets verksamheter. Beräkningen av antal tillstånd per person är dock gjord av utredningen.

Som framgår av tabellen meddelas alltså i genomsnitt knappt tre tillstånd per person såvitt avser hemlig avlyssning av elektronisk kommunikation.[2] Statistiskt sett synes det emellertid inte vara ett ökande problem under den aktuella perioden att de personer som ska bli föremål för avlyssning byter, innehar eller använder flera telefoner eller sim-kort.

Såvitt avser Säkerhetspolisen redovisas inte den myndighetens uppgifter på motsvarande vis i den årliga redovisningen, till följd av sekretess. Från Säkerhetspolisens expert i utredningen har emellertid följande uppgifter inhämtats. Vid cirka 20 procent av de tillstånd där tvångsmedlen verkställs under mer än en månad beslutas det om utökning/ändring av telefonnummer, annan adress eller utrustning under den totala tillståndstiden. Omkring 50 procent av utöknings-/ändringsbesluten fattas vid sammanträden som enbart avser just den frågan och som alltså inte rör frågan om förlängning av tillståndstiden för tvångsmedlet som sådant.

Åklagarmyndighetens expert i utredningen har upplyst om att det inte är alltigenom relevant att beräkna antalet tillstånd per person som ett genomsnitt av samtliga beslut. Det har helt enkelt att göra med att det kan skilja sig mycket från fall till fall och att strategierna med att byta eller använda flera olika nummer eller utrustningar primärt förekommer i vissa kriminella kretsar. I många ärenden aktualiseras inte mer än ett eller två telefonnummer eller adresser eller utrustningar per person vid avlyssningen. Det innebär att antalet tillstånd som aktualiseras i övriga ärenden kan vara väsentligt fler än de som genomsnittsuppgifterna ovan ger vid handen. Någon statistik förs emellertid inte avseende hur vanligt det är i enskilda ärenden att det tillkommer sammanträden endast till följd av att nya nummer, adresser eller utrustningar upptäcks efter att ett inledande tillstånd har meddelats. För att ändå kunna få ett begrepp om omfattningen i enskilda ärenden har vi begärt in uppgifter från Åklagarmyndighetens expert i utredningen. Han har försett utredningen med dels exempel på antalet tillstånd som meddelas i enskilda ärenden, dels exempel på antalet sammanträden per misstänkt som hållits i enskilda ärenden. Exemplen är verkliga men

[2] Det ska framhållas att ett tillstånd alltid innefattar endast ett nummer, en annan adress eller utrustning. Om en ansökan således t.ex. avser tre nummer, adresser eller utrustningar och tillstånd ges till samtliga blir det alltså fråga om tre tillstånd.

ger tyvärr inte en helt säker bild av hur vanligt förekommande den exakta problematiken är, dvs. att kriminella byter eller använder flera telefoner eller sim-kort för att försvåra eller undvika avlyssning vilket får till följd att ett flertal sammanträden aktualiseras i samma ärende.

När det gäller antalet tillstånd i enskilda ärenden har två åklagarkamrars samtliga beslut under två månader kontrollerats i det diarieföringssystem där de hemliga tvångsmedlen registreras. I det ärende (vilket inkluderade fyra misstänkta) som hade flest beslut om hemlig avlyssning av elektronisk kommunikation under den perioden hade det meddelats 26 tillstånd avseende nya adresser. I det ärende med bara en misstänkt som hade flest antal tillstånd hade 17 tillstånd meddelats under samma tid. Uppgifterna säger dock inte något om antalet tillfällen som åklagare behövde infinna sig i rätten för nya beslut (eftersom flera nya telefonnummer, adresser eller elektroniska kommunikationsutrustningar kan innefattas i ett och samma beslut och vid samma sammanträde). Detta till trots ger de ändå en fingervisning om systematiken hos vissa kriminella och om att det kan bli nödvändigt att infinna sig i rätten flera gånger efter att domstolen har konstaterat att det i och för sig finns förutsättningar för hemlig avlyssning av elektronisk kommunikation riktad mot en viss person.

Vidare har utredningens åklagarexpert hämtat in exempel från fyra åklagarkamrar beträffande antal besök i rätten i olika ärenden. Siffrorna utgör en summering av det totala antalet sammanträden per misstänkt person, utan hänsyn till att sammanträden kan ha hållits beträffande fler än en misstänkt vid ett och samma tillfälle. Det är fråga om uppgifter som inte finns lagrade elektroniskt utan som kräver manuell kontroll av akterna i de enskilda ärendena. Det underlag som utredningen därefter fått in, bestående av åtta exempelärenden med olika antal misstänkta, visar att det i vissa ärenden är vanligt med mer än ett sammanträde per misstänkt och månad, vilket är minimiantalet sammanträden som krävs per misstänkt och månad enligt nuvarande lagstiftning (27 kap. 21 § andra stycket och 27 kap. 28 § första stycket rättegångsbalken).[3]

[3] Det bör nämnas att Utredningen om rättssäkerhetsgarantier vid användningen av vissa hemliga tvångsmedel (Ju 2017:04) vid möten med olika aktörer som arbetar med hemliga tvångsmedel fått uppgift om att tillståndstiden för hemlig avlyssning av elektronisk kommunikation nästan alltid bestäms till en månad från beslutet. Undantag sker i praktiken

Exempelärendena består av två ärenden med en misstänkt, tre ärenden med fyra misstänkta, ett ärende med fem misstänkta och två ärenden med sex misstänkta. De varierar i tid mellan tre och nio månader. I det exempelärende med minst antal sammanträden har det hållits fyra sammanträden utöver minimiantalet. Ärendet avsåg en misstänkt person i fem månaders tid. I ärendet med flest antal sammanträden har det hållits 50 sammanträden utöver minimiantalet, beträffande sex misstänkta under nio månader. Det ärende där flest sammanträden hölls under kortast tid var det med fem misstänkta. Där hölls första månaden 31 sammanträden utöver det inledande, varav 18 sammanträden avsåg två av de misstänkta. I övriga ärenden har det, utöver minimiantalet, hållits 13 sammanträden i två ärenden (dels en misstänkt i tre månader, dels fyra misstänkta under tre månader), 14 sammanträden (fyra misstänkta under fem månader), 16 sammanträden (fyra misstänkta under tre månader) och 24 sammanträden (sex misstänkta under sex månader). I de åtta exempelärendena har det totalt hållits 169 sammanträden utöver minimiantalet sammanträden. Sammanträdena kan dock, som nämnts, ha samordnats inom respektive ärende så att åklagare inte har behövt infinna sig i rätten 169 gånger, t.ex. genom att flera nya nummer prövas i ett sammanhang beträffande flera misstänkta. Det kan dessutom inte med säkerhet sägas att samtliga tillkommande sammanträden avsett fall då misstänkta personer haft som strategi att byta eller använda flera sim-kort eller telefoner. Dock kan på goda grunder så antas vara fallet vid majoriteten av sammanträdena.

## 6.3 Bör tillståndet knytas enbart till person?

Utredningens bedömning: Det finns inte tillräckligt tungt vägande skäl för att knyta tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation enbart till person.

Skälen enligt direktiven för att överväga ändringar avseende att i tillståndet ange enbart person i stället för nummer, annan adress

främst av samordningsskäl (för att samtliga tillstånd senare ska kunna prövas vid ett sammanträde om förlängning begärs) när det är fråga om tillkommande nummer, adresser eller utrustningar som upptäcks efter det inledande beslutet.

eller elektronisk kommunikationsutrustning är att det i kriminella kretsar är vanligt med anonyma sim-kort och att personer byter både kort och telefon enbart i syfte att undvika eller försvåra avlyssning eller övervakning. Som framkommit av de exempel som redovisats i föregående avsnitt kan kriminellas agerande i vissa ärenden i allra högsta grad påverka hur resurserna hos de brottsbekämpande myndigheterna används. En sådan ordning – där alltså kriminellas motåtgärder mot brottsbekämpningens metoder får en direkt påverkan på hur resurserna hos de brottsbekämpande myndigheterna används – är inte godtagbar. Frågan är dock om den lösning som vi har att utreda, dvs. att tillståndet knyts enbart till person är den mest ändamålsenliga utifrån såväl behovs- och effektivitetsresonemang som rättssäkerhets- och integritetsperspektiv.

Frågan om att knyta tillståndet enbart till person övervägdes av den dåvarande regeringen så sent som år 2014. Då anfördes att integritets- och rättssäkerhetsskäl alltjämt talade för att lagstiftningen bör vara utformad på ett sådant sätt att beslutsfattaren kan ta ställning till den konkreta åtgärd som avses vid tillståndsgivningen. Bedömningen grundades på att förutsättningarna för delar av den initiala prövningen – bl.a. tillämpningen av proportionalitetsprincipen – skulle försämras om åtgärden inte var bestämd till viss adress, plats eller liknande. Beslutsfattarens möjligheter att bedöma i vilken mån ett tillstånd behöver förenas med villkor för att tillgodose intresset av att enskildas integritet inte kränks i onödan skulle enligt regeringen sannolikt också minska.[4]

En ordning som innebär att domstolens tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation enbart knyts till person, och alltså inte till telefonnummer, adress eller utrustning, innebär ofrånkomligen att bedömningen av kopplingen mellan nummer, adress eller utrustning och den person avlyssningen eller övervakningen ska riktas mot flyttas från domstolen. Konsekvensen av en sådan ordning skulle således bli att det antingen är åklagare eller den verkställande myndigheten som prövar den kopplingen och avgör om åtgärden ska tillåtas i det enskilda fallet. Det skulle i förundersökningsfallen i praktiken innebära att det som domstolen får kvar att pröva är om den misstänkte är skäligen misstänkt för ett brott som kan föranleda åtgärden, om åtgär-

[4] Prop. 2013/14:237 s. 97.

den är av synnerlig vikt för utredningen och om det är proportionerligt att alls vidta åtgärden.

Det kan vid en första anblick te sig förhållandevis oproblematiskt med en sådan förskjutning av prövningen som blir konsekvensen av att knyta tillståndet enbart till person, eftersom domstolen ju ändå skulle pröva om det är proportionerligt att alls avlyssna eller övervaka den misstänkte. Dessutom är ju både åklagare och övriga brottsbekämpande myndigheter vana att utföra proportionalitetsbedömningar som ett led i sitt dagliga arbete. Det kan emellertid ifrågasättas hur reell domstolens prövning, bl.a. avseende åtgärdens proportionalitet, skulle kunna bli med en reglering där tillståndet enbart knyts till person. Det hänger samman med hur de svenska reglerna om hemliga tvångsmedel i övrigt är utformade.

För det första är det, som uttalats i tidigare lagstiftningsärenden, viktigt för domstolen att i sin proportionalitetsprövning kunna ta ställning till den konkreta avlyssnings- eller övervakningsåtgärd som ska utföras. Om domstolen, som skulle bli fallet om tillståndet enbart avsåg person, inte ska pröva kopplingen mellan den misstänkte och telefonnummer, adress eller utrustning minskar tveklöst domstolens möjligheter att ta ställning till den konkreta avlyssnings- eller övervakningsåtgärden. Ett talande exempel är att domstolen i ett sådant fall inte längre kommer att kunna ta ställning till om avlyssning eller övervakning ska tillåtas avseende ett telefonnummer som inte tillhör den misstänkte, men som denne kan förväntas kontakta (jfr 27 kap. 20 § första stycket 2 rättegångsbalken, se även motsvarande bestämmelse i 2 § första stycket 2 preventivlagen). Avlyssningen eller övervakningen riktas i de fallen fortfarande mot den misstänkte men tillståndet avser någon annans nummer, adress eller utrustning. I dag har domstolen möjlighet att, utöver att inte alls tillåta sådan avlyssning eller övervakning, t.ex. föreskriva som villkor i tillståndet att avlyssning eller övervakning endast får ske enligt vissa givna förutsättningar, såsom att det endast är när den misstänkte ringer till numret som avlyssning eller övervakning får ske. Den typen av integritetsskyddande villkor från domstolen skulle i det närmaste bli en chimär om rättens tillstånd kopplades enbart till person.

