Datalagring och integritet

Betänkande av Datalagringsutredningen

Stockholm 2015

STATENS OFFENTLIGA UTREDNINGAR

SOU 2015:31

SOU och Ds kan köpas från Fritzes kundtjänst.
Beställningsadress: Fritzes kundtjänst, 106 47 Stockholm
Ordertelefon: 08-598 191 90
E-post: order.fritzes@nj.se
Webbplats: fritzes.se

För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer
på uppdrag av Regeringskanslets 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/remiss.

Layout: Kommittéservice, Regeringskansliet.
Omslag: Elanders Sverige AB.
Tryck: Elanders Sverige AB, Stockholm 2015.

ISBN 978-91-38-24265-0
ISSN 0375-250X

Till statsrådet Anders Ygeman

Regeringen beslutade den 26 juni 2014 att tillkalla en särskild utredare med uppdrag att utvärdera lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet och analysera Säkerhetspolisens behov av en möjlighet enligt lagen att hämta in uppgifter om brottslig verksamhet som innefattar vissa samhällsfarliga brott. I uppdraget har även ingått att överväga om de rättssäkerhets- och integritetsstärkande åtgärder som vidtogs när inhämtningslagen infördes har varit tillräckliga eller om det finns behov av andra sådana åtgärder. Vidare har det ingått i uppdraget föreslå de förändringar i övrigt som bedöms lämpliga för att stärka skyddet för den personliga integriteten när det gäller reglerna om lagring av uppgifter om elektronisk kommunikation för brottsbekämpande ändamål.

F.d. justitierådet och ordföranden i Högsta förvaltningsdomstolen Sten Heckscher förordnades att fr.o.m. den 1 oktober 2014 vara särskild utredare.

Förordnade experter under hela eller delar av utredningstiden har varit polisöverintendenten Sören Clerton (Polismyndigheten), operative ledaren Fredrik Hallström (Säkerhetspolisen), advokaten Tomas Nilsson (Advokatsamfundet), enhetschefen Emily Alfvén Nickson och föredraganden Ulf Malm (Säkerhets- och integritetsskyddsnämnden), juristen Staffan Lindmark (Post- och telestyrelsen), enhetschefen Lars Korsell och utredaren Nicole Thorell (Brottsförebyggande rådet), professorn Iain Cameron (Uppsala universitet) samt kanslirådet Eva Bloch (Justitiedepartementet).

Rättssakkunnige Daniel Eriksson har varit sekreterare.

Förordnande- respektive anställningstider för experterna och sekreteraren framgår av en förteckning som bifogas.

Utredningen har antagit namnet Datalagringsutredningen.

Sten Heckscher är ensam utredningsman och svarar ensam för innehållet i betänkandet. Experterna har emellertid deltagit i arbetet i sådan utsträckning att det är befogat att använda vi-form i betänkandet. Skilda uppfattningar i enskildheter och beträffande formuleringar kan dock förekomma utan att detta har behövt komma till uttryck i något särskilt yttrande.

Härmed överlämnas betänkandet *Datalagring och integritet* (SOU 2015:31). I och med detta är utredningens uppdrag slutfört.

Stockholm i mars 2015

Sten Heckscher

/Daniel Eriksson

Förteckning över förordnande- respektive anställningstider

Förordnade experter

Polisöverintendenten Sören Clerton, fr.o.m. den 3 december 2014

Operative ledaren Fredrik Hallström, fr.o.m. den 20 oktober 2014

Advokaten Tomas Nilsson, fr.o.m. den 20 oktober 2014

Enhetschefen Emily Alfvén Nickson, fr.o.m. den 20 oktober 2014 till den 1 januari 2015

Föredraganden Ulf Malm, fr.o.m. den 7 januari 2015

Juristen Staffan Lindmark, fr.o.m. den 20 oktober 2014

Enhetschefen Lars Korsell, fr.o.m. den 20 oktober 2014

Utredaren Nicole Thorell, fr.o.m. den 20 oktober 2014

Professorn Iain Cameron, fr.o.m. den 20 oktober 2014

Kanslirådet Eva Bloch, fr.o.m. den 3 december 2014

Sekreterare

Rättssakkunnige Daniel Eriksson, anställd som sekreterare fr.o.m. den 13 oktober 2014