Vidare skulle det exempelvis inte heller vara möjligt för domstolen att ta ställning till om det är proportionerligt att låta avlyssningen eller övervakningen avse en av flera personer gemensamt

använd dator eller telefon, t.ex. en dator på ett internetcafé eller ett bibliotek eller en telefon på den misstänktes arbetsplats, om tillståndet kopplades enbart till person. Dagens ordning innebär nämligen inte att den misstänkte (eller en person som blir föremål för åtgärder enligt preventivlagen eller LSU) måste äga eller inneha den telefon eller adress alternativt det nummer som ska avlyssnas eller övervakas. Det är tillräckligt att numret, adressen eller utrustningen kan antas ha använts eller komma att användas av honom eller henne för att tillstånd ska få meddelas om det också är proportionerligt. Proportionalitetsbedömningen i de fallen liksom möjligheten att i sådana fall föreskriva om integritetsskyddande villkor, t.ex. att det krävs spaning mot den misstänkte så att det endast är när denne använder datorn eller telefonen som avlyssning eller övervakning får ske, skulle alltså lämnas till den brottsbekämpande myndigheten som har att verkställa åtgärden eller till åklagaren om domstolens tillstånd enbart skulle knytas till person.

De nu anförda argumenten talar med viss styrka för att domstolens möjlighet att göra en reell prövning, särskilt proportionalitetsprövning, avsevärt skulle försämras jämfört med dagens situation om tillståndet knöts enbart till person. Det talar för att även fortsättningsvis låta domstolen vara den instans som ska pröva vilka telefonnummer, adresser eller utrustningar som ska få avlyssnas eller övervakas. En sådan ordning synes också vara väl förenlig med Sveriges åtaganden enligt Europakonventionen, jfr t.ex. Europadomstolens uttalanden den 4 december 2015 i rättsfallet Zakharov mot Ryssland, särskilt §§ 264–267.

Till det anförda kommer en mer praktisk aspekt av att domstolens tillstånd knyts enbart till person. Man kan nämligen fråga sig vad som blir konsekvensen om fel person avlyssnas eller övervakas vid en sådan ordning. Det kanske tydligaste exemplet är om domstolens tillstånd innebär att avlyssning eller övervakning får riktas mot en person och åtgärden sedan verkställs avseende ett visst telefonnummer i tron att det används av den personen. Visar det sig när verkställigheten pågår att numret inte alls används av den misstänkte utan av någon annan kan ju den verkställande myndigheten ha genomfört en avlyssning vars laglighet kan ifrågasättas (se t.ex. 4 kap. 8 § brottsbalken) eftersom domstolens tillstånd inte tar sikte på numret utan på personen. Det torde då sakna betydelse att den verkställande myndigheten eller åklagaren, dvs. den som ska pröva

kopplingen mellan numret och personen, har godkänt avlyssningen eller övervakningen eftersom domstolens tillstånd ju endast avser en person som inte använder numret. Om motsvarande situation sker i dag är åtgärden visserligen felaktig (eftersom det inte är den misstänkte som avlyssnas) men den kan knappast vara olaglig eftersom domstolen ju kommit fram till och lämnat tillstånd avseende vilka nummer som får avlyssnas.

Sammantaget kan således konstateras att en ordning som innebär att domstolens tillstånd enbart knyts till person får konsekvenser som inte är enbart positiva när det gäller frågan om att komma till rätta med den effektivitetsproblematik som skisserats i avsnitt 6.1 och 6.2. Konsekvenserna som vi nu exemplifierat skulle möjligen kunna hanteras på ett ändamålsenligt vis, men redan förekomsten av dem talar för att behovet av att knyta tillståndet till person bör vara mycket tungt vägande för att överväga en sådan förändring.

När det gäller behovet av ändringar kan först konstateras att det på en total nivå inte skett några förändringar avseende det genomsnittliga antalet tillstånd per person sedan frågan senast övervägdes (jfr tabell 1 ovan). Sett till omfattningen av problematiken generellt kan det därför inte anses att behovet av att knyta tillståndet enbart till person är större i dag än då.

Rörande den problematik som de brottsbekämpande myndigheterna framhållit och som tar sikte på att det kan bli en bristande kontinuitet i avlyssningen om en kriminell byter eller använder flera telefoner eller sim-kort för att undgå att bli avlyssnad eller övervakad föreslogs år 2014 vissa ändringar avseende beslutsordningen, bl.a. beträffande möjligheten till interimistiska beslut. Lagändringarna trädde i kraft den 1 januari 2015 och innebar att det lämnades större utrymme för interimistiska åklagarbeslut i brådskande fall. Bland annat innebär reglerna att det är möjligt för åklagaren att meddela ett interimistiskt beslut om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd. Även om möjligheten att använda den interimistiska beslutanderätten är tänkt att användas endast i undantagsfall nämns i motiven uttryckligen som exempel bl.a. sim-kortsbyte och risken för att ändamålet med åtgärden går förlorat om rättens tillstånd skulle avvaktas, se prop. 2013/14:237 avsnitt 8.2 och s. 182 f.

Sedan möjligheten till interimistiska beslut infördes i sin nuvarande form har det avseende hemlig avlyssning av elektronisk kommunikation meddelats 48 beslut år 2015 och 74 beslut år 2016. För hemlig övervakning av elektronisk kommunikation har det meddelats 51 beslut år 2015 och 60 beslut år 2016.[5] Det framgår inte av statistiken om det är på grund av strategier från kriminella med flera telefoner eller sim-kort och risker för bristande kontinuitet i avlyssning och övervakning eller om det är på grund av att domstolen varit stängd när behovet uppstått som de interimistiska besluten har meddelats. Av uppgifter till utredningen från åklagare och domare används interimistiska beslut dock i stort sett uteslutande när domstolarna är stängda, dvs. inte för att komma till rätta med problem kopplade till kriminellas metoder. Antalet interimistiska tillstånd är dessutom under alla förhållanden inte sådana att de, med beaktande av de konsekvenser som ovan framhållits, talar för att det finns tungt vägande behov av att ändra så att tillståndet ska avse enbart person.

När det gäller den andra påpekade problematiken – att det innebär en betydande resursanvändning i vissa ärenden för främst Åklagarmyndigheten att infinna sig i rätten inför varje nytt tillstånd när det enda som tillkommit sedan ett inledande tillstånd meddelats är ett eller flera nya telefonnummer, adresser eller kommunikationsutrustningar – gör sig det resonemang gällande som vi fört nyss. Det kan sammanfattas som så att även om en ändring som innebär att tillståndet knyts enbart till person skulle kunna effektivisera förfarandet när kriminella som strategi för att undkomma avlyssning eller övervakning byter eller använder flera telefoner eller sim-kort för ett sådant förslag för långt i förhållande till behovet. De rättssäkerhets- och integritetsskyddsaspekter som i vissa avseenden skulle kunna gå förlorade om tillståndet knöts enbart till person i stället för till telefonnummer, adress eller utrustning står enligt vår bedömning inte i proportion till den eventuella effektivitetsvinst som skulle kunna bli fallet om tillståndet knöts enbart till person. Det finns enligt utredningens mening därför inte tillräckligt tungt vägande skäl för att gå vidare med ett förslag om att knyta tillståndet enbart till person. En annan sak är att den in-

[5] Regeringens skrivelse 2017/18:69 Redovisning av användningen av hemliga tvångsmedel under 2016 s. 16 och 19.

effektivitet som finns inbyggd i det nuvarande systemet till följd av kriminellas agerande i nu aktuellt avseende rimligen kan motverkas på ett annat och mer ändamålsenligt vis än genom att knyta tillståndet enbart till person. Till det återkommer vi i nästa avsnitt.

Vår slutsats är således att de skäl som anfördes senast frågan utreddes fortfarande har fog för sig. Det finns därför inte heller nu skäl att gå vidare med ett förslag om att knyta tillstånd till hemlig avlyssning eller övervakning av elektronisk kommunikation enbart till person. Detta eftersom en sådan ändring, mot bakgrund av hur den svenska regleringen på det hemliga tvångsmedelsområdet ser ut i övrigt, riskerar att få mer långtgående verkningar än att enbart komma till rätta med de problem som uppstår till följd av att vissa kriminella för att försvåra eller undvika avlyssning eller övervakning byter eller använder flera nummer eller utrustningar.

## 6.4 En annan ändring är lämplig och nödvändig

**Utredningens förslag:** En ny regel införs i rättegångsbalken som innebär ett undantag i vissa fall till huvudregeln att sammanträde ska hållas vid ansökan eller anmälan om tillstånd till hemlig avlyssning av elektronisk kommunikation. Om det redan finns ett tillstånd till åtgärden och en ny ansökan eller anmälan gäller samma person och grundas på samma omständigheter som det tidigare tillståndet men avser ett annat telefonnummer, en annan adress eller en annan elektronisk kommunikationsutrustning än det tidigare tillståndet får rätten pröva frågan utan sammanträde om ett sådant skulle vara utan betydelse. Ett offentligt ombud behöver då inte utses innan rättens beslut men ska skyndsamt utses och underrättas om rättens beslut när det har fattats.

Ett tillstånd som meddelas utan sammanträde får inte avse annan tid än det tidigare tillståndet i ärendet.

### 6.4.1 Det finns skäl att överväga ändrade regler i vissa fall

Vi har alltså kommit fram till att det inte finns tillräckligt tungt vägande skäl för att gå vidare med ett förslag om ett knyta tillståndet till hemlig avlyssning eller övervakning av elektronisk kommu-

nikation enbart till person eftersom ett sådant förslag skulle få längre gående konsekvenser än att enbart komma till rätta med de problem som uppstår till följd av att kriminella sätter i system att byta eller använda flera telefoner eller sim-kort. Icke desto mindre kan sådana, förhållandevis enkla, motåtgärder från kriminella för att undvika eller försvåra avlyssning utgöra ett reellt problem ur effektivitetsperspektiv i den brottsbekämpande verksamheten, se särskilt exemplen i slutet av avsnitt 6.2. Det finns därför skäl att överväga om dagens ordning i alla delar är rimlig när det enda som en ansökan om hemlig avlyssning av elektronisk kommunikation egentligen avser är ett eller flera nya nummer, adresser eller kommunikationsutrustningar till följd av sådant agerande från kriminella.

Det är särskilt i vissa utredningar som problemen med byte eller användning av flera sim-kort eller kommunikationsutrustningar förekommer systematiskt. I Ekobrottsmyndighetens, Polismyndighetens och Tullverkets verksamheter är det främst i utredningar beträffande brott som begås inom den organiserade brottsligheten som strategin används. Också i Säkerhetspolisens verksamhet är det mycket vanligt förekommande.

Det är just i de fall där kriminella satt i system att göra telefon- eller nummerbyten eller använda flera olika sådana för att undkomma eller försvåra avlyssning och övervakning som det enligt vår mening finns anledning att överväga ändringar av de svenska reglerna. Det primära skälet till det är att de kriminellas beteende ju leder till att brottsbekämpande resurser används på ett inte avsett vis. Det är inte godtagbart att kriminellas agerande i sådan grad som blir fallet i de angivna situationerna styr resursanvändningen hos brottsbekämpande myndigheter, och därigenom även effektiviteten i det brottsbekämpande arbetet.