Innehåll

Sammanfattning **13**

Summary **23**

1 Författningsförslag **33**

1.1 Förslag till lag om ändring i rättegångsbalken 33

1.2 Förslag till lag om ändring i lagen (2003:389) om elektronisk kommunikation 35

1.3 Förslag till lag om ändring i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott 37

1.4 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400) 38

1.5 Förslag till lag om ändring i postlagen (2010:1045) 39

1.6 Förslag till lag om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet 41

1.7 Förslag till förordning om ändring i förordningen (2003:396) om elektronisk kommunikation 45

2 Utredningens uppdrag och arbete **47**

2.1 Vårt uppdrag 47

2.2 Utredningsarbetet 47

2.3 Betänkandets disposition 48

3 Bakgrund 51

3.1 Rätten till personlig integritet 51
3.1.1 Integritetsbegreppet 51
3.1.2 Skyddsintressen 52
3.1.3 Regleringen av skyddet för privatlivet 53

3.2 Skyddet för personuppgifter 59
3.2.1 EU:s primärrätt 59
3.2.2 Dataskyddsdirektivet 60
3.2.3 Personuppgiftslagen 62
3.2.4 Polisdatalagen 63
3.2.5 Överföring av personuppgifter till tredje land 67

3.3 Elektronisk kommunikation 70
3.3.1 Allmänt om elektronisk kommunikation 70
3.3.2 Integritetsskydd och tystnadsplikt vid elektronisk kommunikation 70
3.3.3 Lagen om elektronisk kommunikation 72

3.4 Brottsbekämpande verksamhet 74
3.4.1 Brottsutredande verksamhet 74
3.4.2 Underrättelseverksamhet 75

3.5 Uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet 81
3.5.1 Allmänt om straffprocessuella tvångsmedel 81
3.5.2 Hur används uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet? 83
3.5.3 Regleringen av tillgången till uppgifter 88
3.5.4 Kontrollmekanismer 97

4 Datalagring 107

4.1 Datalagringsdirektivet 107
4.1.1 Direktivets syfte och tillämpningsområde 107
4.1.2 Lagringsskyldighetens omfattning 107
4.1.3 Hanteringen av lagrade uppgifter 108

4.2 Den svenska regleringen 110
4.2.1 Genomförandeprocessen 110

4.2.2 Lagringsskyldighetens omfattning 110
4.2.3 Utlämnande av uppgifter..... 111
4.2.4 Säkerheten för lagrade uppgifter..... 112

4.3 EU-domstolens dom 114

4.4 Analysen 117
4.4.1 Analysens utgångspunkter..... 117
4.4.2 Lagringsskyldighetens omfattning 118
4.4.3 Tillgången till lagrade uppgifter..... 121
4.4.4 Lagringstiden 128
4.4.5 Säkerheten för lagrade uppgifter..... 130
4.4.6 Samlad bedömning..... 133

4.5 Reaktioner på domen..... 133
4.5.1 Reaktioner i Sverige..... 133
4.5.2 Andra reaktioner..... 139

5 Vilka uppgiftskategorier ska lagras? 159

5.1 Inledning..... 159

5.2 Uppgifter som lagras 159
5.2.1 Lagringsskyldigheten enligt datalagringsdirektivet 159
5.2.2 Lagringsskyldigheten enligt svensk rätt 161

5.3 Behovet av lagrade uppgifter 162

5.4 Utredningens bedömning..... 167

6 Krav på lagring inom EU?..... 169

6.1 Inledning..... 169

6.2 De svenska reglerna om säkerhet och tillsyn 169
6.2.1 Säkerhet..... 169
6.2.2 Tillsyn..... 171

6.3 Överföring av personuppgifter till tredje land..... 172
6.3.1 Bedömningen av skyddsnivån enligt dataskyddsdirektivet..... 172

6.3.2 Europeiska kommissionens beslut om adekvat skyddsnivå ... 174
6.3.3 Förhållandet mellan dataskyddsdirektivet och dataskyddskonventionen ... 176
6.4 Utredningens bedömning ... 178