De exempel som anförts i slutet av avsnitt 6.2 är talande. I de åtta exempelärenden som redovisades där hölls det 169 sammanträden utöver det lagstadgade minimiantalet sammanträden, dvs. ett sammanträde per misstänkt och månad (27 kap. 21 § andra stycket och 27 kap. 28 § första stycket rättegångsbalken). Som tillståndsförfarandet ser ut i dag behöver åklagaren varje gång en ny telefon eller ett nytt nummer upptäcks upprätta och skicka in en ansökan om nytt tillstånd till tingsrätten varefter rätten ska utse offentligt ombud och kalla till sammanträde där ombudet och åklagaren ska närvara. En inte orimlig uppskattning är att den genomsnittliga

tiden det tar för en åklagare att inställa sig till och närvara vid ett sammanträde är i vart fall en timme. Det innebär att de åklagare som ansvarade för förundersökningen i de anförda exemplen kan således ha behövt lägga uppemot 169 timmar, motsvarande drygt fyra arbetsveckor, på att infinna sig i rätten efter att ett inledande tillstånd (eller förlängningstillstånd) hade meddelats. Detta är inte en ändamålsenlig användning av åklagarresurserna annat än om sammanträdet faktiskt tillför ärendet något eller rättssäkerhets- eller integritetsaspekter talar för den gällande ordningen.

Av de skäl som redovisats i avsnitt 6.3 är det av vikt att domstolen är den som fattar beslut om vilka telefonnummer, andra adresser eller elektroniska kommunikationsutrustningar som får avlyssnas för att kunna ta ställning till den konkreta åtgärd som ska genomföras. När det emellertid endast är fråga om en annan telefon eller ett annat nummer i förhållande till vad som tillåtits i det tidigare tillståndet är det svårt att se hur rätten skulle kunna komma till annat resultat än vad man gjort i den inledande tillståndsprövningen och att integritets- eller rättssäkerhetsskäl talar emot att regler införs som begränsar den prövning som ska göras. Mot den bakgrunden finns enligt vår bedömning skäl att, på sätt som gjorts i Finland, överväga ett förenklat förfarande för de fall då kriminella använder det beskrivna förfarandet för att undkomma eller försvåra avlyssning och övervakning.

Eftersom domstolsprövningen således bör behållas och det egentliga problemet är den onödiga resursanvändning som uppstår genom att åklagare inför varje nytt tillstånd behöver infinna sig i rätten bör övervägandena inriktas på om det är nödvändigt med dagens ordning där sammanträde inför åklagare och offentligt ombud är obligatoriskt.

### 6.4.2 De olika beslutsordningarna vid hemlig avlyssning och övervakning av elektronisk kommunikation

Det kan noteras att det vid ansökningar om tillstånd till hemlig övervakning av elektronisk kommunikation inte uppställs något krav på att det ska hållas sammanträde. Inte heller finns något krav på att offentligt ombud ska utses i de fallen, se t.ex. 27 kap. 28 § rättegångsbalken. Bakgrunden till regleringen är att behovet av sådana rättssäkerhetsåtgärder ansetts vara mindre i dessa ärenden jämfört

med sådana som gäller de mer ingripande tvångsmedlen. Det hänger i sin tur samman med dels att det integritetsintrång som tvångsmedlet kan medföra typiskt sett är mindre än när det gäller de övriga tvångsmedlen, dels att sådana frågor som offentliga ombud särskilt bevakar mer sällan torde komma upp vid hemlig övervakning av elektronisk kommunikation.[6] Det kan konstateras att den ordning som gäller för hemlig övervakning av elektronisk kommunikation, utifrån det perspektiv som ovan angivits om att domstolsprövningen inte bör frångås, framstår som klart mer effektiv än ordningen som gäller för hemlig avlyssning av elektronisk kommunikation. Mot den bakgrunden gör vi bedömningen att det inte behövs några ändringar av beslutsordningen vid hemlig övervakning av elektronisk kommunikation och behandlar därför inte den frågan i det följande.

Det kan dock på goda grunder ifrågasättas om inte det nu angivna resonemanget beträffande att inte kräva sammanträde och offentligt ombud vid hemlig övervakning av elektronisk kommunikation kan göras gällande för tillståndsprövning av hemlig avlyssning av elektronisk kommunikation när den som redan är föremål för avlyssning, som en strategi för att undkomma eller försvåra den åtgärden, byter nummer eller telefon frekvent eller använder flera parallellt. I de fallen måste rimligen, som utgångspunkt, det tillkommande integritetsintrånget som det innebär med tillstånd till avlyssning avseende ett nytt nummer eller en ny adress eller utrustning i de allra flesta fall vara detsamma som intrånget vid avlyssning av det redan tillståndsgivna. Det är alltså som regel inte fråga om ett allvarligare integritetsintrång när ett nytt nummer, en ny adress eller utrustning har identifierats i de fallen än vad som är fallet enligt det ursprungliga tillståndet. En ordning som innebär att rätten i dessa situationer även vid hemlig avlyssning av elektronisk kommunikation får fatta sitt beslut på handlingarna i stället för vid ett sammanträde inför åklagaren och ett offentligt ombud framstår därför som rimlig. Givetvis måste en sådan ordning kringgärdas med godtagbara integritetsskydds- och rättssäkerhetsgarantier för att säkerställa att det är just de fall då kriminella ofta byter eller använder flera telefoner eller telefonnummer för att undvika eller försvåra avlyssning som en ny ordning tar sikte på. Annars

[6] Se prop. 2002/03:74 s. 22 ff. och prop. 2013/14:237 s. 120 f.

riskeras att motsvarande konsekvenser som framhållits i avsnitt 6.3 uppstår även här.

### 6.4.3 Den närmare utformningen av en ny reglering

#### Grundförutsättningen – behövs ett sammanträde?

Det är självklart av yttersta vikt att ändringar i gällande reglering inte innebär försämringar i rättssäkerheten eller integritetsskyddet. Som nyss konstaterats torde det mycket sällan vara fråga om ett ökat integritetsintrång, när det redan pågår avlyssning mot en person, att också meddela tillstånd mot ett nytt nummer eller en ny telefon. Emellertid kan det tänkas att ett inledande tillstånd tar sikte på ett mobiltelefonnummer som används uteslutande av den avlyssnade medan det nya nummer som en tillståndsansökan avser är ett nummer som personen delar med någon annan eller ett nummer som den avlyssnade personen förväntas kontakta. I de fallen är det viktigt att den ordning som i dag gäller även fortsättningsvis ska tillämpas, inte minst för upprätthållande av rättssäkerheten. Detta kan enligt vår mening åstadkommas genom att domstolen ges rätten att bestämma när det behövs ett sammanträde då frågan gäller ett tillkommande nummer eller en tillkommande annan adress eller utrustning. Åklagaren bör vara oförhindrad att i samband med sin ansökan upplysa rätten om faktorer som enligt dennes mening talar för respektive emot att hålla ett sammanträde. Det kan för övrigt redan här sägas att en förutsättning för att domstolen alls ska kunna göra en välgrundad bedömning avseende om det behövs ett sammanträde eller inte är att åklagarens framställan och promemoria innehåller tillräckligt med uppgifter för att en domare som inte varit i kontakt med ärendet tidigare ska kunna bilda sig en uppfattning i frågan.

Frågan är då hur det bör uttryckas att domstolen får avgöra när ett sammanträde behövs. Ett sätt är att införa något slags nödvändighetsrekvisit så att sammanträde endast behöver hållas när det är nödvändigt, alternativt inte hållas när det inte är nödvändigt. Det bör emellertid, enligt utredningens uppfattning, redan av bestämmelsen framgå att det är fråga om ett undantag till den huvudregel om att sammanträde ska hållas som följer av 27 kap. 28 § rättegångsbalken som endast ska tillämpas i vissa särpräglade situationer. Ett

nödvändighetsrekvisit möter enligt vår bedömning inte helt det kravet. I stället kan det direkt i lagtext tydliggöras att det är fråga om ett undantag till huvudregeln om sammanträde genom att det anges att domstolen får möjlighet att avgöra när det är utan betydelse med ett sammanträde. Självfallet behöver en sådan regel dock ges en klar innebörd för den kontext den är avsedd, så att risker för tillämpningsglidningar inte uppstår.

### När kan ett sammanträde vara utan betydelse?

Frågan är då hur det bör gå till när domstolen ska avgöra om ett sammanträde vid en ansökan om hemlig avlyssning av elektronisk kommunikation skulle vara utan betydelse. Som redan framgått är målsättningen med den regeländring vi föreslår att ta sikte på den aktuella situationen, dvs. att kriminella byter eller har flera nummer eller telefoner för att undvika och försvåra avlyssning. En första förutsättning bör därför vara att det redan finns ett meddelat tillstånd mot den person som den nya ansökningen eller, i de fall det är fråga om ett interimistiskt beslut, den nya anmälan avser. Det ligger i sakens natur att åtminstone ett tidigare tillstånd måste vara gällande. Har tidigare beslut hävts och samtliga tillstånd som dittills meddelats inte längre är gällande bör det förenklade förfarandet således inte kunna användas.

Vidare måste en förutsättning vara att det är när det nya tillståndet söks på samma grunder som det tidigare som ett förenklat förfarande kan komma i fråga. Det betyder att det förenklade förfarandet inte kan komma i fråga om andra omständigheter till stöd för ansökan än de som åberopats inför det tidigare beslutet görs gällande i den nya ansökan. I förundersökningsfallen krävs således bl.a. att den nya ansökan ska grundas på samma brottsmisstanke som den tillståndsgivna ansökan gjort och i underrättelsefallen att den nya ansökan grundar sig på samma omständigheter som den tidigare ansökan (t.ex. avseende riskbedömning i preventivlagsfallen eller betydelsen för utredningen i LSU-fallen).

Ytterligare en förutsättning bör vara att ansökan eller anmälan avser ett nytt nummer eller en ny adress eller utrustning, och alltså inte någon annan fråga som kan uppstå vid prövningen av hemliga tvångsmedel. Utan de angivna förutsättningarna finns risk att det

öppnas upp för en tillämpning där sammanträde kan underlåtas i andra situationer än de som vårt förslag avser att ta sikte på. Det anförda kan lämpligen i lagtext uttryckas på så vis att om rätten har meddelat tillstånd till hemlig avlyssning av elektronisk kommunikation så får en ansökan eller anmälan om ytterligare tillstånd mot samma person och som grundas på samma omständigheter men avser ett annat telefonnummer eller en annan adress eller annan elektronisk kommunikationsutrustning än det tidigare tillståndet prövas utan sammanträde om ett sammanträde skulle vara utan betydelse.

Frågan om ett sammanträde är utan betydelse bör lämpligen ta sin utgångspunkt i dels det tidigare meddelade tillståndet i förening med de uppgifter som framkommer i den nya ansökan, dels de skäl för att införa regler om ett dylikt förenklat förfarande som vi här föreslår, dvs. att effektivisera förfarandet i de fall kriminella för att försvåra för brottsbekämpande myndigheter byter eller använder flera telefoner och nummer. Det torde därför som regel anses vara utan betydelse med ett sammanträde när de grundläggande förutsättningarna är uppfyllda om det är fråga om samma typ av nummer, adress eller utrustning (t.ex. ett nytt mobiltelefonnummer eller en ny mobiltelefon) och skälet för tillståndsansökan är detsamma som vid föregående prövning (t.ex. att den misstänkte innehar utrustningen eller använder numret). Även om det inte är fråga om samma typ av nummer, adress eller utrustning (t.ex. att det tidigare tillståndet avsåg ett mobiltelefonnummer men den nya ansökan avser IMEI-nummer) men skälet för tillståndsansökan är detsamma som vid föregående prövning bör det oftast vara utan betydelse med sammanträde. Det kan dock tänkas att det nya numret, den nya adressen eller utrustningen används av flera personer (t.ex. en gemensamt använd dator). I så fall torde det närmast undantagslöst krävas sammanträde. Sammanträde bör dessutom alltid behövas när grunden för tillståndet är att den som är föremål för avlyssningsbeslutet förväntas kontakta en annan person, vars nummer, adress eller utrustning tillståndet ska avse, dvs. avlyssning med stöd av 27 kap. 20 § första stycket 2 rättegångsbalken eller 2 § första stycket 2 preventivlagen.