7 Inhämtning av abonnemangsuppgifter ... 183

7.1 Inledning ... 183
7.2 Vilket integritetsintrång innebär utlämnandet av abonnemangsuppgifter? ... 184
7.3 Rutiner för dokumentation och loggning ... 187
7.4 Kontrollsystemet ... 188
7.5 Utredningens förslag ... 190
7.5.1 En särskild tillsynsuppgift? ... 190
7.5.2 Underrättelse till enskild? ... 192
7.5.3 Parlamentarisk kontroll? ... 194
7.5.4 Beslut om inhämtning av abonnemangsuppgifter bör fattas på en viss nivå ... 195
7.5.5 Krav på dokumentation ... 197
7.5.6 Verkställighet ... 197
7.5.7 Utlämnande för andra ändamål ... 198
7.5.8 Utlämnande av abonnemangsuppgifter i underrättelseverksamhet ... 198

8 Uppgifter som omfattas av yrkesmässig tystnadsplikt ... 201

8.1 Inledning ... 201
8.2 Skyddet för yrkesmässig tystnadsplikt ... 202
8.2.1 Tystnadsplikt ... 202
8.2.2 Undantag från vittnesplikt ... 202
8.2.3 Avlyssningsförbud ... 203
8.2.4 Skyldighet att förstöra upptagningar och uppteckningar ... 204
8.2.5 Proportionalitetsprincipen ... 206
8.3 Utredningens förslag ... 208

8.3.1 Förbud mot att hämta in uppgifter om kommunikation med personer som omfattas av yrkesmässig tystnadsplikt? ... 208
8.3.2 Förstörandeskyldighet ... 209

9 Inhämtningslagen ... 211

9.1 Direktiven ... 211

9.2 Utredningens kartläggning ... 212
9.2.1 Metod ... 212
9.2.2 Säkerhetspolisens användning av inhämtningslagen ... 213
9.2.3 Polismyndighetens och Tullverkets användning av inhämtningslagen ... 261

9.3 Åtgärder för att stärka rättssäkerheten eller integritetsskyddet? ... 283
9.3.1 Integritetsstärkande åtgärder vidtogs när inhämtningslagen infördes ... 283
9.3.2 Bör inhämtningslagens beslutsordning ändras? ... 284
9.3.3 Åtgärder inom ramen för den befintliga beslutsordningen ... 294

9.4 Säkerhetspolisens behov av en särskild möjlighet att inhämta uppgifter om viss brottslig verksamhet ... 304
9.4.1 Nuvarande ordning ... 304
9.4.2 Tidigare överväganden ... 305
9.4.3 Säkerhetspolisens behovsbeskrivning ... 307
9.4.4 Utredningens förslag ... 309

10 Övriga frågor ... 313

10.1 Tystnadsplikt för kvarhållande av försändelse enligt lagen om preventiva tvångsmedel ... 313

10.2 Ekobrottsmyndighetens behov av en möjlighet att hämta in uppgifter enligt inhämtningslagen ... 314

10.3 Brottslig verksamhet som innefattar spridning av massförstörelsevapen ... 317

10.4 NAT-teknik 320

11 Genomförande och konsekvenser 321

11.1 Ikraftträdande m.m. 321

11.2 Konsekvenser 321
11.2.1 Inledning 322
11.2.2 Ekonomiska konsekvenser 322
11.2.3 Övriga konsekvenser 323

12 Författningskommentar 325

12.1 Förslaget till lag om ändring i rättegångsbalken 325

12.2 Förslaget till lag om ändring i lagen om elektronisk kommunikation 326

12.3 Förslaget till lag om ändring i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott 327

12.4 Förslaget till lag om ändring i offentlighets- och sekretesslagen 328

12.5 Förslaget till lag om ändring i postlagen 329

12.6 Förslaget till lag om ändring i lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet 330

12.7 Förslaget till förordning om ändring i förordningen om elektronisk kommunikation 332

Bilaga

Kommittédirektiv 2014:101 335

Sammanfattning

Vårt uppdrag

I lagen om elektronisk kommunikation finns bestämmelser som anger att leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster ska lagra vissa uppgifter som genereras eller behandlas i samband med att sådana tjänster tillhandahålls för att uppgifterna ska kunna användas vid brottsbekämpning. Vårt uppdrag har varit att föreslå de förändringar som bedöms lämpliga för att stärka skyddet för den personliga integriteten i förhållande till den regleringen.

Den s.k. inhämtningslagen reglerar Polismyndighetens, Säkerhetspolisens och Tullverkets möjligheter att få tillgång till uppgifter om elektronisk kommunikation i sin underrättelseverksamhet. Utredningen har haft i uppdrag att kartlägga och utvärdera hur lagen har tillämpats samt att överväga om den bör förändras för att stärka rättssäkerheten eller skyddet för den personliga integriteten. Ett annat syfte med uppdraget har varit att analysera Säkerhetspolisens behov av en särskild möjlighet att inhämta uppgifter om viss brottslig verksamhet som inte omfattas av inhämtningslagens huvudregel samt lämna förslag på hur ett sådant behov bör tillgodoses och balanseras mot integritetsintresset.

Bakgrund

Skyddet för privatlivet m.m.

I betänkandets bakgrundsavsnitt redogör vi för de regler om skydd för enskildas privatliv som finns i regeringsformen, Europakonventionen och EU:s rättighetsstadga. Där behandlas också vissa bestämmelser om skydd för enskildas personuppgifter. Vidare innehåller bakgrundsavsnittet beskrivningar av de brottsbekämpande myndig-

heternas verksamhet och de bestämmelser som reglerar dessa myndigheters möjligheter att få tillgång till vissa uppgifter om elektronisk kommunikation som behövs i verksamheten.

Datalagring

Det s.k. datalagringsdirektivet (Europaparlamentets och rådets direktiv 2006/24/EG om lagring av trafikuppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG) syftade till att harmonisera medlemsstaternas regler om skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra vissa uppgifter om elektronisk kommunikation för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal av allvarliga brott. De bestämmelser som genomförde direktivet i svensk rätt finns i lagen om elektronisk kommunikation.

Den 8 april 2014 meddelade EU-domstolen dom i målen C-293/12 och C-594/12, Digital Rights Ireland m.fl., angående giltigheten av datalagringsdirektivet. EU-domstolen förklarade i domen datalagringsdirektivet ogiltigt. Domstolen konstaterade att direktivet innebar ett omfattande och särskilt allvarligt intrång i rätten till privatliv och skyddet av personuppgifter. Domstolen konstaterade dock att en skyldighet att lagra uppgifter är en ändamålsenlig åtgärd för att uppnå syftet att bekämpa allvarlig brottslighet och upprätthålla allmän säkerhet. Eftersom direktivet inte fastställde tydliga och preciserade regler för omfattningen av intrånget i de aktuella rättigheterna ansåg domstolen emellertid att intrången inte begränsades till vad som var absolut nödvändigt för att uppnå sitt syfte. I domen pekade domstolen ut vissa omständigheter som beaktades särskilt vid bedömningen av om direktivet levde upp till kraven på proportionalitet. Domstolen fann vid en samlad bedömning att EU:s lagstiftande församlingar överskridit sina befogenheter då direktivet antogs eftersom det inte lever upp till proportionalitetsprincipen med avseende på de aktuella rättigheterna.

Vilka uppgiftskategorier ska lagras?

Lagringsskyldighetens omfattning enligt svensk rätt regleras av bestämmelser i lagen och förordningen om elektronisk kommunikation. Enligt dessa bestämmelser ska leverantörer av elektroniska kommunikationsnät och kommunikationstjänster lagra vissa uppgifter om bl.a. telefonsamtal, internettrafik och meddelandehantering. Skyldigheten gäller i sex månader räknat från den dag kommunikationen avslutades.

Skyldigheten att lagra dessa uppgifter inkräktar på rättigheter som enskilda är tillförsäkrade enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga. För att en sådan åtgärd ska vara godtagbar krävs att den objektivt sett är ägnad att uppnå syftet med åtgärden och att den är proportionerlig.

Av uppgifter som vi har inhämtat från polisen framgår att samtliga uppgiftskategorier som lagras enligt dagens regler är av stor vikt för den brottsbekämpande verksamheten. Vår bedömning är därför att lagringsskyldighetens inte omfattar annat än vad som är strikt nödvändigt för att uppnå syftet med regleringen. Det bör därför inte göras några förändringar i fråga om vilka uppgiftskategorier som ska lagras.

Krav på lagring inom EU?

Enligt EU-domstolen är den oberoende myndighetskontrollen en grundläggande beståndsdel i skyddet för enskilda individer i samband med behandlingen av personuppgifter. Domstolen pekade i datalagringsdomen på att en brist i datalagringsdirektivet var att den oberoende myndighetskontrollen av att skydds- och säkerhetskraven för de lagrade uppgifterna följs inte fullt ut kunde anses vara garanterad i direktivet. Detta var enligt domstolen en konsekvens av att direktivet inte krävde att uppgifterna skulle lagras inom unionen.