Av de exempel som redovisats i avsnitt 6.2 framgår att problematiken med byten eller användning av flera telefoner eller nummer kan uppkomma flera gånger i samma ärende hos en brottsbekämpande myndighet. Det ligger så att säga i problematikens natur

att så blir fallet. Vår bedömning är att det förenklade förfarandet, som ju i grunden syftar till att effektivisera hanteringen när kriminella vidtar motåtgärder, ska kunna användas i varje fall då nya nummer eller telefoner upptäcks. Någon begränsning av t.ex. antalet nummer eller utrustningar som ska kunna prövas inom ramen för det förenklade förfarandet bör därför inte ställas upp. Inte heller bör domstolen vara förhindrad att tillämpa det förenklade förfarandet beträffande samma person vid olika tillfällen. En annan sak är självfallet att antalet nummer eller utrustningar som en eller flera tillståndsansökningar avser kan påverka det samlade integritetsintrånget eller bedömas medföra rättssäkerhetskonsekvenser och därför kan tala mot att anse ett sammanträde vara utan betydelse. Frågor av den karaktären bör dock enligt vår uppfattning lösas i den praktiska rättstillämpningen vid prövningen av den föreslagna bestämmelsen.

Som kommer att framgå nedan ska ett tillstånd som lämnas med tillämpning av det förenklade förfarandet inte kunna sträcka sig längre än den tid som det tidigare tillståndet gäller för. Det innebär att tillståndsprövning kommer att ske vid sammanträde åtminstone en gång per månad (se 27 kap. 21 § andra stycket och 27 kap. 28 § rättegångsbalken) i de fall åklagaren begär att ett tillstånd ska förlängas. Även den omständigheten bör vägas in vid bedömningen av om ett sammanträde är utan betydelse.

Ingenting bör hindra att det förenklade förfarandet används efter att åklagaren har meddelat ett interimistiskt beslut, förutsatt såklart att förutsättningarna är uppfyllda och att domstolen finner att det skulle vara utan betydelse med ett sammanträde. Det bör därför framgå av den föreslagna bestämmelsen att det både är vid ansökan och anmälan som det förenklade förfarandet kan användas.

### Ska ett offentligt ombud utses och i så fall – när?

Nästa fråga att ställa sig är vad som ska gälla om domstolen kommer fram till att ett sammanträde skulle vara utan betydelse. Bör ett offentligt ombud då utses i enlighet med nuvarande ordning och ges möjlighet att yttra sig innan domstolen meddelar sitt beslut? Enligt vår bedömning bör det främst vara i de fall där en avlyssnad person som en strategi för att undkomma och försvåra avlyssning byter eller använder flera telefoner eller nummer som domstolen

kan komma fram till att ett sammanträde skulle vara utan betydelse. Vid sådana förhållanden kan det ifrågasättas vilken skillnad det offentliga ombudet kan göra i samband med prövningen. Det bör särskilt hållas i åtanke att ett av skälen bakom införandet av reglerna om offentliga ombud var att dessa skulle verka för att omständigheterna i ärendet blir allsidigt belysta.[7] Med de förutsättningar vi föreslår ska gälla för prövningen av om ett sammanträde är utan betydelse finns, i de fall tingsrätten gör bedömningen att så är fallet, inte några särskilda frågor kvar att belysa allsidigt. Den enda egentliga kvarstående frågan är om det nya numret eller den nya adressen eller utrustningen, som typiskt sett kommer motsvara vad som fått avlyssnas enligt det tidigare tillståndet, ska få avlyssnas. Vår bedömning är därför att betydelsen av att ytterligare en oberoende part utöver domaren, dvs. det offentliga ombudet, innan beslutet granskar ansökan i dessa fall framstår som mycket begränsad med hänsyn till den bedömning som rätten gjort. Det talar med styrka för att när domstolen konstaterar att det inte behövs ett sammanträde så bör ett offentligt ombud inte utses på sätt som föreskrivs i 27 kap. 28 § första stycket rättegångsbalken. Detta resonemang står också i överensstämmelse med det som Utredningen om vissa hemliga tvångsmedel redovisade för att inte införa offentliga ombud i ärenden om hemlig övervakning av elektronisk kommunikation. Där angavs bl.a. följande (vår kursivering).

> Skäl som talar mot att utvidga tillämpningen av systemet med offentliga ombud till att omfatta även hemlig teleövervakning är sålunda dels att det integritetsintrång som tvångsmedlet medför typiskt sett är mindre än det från de övriga nämnda tvångsmedlen, dels att flera sådana frågor som de offentliga ombuden är särskilt ägnade att bevaka mera sällan torde komma upp vid hemlig teleövervakning. Härtill kommer att *det finns ett värde i sig av att medverkan av offentliga ombud koncentreras till ärenden där behovet och funktionen av detta […] i praktiken visat sig vara starka*. På så sätt undviks risken att ombudens roll vattnas ur eller att systemet uppfattas som ”ett spel för gallerierna”.[8]

Mot bakgrund av det som nu redovisats gör vi sammantaget bedömningen att det, när domstolen finner att det är utan betydelse att hålla ett sammanträde, inte är nödvändigt att utse ett offentligt ombud innan domstolen fattat beslut i frågan om tillstånd.

[7] Se t.ex. prop. 2002/03:74 s. 24.
[8] SOU 2012:44 s. 673.

Inom utredningen har emellertid diskuterats om det vore ändamålsenligt att låta ett offentligt ombud i efterhand ta del av rättens beslut för att, om ombudet inte delar rättens bedömning avseende det nya numret, den nya adressen eller utrustningen ha möjlighet att ifrågasätta rättens beslut inför högre rätt. För ett sådant förhållningssätt talar enligt utredningens mening att domstolens beslut på det viset kan underkastas både en direkt granskning och, i förlängningen, överprövning. Den enda egentliga granskningen som domstolens beslut annars kan utsättas för är Justitiekanslerns eller Justitieombudsmannens tillsyn. Vetskap från rättens sida om att beslutet kan komma att granskas borgar för att ett system som ger rätten möjlighet att inte hålla sammanträde inte överutnyttjas, dvs. det kan motverka tillämpningsglidningar. Samtidigt är ju skälet till införande av en sådan regel som vi föreslår att det i praktiken inte finns några ökade integritetsrisker med den föreslagna ordningen eftersom domstolen i det inledande skedet ska avgöra om det behövs en mer allsidig belysning av ansökan eller anmälan utifrån förutsättningarna i det enskilda fallet. Det gör att det blir en aning inkonsekvent att utse ett offentligt ombud i efterhand. Dessutom kan en sådan granskande roll som de offentliga ombuden får om de utses först sedan beslut har meddelats sägas ligga närmare en tillsynsfunktion än den hittillsvarande funktionen som det offentliga ombudet haft. Trots den möjliga inkonsekvensen och den riktningsförändring som en ordning där offentliga ombud utses i efterhand innebär är det vår bedömning att de fördelar, inte minst från rättssäkerhetssynpunkt, som det innebär att beslutet får granskas av ett offentligt ombud och kan överklagas väger över.

Det bör således införas en bestämmelse om att ett offentligt ombud ska utses när rätten har meddelat sitt beslut. En sådan regel kan lämpligen följa det mönster som gällde innan reglerna om interimistiska åklagarbeslut infördes, se t.ex. prop. 2002/03:74 s. 51. Då kunde rätten under vissa förutsättningar fatta beslut om hemlig avlyssning av elektronisk kommunikation utan att ett offentligt ombud närvarade vid ett sammanträde. Om ett tillstånd hade meddelats på det sättet skulle dock ett offentligt ombud i efterhand ha rätt att ta del av ärendet och ha möjlighet att överklaga. På motsvarande sätt bör ett offentligt ombud som utses när rätten har fattat ett beslut på handlingarna efter att ha konstaterat att det inte behövs ett sammanträde skyndsamt underrättas om beslutet och ha rätt att

ta del av vad som förekommit. På så sätt kan gransknings- och överklaganderätten som tillkommer det offentliga ombudet bibehållas.

Av 27 kap. 26 § andra stycket rättegångsbalken följer att ett offentligt ombud har rätt att ta del av det som förekommer i ärendet, yttra sig i ärendet och överklaga rättens beslut. När, som i nu aktuella fall, ett offentligt ombud utses efter att rätten har fattat sitt beslut ligger det i sakens natur att ombudet inte kan yttra sig i ärendet inför första instans. Det behövs emellertid enligt vår bedömning inte någon särreglering i förhållande till den nämnda regleringen eftersom det offentliga ombudet, om ett beslut överklagas, har rätt att yttra sig i ärendet i högre rätt.

### Det nya tillståndet ska inte gälla för annan tid än det tidigare

Enligt 27 kap. 21 § andra stycket rättegångsbalken ska det i ett beslut att tillåta hemlig avlyssning av elektronisk kommunikation anges vilken tid tillståndet avser. Tiden får inte bestämmas längre än nödvändigt och får inte heller, när det gäller tid som infaller efter beslutet, överstiga en månad från dagen för beslutet. Motsvarande gäller tillstånd till den åtgärden enligt 7 § preventivlagen och 21 § LSU.

Eftersom den reglering vi nu föreslår är tänkt att fungera som ett förenklat förfarande, främst baserat på att det redan meddelats ett motsvarande tillstånd till hemlig avlyssning av elektronisk kommunikation, bör av såväl effektivitets- som rättssäkerhetsskäl både det tidigare tillståndet och därpå följande tillstånd prövas vid ett och samma sammanträde i närvaro av ett offentligt ombud om förlängning av tillstånden aktualiseras. Med den nyss angivna regleringen om hur lång tid ett tillstånd till hemlig avlyssning av elektronisk kommunikation får avse finns emellertid typiskt sett möjlighet att sätta tiden för ett tillkommande tillstånd till en senare tidpunkt än den då det tidigare tillståndet upphör. Motsvarande problematik uppstår redan i dag när tillkommande tillstånd meddelas. I praktiken hanteras detta, enligt uppgift från domare och åklagare, typiskt sett på så vis att ett tillkommande tillstånd meddelas för den tid som återstår av det inledande tillståndet. På så sätt prövas alla tillstånd beträffande en person, om förlängning, begärs i ett sammanhang. Även om det kan förväntas fungera på motsvarande vis när

ett tillkommande tillstånd har meddelats enligt det föreslagna förenklade förfarandet bör det inte kunna komma i fråga att ett tillkommande tillstånd kan löpa längre än det inledande. Inte heller ska den regeländring vi föreslår öppna upp för att förlängningsansökningar kan prövas med det förenklade förfarandet. För att förhindra detta bör det tas in en bestämmelse om att det tillkommande tillståndet inte får avse annan tid än det inledande tillståndet.

### Placering av en ny bestämmelse

Den nya regeln bör införas bland reglerna om offentliga ombud i rättegångsbalken. Eftersom det är fråga om ett undantag till huvudregeln i 27 kap. 28 § första stycket rättegångsbalken bör den införas som en regel i direkt anslutning till den bestämmelsen, förslagsvis som en ny 28 a § i samma kapitel. Genom att införa en ny bestämmelse där uppnås också den fördelen att regeln blir tillämplig även i de fall då personer är föremål för avlyssning enligt bestämmelserna i preventivlagen och LSU, eftersom dessa lagar hänvisar till 27 kap. 26–30 §§ rättegångsbalken. I de fall personer som är föremål för åtgärder enligt de lagarna använder sig av samma modus som utgör skälet till vårt förslag finns inte anledning att göra annan bedömning än den som vi har redovisat hittills.

### Några praktiska konsekvenser av förslaget

I dag sker i praktiken ansökningar eller anmälningar om tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation på olika sätt. De senare, för vilka det inte krävs sammanträde, skickas typiskt sett elektroniskt till tingsrätten som krypterade och lösenordskyddade filer medan de förra lämnas in fysiskt i pappersform i samband med att sammanträde ska hållas. Med vårt förslag kommer det ibland inte att behöva hållas sammanträde vid prövningen av hemlig avlyssning av elektronisk kommunikation. Eftersom den ändringen syftar till att effektivisera förfarandet bör hanteringen av ansökningar och anmälningar om den åtgärden ses över. Rimligen måste även sådana ansökningar och anmälningar kunna ges in elektroniskt till rätten, på motsvarande vis som i dag sker vid hemlig övervakning av elek-

tronisk kommunikation. Om ansöknings- och anmälningsförfarandet inte hanteras på det viset riskerar nämligen våra förslag att inte bli så effektiva som avsett.