Vi har mot den bakgrunden övervägt om det bör införas ett förbud mot att uppgifter som lagras enligt de svenska reglerna förs över till ett s.k. tredje land för lagring där. Emellertid har vi funnit att det svenska regelverket är utformat på ett sådant sätt att tillsynsmyndigheten, Post- och telestyrelsen, har möjligheter att bedriva en aktiv och ändamålsenlig tillsynsverksamhet även gentemot leverantörer som väljer att lagra uppgifter utanför unionen. Vidare har vi

beaktat att personuppgifter får föras över till tredje land endast om landet i fråga säkerställer en adekvat nivå av skydd för uppgifterna. Kravet på adekvat skydd innebär bl.a. att det tredje landet ska ha inrättat kontrollmekanismer som bevakar att landets skyddsregler i fråga om personuppgifter följs. Vår bedömning är därför att den oberoende myndighetskontrollen är garanterad i svensk rätt även i förhållande till leverantörer som skulle välja att lagra uppgifter utanför EU. Vidare har vi funnit att ett krav i nationell rätt på lagring inom EU eller EES inte går att förena med den övriga EU-regleringen på området samt med Sveriges åtaganden enligt dataskyddskonventionen.

Mot den bakgrunden gör vi bedömningen att det inte bör införas något generellt förbud mot att uppgifter som lagras enligt de svenska datalagringsreglerna förs över till tredje land för lagring där.

Inhämtning av abonnemangsuppgifter

En av de brister i datalagringsdirektivet som EU-domstolen pekade på i sin dom var att direktivet inte angav några objektiva kriterier för att avgränsa de nationella myndigheternas tillgång till och användning av de lagrade uppgifterna. Domstolen noterade också att direktivet inte krävde att tillgången till uppgifter skulle vara underkastad någon förhandskontroll av en domstol eller oberoende myndighet som har till uppgift är att se till att tillgången begränsas till vad som är strikt nödvändigt.

Abonnemangsuppgifter som lagras med stöd av de svenska datalagringsreglerna får lämnas ut till brottsbekämpande myndigheter utan krav på att den brottslighet som uppgifterna lämnas ut för ska vara av någon viss svårhetsgrad. Vidare får uppgifter hämtas in efter beslut av den brottsbekämpande myndigheten och således utan föregående kontroll av en oberoende instans.

Vi har mot den bakgrunden övervägt ett flertal olika åtgärder som skulle kunna bidra till att stärka kontrollen över de brottsbekämpande myndigheternas tillämpning av reglerna om inhämtning av abonnemangsuppgifter. Bland annat har vi övervägt om ett tillsynsorgan bör få i uppgift att utöva tillsyn som specifikt tar sikte på tillämpningen av dessa regler. Vi gör dock bedömningen att nackdelarna med en sådan ordning överväger fördelarna. Däremot

föreslår vi att beslut om inhämtning av abonnemangsuppgifter ska få fattas endast av vissa särskilt utpekade befattningshavare inom den myndighet som begär uppgifterna. Vidare föreslår vi att beslut om inhämtning av sådana uppgifter ska dokumenteras på visst sätt. Dessa åtgärder bedöms kunna bidra till högre kvalitet i beslutsfattandet och till att den tillsyn som bedrivs av JO, JK, Datainspektionen och SIN blir mer effektiv. Vidare lämnar vi förslag på vissa förtydliganden i bestämmelsen om inhämtning av abonnemangsuppgifter. Syftet är att göra det tydligt att bestämmelsen kan tillämpas i de brottsbekämpande myndigheternas underrättelseverksamhet.

Uppgifter som omfattas av yrkesmässig tystnadsplikt

EU-domstolen lyfte i sin dom fram att en brist i datalagringsdirektivet var att det inte innehöll några undantag från lagringskravet, vilket innebar att det var tillämpligt även på personer vilkas kommunikation enligt nationell rätt omfattas av tystnadsplikt.