Det kan emellertid inte anses lämpligt att inom ramen för denna utredning komma med förslag på ett område som de myndigheter som är involverade själva kan förfoga över. Det får därför ankomma på dem att, på sätt som redan gjorts för hemlig övervakning av elektronisk kommunikation, upparbeta effektiva rutiner för själva ansökningarna och anmälningarna inom ramen för det förenklade förfarande som vi föreslår.

När det gäller förslaget om att offentligt ombud ska utses först när tillstånd har meddelats av rätten har vi föreslagit att så ska ske skyndsamt, men inte satt någon bortre tidsgräns för när rätten kan utse ett ombud. I skyndsamhetskravets natur ligger, inte minst med hänsyn till den typ av ärenden det är fråga om, att rätten inom en begränsad tid ska agera på föreskrivet vis. I praktiken bör det dock, även med ett skyndsamhetskrav vara möjligt för rätten att avvakta med att utse och underrätta ett offentligt ombud någon dag, för att på så vis kunna utse en person som ändå ska till tingsrätten, eller för att kunna utse samma ombud som varit förordnat i det tidigare ärendet. I många av de större domstolarna hålls så gott som dagligen sammanträden i hemliga tvångsmedelsärenden och en effektiv resursanvändning, även såvitt avser offentliga ombud, är naturligtvis av stort värde. När rätten således kan förvänta sig att ett offentligt ombud kommer att behövas i ett annat ärende där det ska hållas sammanträde i närtid bör därför, om möjligt, det ombudet utses även för att granska beslut som fattats inom ramen för det förenklade förfarandet. I domstolar där det inte är sådan omfattning på ärendena att offentliga ombud mer eller mindre dagligen närvarar vid sammanträden bör det offentliga ombudet emellertid alltid utses och underrättas så snart som möjligt efter beslutet.

Något bör också klargöras beträffande den omständigheten att det tidigare tillståndet måste vara gällande för att det förenklade förfarandet ska få användas. Av 27 kap. 23 § rättegångsbalken följer att åklagare eller domstol om det inte längre finns skäl för ett beslut om hemlig avlyssning av elektronisk kommunikation omedelbart ska upphäva beslutet. Denna regel kommer givetvis gälla även framledes. Det får inte förekomma att tidigare beslut ej hävs för att möjliggöra för det förenklade förfarandet. En annan sak är att det

kan tänkas att det meddelas ett inledande tillstånd beträffande en person med det ordinarie förfarandet och att det därefter, med tillämpning av det förenklade förfarandet, meddelas ytterligare ett tillstånd. Om det inledande beslutet hävs men det andra tillståndet fortfarande gäller bör det vara möjligt att pröva ytterligare tillståndsansökningar med det förenklade förfarandet.

# 7 Konsekvenser och genomförande

## 7.1 Konsekvenser

**Utredningens bedömning:** Förslaget om ett förenklat förfarande för tillståndsprövning av ansökan om hemlig avlyssning av elektronisk kommunikation i vissa fall bedöms medföra att resurser inom Ekobrottsmyndigheten och Åklagarmyndigheten som i dag läggs på att åklagare infinner sig i rätten kommer att minska. Även domstolars resursåtgång kopplad till sammanträden bedöms minska. Resurserna som frigörs kommer kunna användas på annat håll inom rättsväsendet.

Inga andra konsekvenser bedöms uppstå till följd av förslaget.

### 7.1.1 Inledning

Av 14 § kommittéförordningen följer att om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet. Enligt samma paragraf ska samhällsekonomiska konsekvenser i övrigt redovisas om förslaget innebär sådana. Det är vidare i den förordningens 15 § angivet att om förslaget har betydelse för den kommunala självstyrelsen, 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 så ska konsekvenserna i de olika avseendena redovisas i betänkandet.

Vår bedömning är att vårt förslag inte kommer att ha någon som helst betydelse för merparten av de olika områden för vilka det finns förordningskrav att redovisa konsekvenser. Det gäller betydelsen för den kommunala självstyrelsen, 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 och för möjligheterna att nå de integrationspolitiska målen. De områdena behandlas därför inte vidare här.

### 7.1.2 Konsekvenser för de brottsbekämpande myndigheterna

När det gäller ekonomiska konsekvenser kan till en början konstateras att vårt förslag om ett förenklat förfarande syftar till att begränsa betydelsen av att kriminella som strategi för att undvika eller försvåra avlyssning ofta byter eller använder flera telefoner eller nummer. Som framgått i kapitel 6 har den problematik som kan uppstå till följd av ett sådant agerande inte lett till någon anmärkningsvärd ökning av antalet tillstånd på total nivå, se tabell 1 i avsnitt 6.2. Det leder oss för det första till slutsatsen att vårt förslag inte kommer att ge något större genomslag på total nivå kostnadsmässigt. Däremot bör det leda till att Ekobrottsmyndigheten och Åklagarmyndigheten, som ju med förslaget inte i samma omfattning som i dag kommer att behöva skicka åklagare till sammanträde, och övriga brottsbekämpande myndigheter, som inte sällan medverkar vid sammanträden, kan lägga mer resurser än i dag på sina respektive kärnverksamheter.

Det saknas ett säkert statistiskt underlag beträffande omfattningen av problematiken för att kunna göra säkra beräkningar av tidsåtgång och besparing av sådan med vårt förslag. De antaganden som görs i det följande utgår därför från genomsnittsberäkningarna och exemplen i avsnitt 6.2. Antagandena får betraktas som osäkra, därav det vida spannet.

Som framgår av tabell 1 i avsnitt 6.2 meddelas det per varje person som ett tillstånd till hemlig avlyssning av elektronisk kommunikation avser i genomsnitt knappt tre tillstånd beträffande telefonnummer, adresser eller elektroniska kommunikationsutrustningar.

Dessa genomsnittsberäkningar säger dock ingenting om hur ofta det meddelas ytterligare tillstånd efter det första sammanträdet.

För varje nytt tillstånd om hemlig avlyssning av elektronisk kommunikation efter det inledande krävs att ett sammanträde ska hållas vid tingsrätten. Det innebär för åklagaren att denne dels behöver upprätta och lämna in ansökan om det nya tillståndet till tingsrätten, dels infinna sig i rätten för sammanträdet. Det är svårt att exakt beräkna tidsåtgången för dessa åtgärder men en rimlig uppskattning är att det tar åklagaren mellan en och två timmar i anspråk med samtliga de göromål som ankommer på denne, varav cirka 30 minuter för upprättande av de handlingar som ska ges in till domstolen, när det enda som är nytt är att ett nummer eller en annan adress eller utrustning tillkommit.

Givet den nu antagna uppskattningen av tidsåtgång och ett antagande om att det i genomsnitt hålls cirka 0,5–1,5 sammanträden[1] per person som är föremål för hemlig avlyssning av elektronisk kommunikation efter det inledande sammanträdet blir den genomsnittliga tidsåtgången per sammanträde någonstans mellan 0,5–3 timmar (som minst 1 x 0,5 och som mest 2 x 1,5). Eftersom det meddelas beslut om hemlig avlyssning av elektronisk kommunikation mot ungefär 1 200 personer årligen innebär det anförda att åklagare i genomsnitt kan beräknas lägga 600–3 600 timmar årligen på sammanträden efter det inledande för att nya nummer, adresser eller utrustningar upptäcks. Det motsvarar således ungefär mellan en tredjedels årsarbetskraft och två årsarbetskrafter.

En ordning som vi föreslagit, som innebär att åklagaren inte är tvungen att infinna sig i rätten inför samtliga tillkommande domstolsbeslut, kan förväntas minska tidsåtgången för tilläggstillstånd i åklagarnas verksamhet. Givet de nyss gjorda uppskattningarna och antagandet att det tar åklagaren i genomsnitt cirka 30 minuter att upprätta och lämna in en ansökan till tingsrätten skulle tidsåtgången för åklagarens arbete i dessa delar kunna minska med mellan 300 och 3 000 timmar årligen (alltså från 600 timmar minus den tid som fortfarande kommer att krävas även med vårt förslag, dvs. 300 timmar, till 3 600 timmar minus den tid som kommer att

[1] Det finns ingen säker statistik på hur många tillstånd som meddelas efter att ett initialt tillstånd meddelats men det synes utifrån uppgifter från de brottsbekämpande myndigheterna inte vara ovanligt att ytterligare tillstånd meddelas efter ett inledande beslut.

krävas även med vårt förslag, dvs. 600 timmar). Detta förutsatt att domstolarna anser att det är utan betydelse med sammanträde.

Ett annat sätt att beräkna besparingen av tidsåtgång med vårt förslag är att i stället utgå från de åtta exempelärenden som redovisas i slutet av avsnitt 6.2 och som tar sikte på hur många sammanträden som hållits i ärendena. Av dessa framgår att det, utöver det lagstadgade minimiantalet sammanträden, kan ha hållits 169 sammanträden. Totalt fanns det i ärendena 31 misstänkta personer. Det hölls således i genomsnitt drygt fem sammanträden per person, utöver minimiantalet. Eftersom det är sådana sammanträden som med vårt förslag inte alltid kommer att behöva hållas kan den minskade tidsåtgången för åklagare (och andra brottsbekämpande myndigheter) beräknas utifrån antaganden om hur vanligt förekommande problematiken är.

År 2016 meddelades 3 456 tillstånd till hemlig avlyssning av elektronisk kommunikation. Givet att antalet tillstånd under samma tidsperiod som exempelärendena avser är ungefär detsamma motsvarar 169 tillstånd (förutsatt då att samtliga ansökningar ledde till tillstånd) knappt fem procent av samtliga tillstånd. Eftersom det är fråga om exempelärenden som inte har inhämtats från hela Åklagarmyndigheten utan endast från fyra kamrar torde således den totala andelen av ärenden där det hålls mer än fem sammanträden utöver antalet minimisammanträden vara avsevärt högre. Mot den bakgrunden, men också med beaktande av att det i genomsnitt inte meddelas mer än knappt tre tillstånd per misstänkt person (se tabell 1 i avsnitt 6.2), gör vi antagandet att det beträffande cirka 20–30 procent av de misstänkta personerna som blir föremål för hemlig avlyssning av elektronisk kommunikation hålls drygt fem sammanträden, utöver minimiantalet sammanträden. Det innebär således, utifrån att totalt cirka 1 200 personer per år blir föremål för hemlig avlyssning av elektronisk kommunikation, att cirka 240–360 misstänkta personer som blir föremål för hemlig avlyssning av elektronisk kommunikation kan förväntas ha som strategi att byta eller använda flera telefoner och sim-kort för att försvåra eller undkomma avlyssning.

Om man således antar att antalet sammanträden kan minska med fem per misstänkt blir det med de angivna antagandena en minskning med 1 200–1 800 sammanträden per år. Med motsvarande antaganden om tidsåtgång per sammanträde som gjordes i

det tidigare räkneexemplet, dvs. att det tar åklagaren mellan 30 minuter och 1,5 timmar att inställa sig för sammanträde, innebär det nu anförda att tidsåtgången för åklagare minskar med mellan 600 timmar (vid 1 200 sammanträden multiplicerat med 30 minuter per sammanträde) och 2 700 timmar (vid 1 800 sammanträden multiplicerat med 1,5 timmar per sammanträde).

Som torde ha framgått är inget av de två beräkningssätt vi använt särskilt exakt. De ger emellertid en fingervisning om hur vårt förslag kan bidra till att minska en onödig resursanvändning av åklagare. Det ska också framhållas att det vid sammanträden i domstolen nästan alltid närvarar personal från andra brottsbekämpande myndigheter än Ekobrottsmyndigheten eller Åklagarmyndigheten, t.ex. utredare från Polismyndigheten eller Tullverket som biträder åklagaren. Vårt förslag kommer således innebära att även dessa myndigheters resurser kan användas på ett mer ändamålsenligt vis, troligen i motsvarande mån som beträffande åklagarna.