Vi har därför övervägt om det bör införas ett förbud mot att hämta in uppgifter om kommunikation med personer som omfattas av yrkesmässig tystnadsplikt. I svensk rätt är det emellertid en uppgifts innehåll som avgör om den omfattas av tystnadsplikt. Vid inhämtning av s.k. metadata känner den myndighet som hämtar in uppgifterna normalt inte till innehållet i kommunikationen. Vår bedömning är därför att ett sådant förbud skulle vara mycket svårt att tillämpa. Vidare bedömer vi att ett sådant förbud skulle vara av begränsad praktisk betydelse. Detta eftersom proportionalitetsprincipen normalt hindrar att uppgifter hämtas in, om myndigheterna i något undantagsfall på förhand skulle känna till att kommunikationen omfattas av tystnadsplikt. Däremot föreslår vi att det ska införas regler om att uppgifter om sådan kommunikation ska förstöras i de fall myndigheterna i efterhand får kännedom om att kommunikationen omfattas av sådan tystnadsplikt.

Inhämtningslagen

Kartläggningen

En del av vårt uppdrag har varit att kartlägga den hittillsvarande tillämpningen av inhämtningslagen. Den undersökningsmetod som vi har valt innebär att vi på djupet har granskat ett urval av underrättelseärenden där inhämtningslagen har tillämpats av Polismyndigheten, Säkerhetspolisen eller Tullverket. I samband med undersökningen har utredningen, i vart och ett av de utvalda ärendena, tagit del av de beslut enligt inhämtningslagen som fattats i ärendena samt bakomliggande skriftligt material. Därefter har företrädare för utredningen intervjuat den ansvarige handläggaren om ärendet. Syftet har varit att på djupet tränga in i frågorna om nytta, behov och integritetsintrång.

Resultatet av kartläggningen redovisas i detalj i betänkandet och har varit en viktig del av underlaget för vår analys, våra bedömningar och våra förslag i fråga om inhämtningslagen. Vi har kunnat konstatera att de brottsbekämpande myndigheterna hanterar ärenden enligt inhämtningslagen på ett i allt väsentligt tillfredsställande sätt. Vidare har vi funnit att lagen är ett viktigt redskap i myndigheternas underrättelseverksamhet. Tillämpningen av lagen leder i de allra flesta fall till att myndigheterna får tillgång till relevant information som bidrar till att föra underrättelseärendena framåt. Det finns därför underlag för bedömningen att lagen innebär beaktansvärd nytta i underrättelseverksamheten. Lagen leder dock även till integritetsintrång, både för de personer som ärendena avser och de personer som dessa har kontakt med.

Inhämtningslagens beslutsordning

EU-domstolen pekade i datalagringsdomen på att direktivet inte föreskrev att de behöriga nationella myndigheternas tillgång till lagrade uppgifter skulle vara underkastad någon förhandskontroll utförd av en domstol eller oberoende myndighet. Vi har därför, och i enlighet med våra direktiv, övervägt bl.a. om allmän domstol bör anförtros uppgiften att fatta beslut om inhämtning av uppgifter. Emellertid har vi funnit att frågor om inhämtning av uppgifter i underrättelseverksamhet lämpar sig mindre väl för prövning i allmän

domstol. I underrättelseverksamheten, som är skild från och ligger i tiden före en förundersökning, är syftet att genom en bred informations- och kunskapsinsamling ge underlag för bearbetning och analys. Utgångspunkten för underrättelseverksamheten är, ofta utifrån en mer övergripande ansats, att studera och kartlägga en befarad brottslig verksamhet för att förebygga eller förhindra att brottsligheten genomförs. Eftersom verksamheten inte som i en förundersökning, är inriktad mot någon specifik brottslig gärning – och ofta inte heller mot någon särskild utpekad person – gör sig partsintresset inte heller gällande på samma sätt i underrättelseverksamheten som under en förundersökning. Integritetsaspekten i underrättelseskedet präglas därför mer av ett medborgarperspektiv än av ett sådant tvåpartsförfarande som lämpar sig för prövning i allmän domstol. Det finns också anledning att vara tveksam till om domstolarna skulle ha möjlighet att tillgodose behovet av snabba beslut.

Vi har också övervägt om beslutsbefogenheten enligt inhämtningslagen bör anförtros åklagare eller ett nytt beslutsorgan, t.ex. en nämnd. Sådana alternativ har samma svagheter som en domstolsprövning. Det finns också andra nackdelar. Vi bedömer t.ex. att en uppgift för åklagare att fatta beslut om den aktuella inhämtningen skulle vara svår att förena med den roll åklagarna har i det straffprocessuella systemet. Mot bakgrund av att dagens beslutsordning fungerar väl gör vi därför bedömningen att beslut enligt inhämtningslagen även i fortsättningen bör fattas av de brottsbekämpande myndigheterna.