Det ska också framhållas att den föreslagna regeländringen torde innebära att när det förenklade förfarandet används så kommer domstolens beslut att kunna meddelas snabbare än vad som är möjligt i dag eftersom sammanträdet inte kommer att behöva inväntas innan beslutet. En konsekvens av det är också att inkoppling av en ny avlyssning kommer att kunna göras snabbare än i dag och att regeländringen således också kommer att minska det glapp som kan uppstå i avlyssningen av en person när denne byter eller använder flera nummer, adresser eller utrustningar i sin kommunikation. Den vinst för brottsbekämpningen som denna effektivitets- och kontinuitetsförbättring medför går emellertid inte att beräkna.

### 7.1.3 Konsekvenser hänförliga till offentliga ombud

Vårt förslag innebär att offentliga ombud inte kommer att närvara vid sammanträde när tingsrätten bedömer att ett sådant skulle vara utan betydelse, eftersom det ju i de fallen inte kommer att hållas något sammanträde. Emellertid ska de offentliga ombuden enligt förslaget utses i efterhand för att ha möjlighet att granska rättens beslut. Som vi framhållit i slutet av avsnitt 6.4.3 torde tingsrätterna i vissa fall med vårt förslag kunna utse ett offentligt ombud som ska till eller är i rätten i ett annat ärende. Om så sker kan kostna-

derna för offentliga ombud förväntas minska något. Det torde emellertid, med hänsyn till att de offentliga ombuden ändå ska ha möjlighet att gå igenom de ärenden som de utses i, inte vara fråga om någon signifikant kostnadsminskning för offentliga ombud. Själva syftet med förändringen är, som framgått, inte heller att minska på kostnader i detta avseende utan att effektivisera förfarandet. Vi konstaterar att vårt förslag under alla förhållanden inte kommer leda till några kostnadsökningar men att det inte heller kan förväntas minska kostnaderna signifikant.

### 7.1.4 Konsekvenser för domstolarna

För domstolarna blir den mest framträdande konsekvensen av vårt förslag att det inte alltid kommer att vara nödvändigt att hålla sammanträde. Typiskt sett torde det ta kortare tid att fatta beslut på handlingarna än vad det gör att fatta dem efter sammanträde, även med beaktande av att domstolen kommer behöva ta ställning till om det behövs sammanträde eller inte. Vår bedömning är därför att vårt förslag, om än marginellt, torde minska domstolarnas tidsåtgång i ärenden om hemlig avlyssning av elektronisk kommunikation.

## 7.2 Ikraftträdande m.m.

**Utredningens förslag:** Den föreslagna lagändringen ska träda i kraft den 1 april 2019.

**Utredningens bedömning:** Tillämpningen av den föreslagna regleringen bör ingå i regeringens årliga redovisning till riksdagen. Det finns inte behov av några särskilda övergångsbestämmelser.

Den föreslagna lagändringen bör inte minst av effektivitetsskäl träda i kraft så snart som möjligt. Vår bedömning är att det med hänsyn till remissförfarande och övriga beredningsåtgärder inte är möjligt att låta de nya bestämmelserna träda i kraft förrän den 1 april 2019. Lämpligen bör uppgifter om användningen av det för-

enklade förfarandet finnas med i den redovisning av användningen av hemliga tvångsmedel som regeringen årligen gör till riksdagen.

När det gäller processrättslig lagstiftning är utgångspunkten att nya regler ska tillämpas genast efter ikraftträdandet. Det innebär att nya regler ska tillämpas på varje processuell företeelse som inträffar efter det att regleringen har trätt i kraft. Det medför att de brottsbekämpande myndigheterna och domstolarna ska tillämpa de nya bestämmelserna även i förundersökningar och tvångsmedelsärenden som har inletts innan de föreslagna bestämmelserna träder i kraft. En sådan ordning är enligt vår bedömning lämplig avseende den av utredningen föreslagna lagändringen. Det finns därför inte behov av några särskilda övergångsbestämmelser.

# 8 Författningskommentar

## 8.1 Förslaget till lag om ändring i rättegångsbalken

**27 kap.**

*28 a §*

*Om rätten har meddelat tillstånd till hemlig avlyssning av elektronisk kommunikation får en ansökan eller anmälan om ytterligare tillstånd mot samma person och som grundas på samma omständigheter men avser ett annat telefonnummer, en annan adress eller en annan elektronisk kommunikationsutrustning än det tidigare tillståndet prövas utan sammanträde och utan att offentligt ombud utsetts om ett sammanträde skulle vara utan betydelse.*

*Ett tillstånd som har meddelats utan att sammanträde hållits enligt första stycket får inte avse annan tid än det tidigare tillståndet.*

*När rätten prövat en ansökan eller anmälan enligt första stycket ska ett offentligt ombud skyndsamt utses och underrättas om beslutet.*

I paragrafen, som är ny, finns undantag till bestämmelsen i 28 § första stycket som innebär ett förenklat beslutsförfarande vid prövningen i vissa fall av om hemlig avlyssning av elektronisk kommunikation ska tillåtas. Övervägandena finns i avsnitt 6.4.

I paragrafens *första stycke* framgår förutsättningarna för att få göra undantag från kravet på sammanträde efter ansökan eller anmälan om hemlig avlyssning av elektronisk kommunikation. För det första krävs att rätten tidigare ska ha meddelat ett tillstånd till den åtgärden. Det kan alltså aldrig komma i fråga att underlåta att hålla sammanträde vid en inledande ansökan eller, efter ett interimistiskt åklagarbeslut, vid en inledande anmälan om hemlig avlyssning av elektronisk kommunikation i ett ärende. Det ligger i sakens natur att ett tidigare tillstånd fortfarande ska vara gällande. Åklag-

are eller domstol får således inte ha hävt det tidigare beslutet så att det inte längre finns något gällande tillstånd. Vidare ska ansökan eller anmälan gälla samma person som avlyssning redan får riktas mot enligt det tidigare tillståndet. Det krävs också att den nya ansökan eller anmälan grundar sig på samma omständigheter som det tidigare meddelade tillståndet grundats på. Det innebär t.ex. att brottsmisstanken ska vara densamma och att andra omständigheter, t.ex. för att klargöra varför åtgärden är av de synnerlig vikt för utredningen, än sådana som legat till grund för det tidigare tillståndet inte får åberopas om det förenklade förfarandet enligt bestämmelsen ska kunna aktualiseras. Det är också en grundläggande förutsättning att den nya ansökan eller anmälan avser ett annat telefonnummer, en annan adress eller en annan elektronisk kommunikationsutrustning än det tidigare tillståndet. Endast om de nu angivna förutsättningarna föreligger får domstolen pröva om det behöver hållas ett sammanträde eller inte. Brister det i någon av dessa förutsättningar gäller 28 § utan undantag. I praktiken innebär således de grundläggande förutsättningarna att det förenklade förfarandet endast får användas om alla förutsättningar förutom nummer, adress eller utrustning är likadana som de var vid prövningen av det tidigare meddelade tillståndet.

Kravet för att pröva ansökan utan att hålla sammanträde är att ett sådant skulle vara utan betydelse. Att ett sammanträde ska vara utan betydelse innebär att undantaget ska tillämpas endast i vissa fall. I praktiken är det främst avsett att träffa de situationer då kriminella som en strategi eller metod för att undkomma eller försvåra de brottsbekämpande myndigheternas avlyssning byter eller använder flera telefoner eller nummer.

En situation då det som regel bör kunna anses att ett sammanträde är utan betydelse är när det är fråga om nummer, adress eller utrustning (t.ex. ett nytt mobiltelefonnummer eller en ny mobiltelefon) av samma slag som i det tidigare meddelade tillståndet och kopplingen till den som avlyssningen ska riktas mot är densamma som vid föregående prövning (t.ex. att den misstänkte innehar utrustningen eller använder numret). Det förenklade förfarandet är däremot inte avsett att användas när skälet för ansökan är att den som är föremål för avlyssningsbeslutet förväntas kontakta en annan person, vars nummer, adress eller utrustning tillståndet ska avse, dvs. när det tidigare tillståndet avser ett telefonnummer eller en annan adress eller ut-

rustning som tillhör någon annan än den som är föremål för avlyssningen. Mellan dessa två ytterlighetsfall ryms en rad olika situationer som får bedömas utifrån omständigheterna i det enskilda fallet. Bestämmelsen är dock inte avsedd att utesluta att det förenklade förfarandet används i situationer då det t.ex. är fråga om ett telefonnummer i det tidigare tillståndet men en viss telefon i den nya ansökan. Avser den nya ansökan emellertid en telefon eller dator som används av flera personer gemensamt, t.ex. i en familj eller på en arbetsplats, bör det förenklade förfarandet inte kunna komma i fråga.

Prövningen av om ett sammanträde är utan betydelse ska utgå från såväl det tidigare meddelade beslutet och de uppgifter som framkommer i den nya ansökan som att det förenklade förfarandet har till syfte att effektivisera hanteringen när kriminella för att försvåra för brottsbekämpande myndigheter byter eller använder flera telefoner och nummer. I prövningen av om det är utan betydelse med sammanträde ligger dessutom att rätten ska göra bedömningar av riskerna för den personliga integriteten och rättssäkerheten om sammanträde inte hålls.

Om rätten kommer fram till att det skulle vara utan betydelse med ett sammanträde får den alltså pröva ansökan eller anmälan på handlingarna. I de fallen ska inte heller ett offentligt ombud utses inför prövningen, vilket också utgör ett undantag från 28 §. Det finns inget hinder mot att bestämmelsen om förenklat förfarande tillämpas flera gånger mot samma person eller att flera nummer, adresser eller utrustningar tillåts inom ramen för ett förenklat förfarande, förutsatt att tingsrätten bedömt sammanträde vara utan betydelse. Dock kan självfallet sådana omständigheter som att flera tillstånd redan har meddelats med användning av det förenklade förfarandet påverka domstolens bedömning av betydelsen av sammanträde.

I *andra stycket* föreskrivs att rättens nya tillstånd inte får avse annan tid än det tidigare tillståndet. Det försäkrar att en eventuell prövning av förlängning av tillståndet sker vid sammanträde där ett offentligt ombud närvarar, enligt huvudregeln i 28 §. Sammanträde ska således alltid hållas när det är fråga om ansökan om förlängning av redan meddelade tillstånd och det förenklade förfarandet får då inte användas. Andra stycket innebär således att tillstånd till hemlig avlyssning av elektronisk kommunikation alltid kommer att ställas

under rättens prövning, vid sammanträde där ett offentligt ombud närvarar, åtminstone en gång per månad, jfr 21 § andra stycket.

Enligt bestämmelsens *tredje stycke* ska ett offentligt ombud utses skyndsamt när rätten har prövat en ansökan eller anmälan enligt det förenklade förfarande som gäller enligt första stycket. Den som utses har rätt att ta del av vad som förekommit i ärendet och överklaga domstolens beslut i enlighet med vad som gäller enligt 26 § andra stycket. Någon rätt att yttra sig innan tingsrättens beslut finns givetvis inte eftersom ombudet utses först i efterhand.

# Kommittédirektiv 2016:36

## Hemlig dataavläsning

Beslut vid regeringssammanträde den 12 maj 2016

### Sammanfattning

En särskild utredare ska undersöka om bestämmelser om hemlig dataavläsning bör införas i svensk rätt för att säkerställa att de brottsbekämpande myndigheterna kan upprätthålla sin förmåga att bekämpa brott.

Utredaren ska bl.a.

- ta reda på vilket behov av hemlig dataavläsning som finns,
- undersöka om hemlig dataavläsning skulle vara en effektiv metod för att bekämpa terroristbrottslighet och andra allvarliga brott,
- klargöra om intresset av att upprätthålla ett starkt skydd för den personliga integriteten ger utrymme för att tillåta hemlig dataavläsning,
- analysera om det är lämpligt att införa hemlig dataavläsning som ett nytt straffprocessuellt tvångsmedel, och
- lämna fullständiga förslag till författningsändringar eller andra förändringar oavsett vad analysen föranleder.

Uppdraget ska redovisas senast den 13 november 2017.

## Förutsättningarna för att bekämpa brott har förändrats

Under senare år har den ökande internationaliseringen i kombination med teknikutvecklingen och en tilltagande internetanvändning inneburit att kriminaliteten delvis har ändrat karaktär. Internet erbjuder lättillgängliga kontaktytor för brottsplanering inom och utom landets gränser och utgör bl.a. en etablerad plattform för våldsbejakande extremism och terrorismpropaganda. Viss typ av kriminalitet, t.ex. barnpornografibrott, har internet som brottsplats. Utvecklingen innebär att även förutsättningarna för att förhindra brott och säkra bevis för begångna brott har förändrats radikalt. Uppgifter om elektronisk kommunikation och andra elektroniska spår är i dag helt nödvändiga för brottsbekämpningen.

Samtidigt har teknik- och kommunikationsutvecklingen under de senaste åren begränsat det praktiska användningsområdet för hemlig avlyssning av elektronisk kommunikation (hemlig avlyssning). Hemlig avlyssning används av brottsbekämpande myndigheter för att komma åt innehållet i kommunikation mellan individer. Nuvarande lagstiftning tillåter hemlig avlyssning av såväl traditionell telefoni som internetbaserad kommunikation, t.ex. ip-telefoni, e-post och sociala medier. Eftersom internetbaserad kommunikation mellan individer allt oftare krypteras när den skickas från avsändare till mottagare får myndigheterna emellertid ofta bara tillgång till krypterad information inom ramen för ett tillstånd till hemlig avlyssning. För leverantörer av internetbaserade tjänster finns det, till skillnad från för leverantörer av traditionell telefoni, inte någon skyldighet att anpassa sina tekniska system så att de kan lämna ut kommunikation som de krypterar i sina nät till brottsbekämpande myndigheter i klartext. De brottsbekämpande myndigheterna har inte någon egen möjlighet att dekryptera kommunikation i realtid. Det är inte heller realistiskt för myndigheterna att bygga upp och underhålla en sådan teknisk förmåga i förhållande till de olika operatörernas system.

Det finns andra tekniska svårigheter med att avlyssna internetbaserad kommunikation inom ramen för ett tillstånd till hemlig avlyssning. Det beror framför allt på att enskilda personer enkelt kan köpa anonymiseringstjänster som skyddar deras identitet, ip-adress, på nätet så att kommunikationen blir helt anonym. Teknikutvecklingen har också medfört att det inte längre är självklart att en viss ip-adress motsvarar en enskild abonnent. Flera abonnenter

kan dela på en och samma adress vilket medför att ip-adressen inte är synonym med den misstänktes identitet på nätet. Den stora mängden krypterad information på nätet innebär också att det kan vara svårt för brottsbekämpande myndigheter att identifiera vad som är kommunikation mellan individer i det samlade flödet.

En effektiv brottsbekämpning förutsätter att de brottsbekämpande myndigheterna har ändamålsenliga verktyg för att bekämpa brott. Flera länder tillåter att de brottsbekämpande myndigheterna använder sig av hemlig dataavläsning som metod. I Danmark har hemlig dataavläsning använts sedan 2002. I Finland möjliggör relativt ny lagstiftning hemlig dataavläsning. Också Tyskland använder sig av en sådan metod. De olika länderna har reglerat metoden på olika sätt. Norge arbetar för närvarande med ett lagförslag om hemlig dataavläsning som ska presenteras för Stortinget. Viktiga lärdomar kan dras av hur andra länder till exempel har valt att avgränsa vilka brott som verktyget får användas för och hur överskottsinformation ska hanteras.

Beredningen för rättsväsendets utveckling (BRU) föreslog 2005 att hemlig dataavläsning skulle införas som ett nytt tvångsmedel i svensk rätt (SOU 2005:38). Som bakgrund till förslaget anfördes bl.a. att den organiserade brottsligheten alltmer söker sig till kommunikationsformer som är säkrare än telefoner, utnyttjar modern teknik och använder internet som ett arbetsredskap i verksamheten. Möjligheten att kommunicera på ett relativt anonymt och säkert sätt (främst frågan om kryptering) framhölls vid sidan av globaliseringen och mobiliteten som stora utmaningar som den internetrelaterade brottsligheten ställer upp för rättsväsendet. Beredningen bedömde det helt nödvändigt att de brottsbekämpande myndigheterna skulle ha möjlighet att använda effektiva arbetsmetoder, inte minst med anknytning till internet, för att den kvalificerade brottsligheten med dess struktur, inriktning och tillvägagångssätt skulle kunna bekämpas (SOU 2005:38, s. 360). Förslaget kritiserades av många remissinstanser och har inte lett till lagstiftning. Den huvudsakliga kritiken gällde att det föreslagna tvångsmedlets effektivitet och integritetseffekter inte ansågs tillräckligt klarlagda. Dessutom ifrågasatte flera remissinstanser om beskrivningen av teknikutvecklingen var rättvisande och därmed om behovet av åtgärder var så tungt vägande att det motiverade ett nytt tvångsmedel.

På motsvarande sätt som BRU redovisade Utredningen om vissa hemliga tvångsmedel några år senare att det vid den kartläggning av tillämpningen av vissa hemliga tvångsmedel som utredningen genomfört hade framkommit att personer inom den organiserade brottsligheten ägnar stor möda åt att anpassa sin kommunikation så att myndigheterna inte ska kunna avlyssna den. Utredningen konstaterade att krypterade telefonitjänster används liksom e-post och att det finns exempel på hur gemensamma mejlkonton utnyttjas för att undgå att meddelanden sänds mellan konton (SOU 2012:44, s. 765).

Det är avgörande att de brottsbekämpande myndigheterna upprätthåller sin förmåga att bekämpa brott. Teknik- och samhällsutvecklingen innebär att det nu finns anledning att på nytt undersöka om hemlig dataavläsning bör införas som ett straffprocessuellt tvångsmedel. Vid en sådan bedömning måste det säkerställas att grundläggande rättigheter respekteras och att intrång i enskildas integritet minimeras.

## Uppdraget att undersöka om hemlig dataavläsning bör införas som ett nytt straffprocessuellt tvångsmedel

Det finns inte någon fastställd definition av hemlig dataavläsning. Som utgångspunkt för en analys kan begreppet definieras som en metod för de brottsbekämpande myndigheterna att med någon form av tekniskt hjälpmedel i hemlighet bereda sig tillgång till en dator eller annan teknisk utrustning som används för kommunikation och därigenom få besked om hur utrustningen används i realtid och vilken information som finns i den. Detta kan t.ex. ske genom att en hård- eller mjukvara placeras, antingen fysiskt eller elektroniskt, via en eller flera trojaner, i en användares tekniska utrustning.

Enligt 2 kap. 6 § regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om intrånget sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Övervägandena om att införa regler om hemlig dataavläsning i svensk rätt fordrar en avvägning mellan å ena sidan samhällets behov av en effektiv brottsbekämpning och å andra sidan den enskildes rätt till integritet i förhållande till staten. Bara om hemlig dataavläsning bedöms vara en proportionerlig åtgärd kan den tillåtas. För att det ska vara möjligt att göra den avvägning som behövs måste det inledningsvis

fastställas om det finns ett reellt behov av hemlig dataavläsning som metod i brottsbekämpningen eller om den brottsbekämpande förmågan kan upprätthållas med mindre integritetskänsliga metoder. Hur stort behovet av hemlig dataavläsning kan bedömas vara beror bl.a. på hur den moderna brottsligheten ser ut och samhällsutvecklingen i övrigt. Den tekniska utvecklingen och de förändrade förutsättningar för kommunikation som den medfört behöver särskilt uppmärksammas. Endast under förutsättning att behovet är tungt vägande och grundligt redovisat kan det ligga till grund för fortsatta överväganden om att införa metoden.

Nästa fråga blir i vilken utsträckning hemlig dataavläsning kan förväntas vara en effektiv metod för brottsbekämpning i förhållande till behovet. Svaret på den frågan är i stor utsträckning beroende av hur metoden tekniskt kan utformas. Undersökningen ska utgå från de tekniska möjligheter som finns och beakta de svårigheter vid verkställighet som kan förutses. Frågan hur bearbetning av information som inhämtas genom metoden kan förväntas gå till kommer att ha betydelse liksom hur myndigheterna ska skaffa den tekniska förmåga som krävs för att använda metoden. Risken för att de personer som begår brott anpassar sitt beteende för att komma runt de nya övervakningsverktygen och hur det skulle påverka effektiviteten behöver beaktas. Även frågan om vilka resurser metoden förutsätter bör belysas.

Behovet och den förväntade effekten behöver vidare bedömas utifrån olika brott. Hemlig dataavläsning skulle kunna vara en effektiv metod för att bekämpa terroristbrottslighet. Det kan även finnas andra allvarliga brott som hemlig avlyssning av elektronisk kommunikation får användas mot och som är svåra att utreda utan tillgång till hemlig dataavläsning. Behovet och den förväntade effekten behöver också belysas utifrån olika syften med åtgärden. Straffprocessuella tvångsmedel kan användas både i syfte att förhindra och att utreda brott. Behovet kan skilja sig mellan dessa användningsområden. Exempelvis har behovet av att kunna använda hemlig rumsavlyssning i preventivt syfte bedömts vara mindre än motsvarande behov för andra hemliga tvångsmedel (prop. 2013/14:237 s. 101). Hemlig avlyssning kan användas både för att förhindra och utreda brott medan hemlig rumsavlyssning enbart är tillåtet för att utreda brott inom ramen för en förundersökning. Behovet av den tänkta åtgärden kan också vara olika för olika brott. För effekten av tvångs-

medlet är det vidare av betydelse vilka beviskrav som ska ställas på tvångsåtgärdens betydelse för det fastställda ändamålet med åtgärden.

Varje befogenhet för staten att bereda sig tillgång till information om medborgarna leder till ingrepp i den personliga integriteten. Ramarna för intrånget bestäms av hur befogenheten avgränsas och utformas i lag. En behörighet för brottsbekämpande myndigheter att i realtid hemligt läsa information i och från datorer och andra tekniska utrusningar, t.ex. mobiltelefoner, skulle potentiellt kunna innebära ett mycket omfattande intrång i enskildas privatliv. Vid överväganden om hemlig dataavläsning måste därför integritetseffekterna beskrivas noga. Det måste så långt det är möjligt redogöras för hur skyddet för den personliga integritetens kärnområden, dvs. sådant som rör individen och dennes personlighet, skulle påverkas av hemlig dataavläsning, bl.a. risken för att andra personer än den som är föremål för tvångsåtgärden påverkas. Regleringen av bland annat hur överskottsinformation får användas och hur tillsyn ska utföras spelar en viktig roll i denna bedömning. Behovet och den förväntade nyttan av att kunna använda hemlig dataavläsning för de olika syftena där ett behov har identifierats måste vägas mot det förväntade integritetsintrånget av en sådan användning. Även frågor om hur metoden skulle påverka enskildas egendomsskydd när det gäller tekniska utrustningars lagringsutrymme (eventuella begränsningar i överföring av datamängd och kapacitet) och kostnader för enskilda behöver beaktas.

Oavsett hur avgränsningen mellan integritets- och effektivitetshänsyn utfaller är det ett ovillkorligt krav att de bestämmelser som föreslås uppfyller högt ställda krav på rättssäkerhet. Det finns därför anledning att noga analysera vilka kvalifikationskrav som är nödvändiga för tillämpningen, hur beslutsordningen bör se ut, hur efterhandskontroll och övrig tillsyn bör fungera, hur underrättelseskyldighet till enskilda bör utformas, hur jurisdiktionsreglerna kan upprätthållas och hur användningen av överskottsinformation ska regleras.

Utredaren ska

- ta reda på vilket behov de brottsbekämpande myndigheterna har av att hemligt i realtid bereda sig tillgång till information i datorer och andra tekniska utrustningar för att effektivt kunna fullgöra sin uppgift, bl.a. i förhållande till övriga metoder för att bekämpa brott inklusive övriga (hemliga) tvångsmedel, och vid analysen särredovisa Åklagarmyndighetens, Ekobrottsmyndighetens, Polismyndighetens, Säkerhetspolisens och Tullverkets behov,
- undersöka vilka möjligheter som modern teknik kan ge de brottsbekämpande myndigheterna att i realtid i hemlighet läsa information i datorer och andra tekniska utrustningar och vilka begränsningar som följer av tekniken och av möjligheten att använda motmedel mot en sådan åtgärd,
- kartlägga och med beaktande av eventuell sekretess beskriva hur en sådan metod kan förväntas verkställas och avbrytas eller avslutas inklusive de operativa svårigheterna med detta,
- analysera i vilken utsträckning det kan bidra till en effektiv brottsbekämpning att ge brottsbekämpande myndigheter befogenhet att i realtid i hemlighet läsa information i datorer och andra tekniska utrustningar,
- undersöka vilket integritetsintrång detta skulle medföra för enskilda och beskriva vilka avgränsningar som behövs,
- utifrån en avvägning mellan effektivitets- och integritetsskäl ta ställning till om de brottsbekämpande myndigheterna bör ges möjlighet att använda hemlig dataavläsning för att bekämpa terroristbrottslighet och andra allvarliga brott, som i dag ger möjlighet till hemlig avlyssning av elektronisk kommunikation,
- avgöra de närmare förutsättningarna för en sådan användning bl.a. i fråga om syfte, tillämpningsområde och rättssäkerhetsgarantier i enlighet med Europakonventionen och den praxis som Europeiska domstolen för de mänskliga rättigheterna har utvecklat,
- ta ställning till i vilken utsträckning åtgärden ska kunna användas i det internationella rättsliga samarbetet, och

- lämna förslag till författningsändringar eller andra förändringar oavsett vad analysen föranleder.

Vid utarbetandet av lagförslag ska utredaren så långt som det är möjligt välja en teknikneutral reglering. Uppgifter i utredningen ska redovisas med beaktande av eventuell sekretess. Utredaren är fri att lämna sådana närliggande förslag till författningsändringar som bedöms vara nödvändiga.

## Ekonomiska konsekvenser

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för staten, kommuner och landsting och konsekvenserna i övrigt av förslagen. Om förslagen förväntas leda till kostnadsökningar för staten, kommuner och landsting, ska utredaren föreslå hur dessa ska finansieras. Utredaren ska också redovisa i vilken utsträckning resursutnyttjandet i rättsväsendet kan bli effektivare genom förslagen.

## Lagstiftning i andra länder

Utredaren ska redovisa gällande rätt och eventuellt pågående arbete i övriga nordiska länder samt de övriga länder som bedöms vara relevanta för utredningsuppdraget och i övrigt göra de internationella jämförelser som utredaren bedömer befogade.

## Samråd och redovisning

Utredaren ska vid genomförande av uppdraget inhämta upplysningar från företrädare för berörda myndigheter och organ, särskilt Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Säkerhets- och integritetsskyddsnämnden, Post- och telestyrelsen och Sveriges advokatsamfund.

Utredaren ska också hålla sig informerad om och beakta sådant arbete inom Regeringskansliet samt inom EU och andra internationella forum som är relevant för uppdraget. Utredaren ska särskilt uppmärksamma det pågående arbetet inom ramen för utredningen om moderna regler om beslag och husrannsakan (dir. 2016:20) och

samordna sina bedömningar med den utredningen i den utsträckning det behövs.

Uppdraget ska redovisas senast den 13 november 2017.

(Justitiedepartementet)

# Kommittédirektiv 2017:102

## Tilläggsdirektiv till Utredningen om hemlig dataavläsning (Ju 2016:12)

Beslut vid regeringssammanträde den 19 oktober 2017

### Utvidgning av och förlängd tid för uppdraget

Regeringen beslutade den 12 maj 2016 kommittédirektiv om att undersöka om det bör införas bestämmelser om hemlig dataavläsning i svensk rätt (dir. 2016:36).

Utredaren får nu även i uppdrag att

- analysera och ta ställning till om tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan knytas enbart till den person som åtgärden avser, i stället för till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning, och
- föreslå de författningsändringar eller andra åtgärder som behövs.

Utredningstiden förlängs. Uppdraget ska i den del som omfattas av dessa direktiv redovisas senast den 13 april 2018. Uppdraget i övrigt ska fortfarande redovisas senast den 13 november 2017.

*Tillstånd till hemlig avlyssning och hemlig övervakning av elektronisk kommunikation är knutna till ett visst telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning*

I den brottsbekämpande verksamheten är det ibland nödvändigt att använda hemliga tvångsmedel. Till dessa räknas bl.a. hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation.

Hemlig avlyssning av elektronisk kommunikation får endast avse ett visst telefonnummer, annan adress (t.ex. e-postadress) eller en viss elektronisk kommunikationsutrustning, med viss anknytning till den person som åtgärden avser. Detsamma gäller som huvudregel även vid hemlig övervakning av elektronisk kommunikation. Vilket telefonnummer eller liknande som tvångsmedlet avser ska anges i tillståndsbeslutet. Tillstånden beslutas normalt av domstol.

I kriminella kretsar är det vanligt med anonyma sim-kort och att personer byter både kort och telefon i syfte att undvika avlyssning eller övervakning. Varje gång det sker ett sådant byte måste ett nytt tvångsmedelsbeslut meddelas eftersom tillstånden avser ett visst nummer eller liknande. Det har tidigare diskuterats om tillstånden i stället borde knytas enbart till den person som tvångsmedelsbeslutet avser (se t.ex. prop. 2013/14:237, s. 96–97 och 106). En sådan ordning skulle enligt de brottsbekämpande myndigheterna kunna bidra till en mer effektiv verkställighet och till att säkerställa att rätt person avlyssnas eller övervakas. Regeringen var dock inte beredd att göra några förändringar då och anförde bl.a. att förutsättningarna för tillämpningen av proportionalitetsprincipen skulle försämras om åtgärden inte var bestämd till en viss adress eller liknande. Detsamma gällde enligt regeringen möjligheten att bedöma om tillståndet behöver förenas med villkor för att tillgodose intresset av att enskildas personliga integritet inte kränks i onödan. För att bidra till behovet av effektivisering utökades däremot möjligheten för åklagare att fatta interimistiska beslut om hemlig avlyssning och hemlig övervakning av elektronisk kommunikation (prop. 2013/14:237, bet. 2014/15:JuU2, rskr. 2014/15:22).

Åklagarmyndigheten har därefter tagit upp frågan på nytt. Enligt myndigheten är det ovanligt att domstolen gör någon egentlig prövning av kopplingen mellan den misstänkte och adressen, utan prövningen koncentreras i första hand till om det kan antas att

brott begåtts och till kopplingen mellan den misstänkte och brottet. Enligt Åklagarmyndigheten bör man överväga en ordning där domstolen fattar ett grundbeslut, men där åklagaren är behörig att besluta om avlyssning eller övervakning av ytterligare telefonnummer eller andra adresser (dnr Ju2015/3153/Å). Vidare har riksdagen tillkännagett som sin mening att det bör utredas om denna typ av beslut skulle kunna kopplas till en person i stället för till ett telefonnummer eller annan adress (bet. 2016/17:JuU17, punkt 6, rskr. 2016/17:212).

*Kan tillståndet i stället knytas enbart till den person som åtgärden avser?*

För att brottslighet ska kunna bekämpas på ett effektivt sätt krävs att de brottsbekämpande myndigheterna har tillgång till ändamålsenliga och verkningsfulla verktyg. Personer som är föremål för tvångsmedel kan i dag tillfälligt undgå hemlig avlyssning och hemlig övervakning av elektronisk kommunikation i realtid genom att t.ex. byta telefon eller sim-kort. Enligt Åklagarmyndigheten finns det ett utrymme för att förändra hanteringen av situationer när nya adresser eller liknande aktualiseras efter att ett initialt beslut om avlyssning eller övervakning har fattats. En ny analys om det finns förutsättningar att knyta rätten att använda tvångsmedlen till den person som tvångsmedelsbeslutet avser och inte till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning ska göras. Samtidigt är det viktigt att reglerna och deras tillämpning uppfyller mycket högt ställda krav på rättssäkerhet och att intrång i enskildas integritet minimeras. En särskild fråga är vilka konsekvenser en sådan förändring kan ha för rättssäkerheten och enskildas personliga integritet. För att säkerställa att rätt person blir föremål för tvångsmedlet är det också angeläget att prövningen av om avlyssningen eller övervakningen ska avse ett nytt telefonnummer eller liknande är reell och väl underbyggd.

Utredaren ska

- analysera och ta ställning till om tillstånd till hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan knytas enbart till den person som åtgärden avser, i stället för till ett telefonnummer, annan adress eller en viss elektronisk kommunikationsutrustning, och
- föreslå de författningsändringar och andra åtgärder som behövs.

## Redovisning av uppdraget

Utredningstiden förlängs. Uppdraget ska i den del som omfattas av dessa direktiv redovisas senast den 13 april 2018. Uppdraget i övrigt ska fortfarande redovisas senast den 13 november 2017.

(Justitiedepartementet)

# Statens offentliga utredningar 2018

## Kronologisk förteckning

1. Ett reklamlandskap i förändring – konsumentskydd och tillsyn i en digitaliserad värld. Fi.
2. Stärkt straffrättsligt skydd för blåljusverksamhet och andra samhällsnyttiga funktioner. Ju.
3. En strategisk agenda för internationalisering. U.
4. Framtidens biobanker. S.
5. Vissa processuella frågor på socialförsäkringsområdet. S.
6. Grovt upphovsrättsbrott och grovt varumärkesbrott. Ju.
7. Försvarsmaktens långsiktiga materielbehov. Fö.
8. Kunskapsläget på kärnavfallsområdet 2018. Beslut under osäkerhet. M.
9. Ökad trygghet för studerande som blir sjuka. U.
10. Myndighetsgemensam indelning – samverkan på regional nivå. Volym 1. Myndighetsgemensam indelning – författningsändringar till följd av ny landstingsbeteckning. Volym 2. Fi.
11. Vårt gemensamma ansvar – för unga som varken arbetar eller studerar. U.
12. Uppdrag: Samverkan 2018. Många utmaningar återstår. A.
13. Finansiering av infrastruktur med skatt eller avgift? Fi.
14. Bidragsbrott och underrättelseskyldighet vid felaktiga utbetalningar från välfärdssystemen – en utvärdering. Fi.
15. Mindre aktörer i energilandskapet – genomgång av nuläget. M.
16. Vägen till självkörande fordon – introduktion. Del 1 + 2. N.
17. Med undervisningsskicklighet i centrum – ett ramverk för lärares och rektorers professionella utveckling. U.
18. Statens stöd till trossamfund i ett mångreligiöst Sverige. Ku.
19. Forska tillsammans – samverkan för lärande och förbättring. U.
20. Gräsrotsfinansiering. Fi.
21. Flexibel rehabilitering. A.
22. Ett ordnat mottagande – gemensamt ansvar för snabb etablering eller återvändande. A.
23. Konstnär – oavsett villkor? Ku.
24. Tid för utveckling. A.
25. Juridik som stöd för förvaltningens digitalisering. Fi.
26. Några frågor i skyddslagstiftningen. Fö.
27. Ekonomiska sanktioner mot terrorism. UD.
28. En nationell alarmeringstjänst – för snabba, säkra och effektiva hjälpinsatser. Ju.
29. Validering i högskolan – för tillgodoräknande och livslångt lärande. U.
30. Förenklat förfarande vid vissa beslut om hemlig avlyssning. Ju.

# Statens offentliga utredningar 2018

## Systematisk förteckning