Åtgärder inom ramen för den befintliga beslutsordningen

Vi har också övervägt vissa åtgärder som skulle kunna vidtas inom ramen för den befintliga beslutsordningen och som skulle kunna bidra till att förstärka kontrollen över tillämpningen. Bland annat har vi övervägt om möjligheten att delegera beslutsbefogenhet inom den beslutande myndigheten kan skärpas. Vi har dock funnit att den nuvarande delegationsbestämmelsen har en så strikt utformning som man rimligen kan begära. Vi föreslår därför inte några ändringar av den.

Inom både Polismyndigheten och Tullverket finns numera centralt placerade enheter som har ett övergripande ansvar för att skapa en-

hetliga riktlinjer för handläggningen av ärenden enligt inhämtningslagen och följa upp hur denna verksamhet hanteras inom respektive myndighet. Vi bedömer att detta med stor sannolikhet kommer att bidra till att höja och garantera kvaliteten i beslutsprocessen hos myndigheterna. Vidare arbetar såväl Polismyndigheten som Tullverket f.n. med att utarbeta nya system för delegation av beslutsbeslutsbefogenhet enligt lagen. Vi anser oss kunna utgå från att myndigheterna i det arbetet kommer att se till att besluten fattas på en tillräckligt hög nivå för att garantera en beslutsordning som uppfyller höga krav på kompetens och rättssäkerhet.

Vidare har vi övervägt om det skulle vara möjligt att vidta någon eller några åtgärder för att förbättra förutsättningarna för SIN:s tillsynsverksamhet. Vi har då kommit fram till att det bör föreskrivas att myndigheternas skyldighet att underrätta nämnden om beslut som fattats enligt inhämtningslagen bör fullgöras genom att myndigheten ger in själva beslutet till nämnden. Däremot bedömer vi att det inte vore lämpligt att förändra kraven på vilka uppgifter besluten ska innehålla. Vi bedömer också att det inte är nödvändigt att förändra kraven på dokumentation i ärenden enligt inhämtningslagen. Anledningen till det är att det har kommit fram att skälen för inhämtningsbesluten i regel finns dokumenterade i ärendena och att de således är tillgängliga för SIN.

Slutligen har vi också övervägt om det finns anledning att öka möjligheterna för teleoperatörerna att lämna uppgifter till SIN angående verkställigheten av beslut enligt inhämtningslagen. Vi bedömer dock att en sådan möjlighet inte skulle leda till någon förbättring av förutsättningarna för SIN:s tillsyn.

Säkerhetspolisens behov av en särskild möjlighet att inhämta uppgifter om viss brottslig verksamhet

Enligt inhämtningslagens huvudregel får uppgifter hämtas in, om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Enligt en särskild tidsbegränsad bestämmelse får uppgifter hämtas in också om brottslig verksamhet som innefattar vissa brott med lägre straffminimum än fängelse i två år (3 §). De brott som omfattas av bestämmelsen utgör sådan samhällsfarlig brottslighet

som bekämpas av Säkerhetspolisen. En del av vårt uppdrag har varit att analysera Säkerhetspolisens behov av en sådan möjlighet och att lämna förslag på hur detta behov bör tillgodoses och balanseras mot integritetsintresset.

Genom vår kartläggning har det kommit fram att tillämpningen av inhämtningslagen har lett till beaktansvärd nytta i samband med underrättelsearbete avseende brottslig verksamhet som innefattar flera av de brott som i dagsläget omfattas av bestämmelsen. Vi bedömer därför att möjligheten att hämta in uppgifter om brottslig verksamhet som innefattar dessa brott bör finnas kvar och att den i fortsättningen bör gälla permanent.

Vidare har det kommit fram att Säkerhetspolisen har ett stort behov av att kunna hämta in uppgifter om brottslig verksamhet som innefattar s.k. statsstyrt företagsspioneri samt grov misshandel och olaga frihetsberövande som begås 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 (s.k. systemhotande brottslighet). Vi föreslår därför att möjligheten att hämta in uppgifter ska omfatta även dessa brott.

Summary

Our remit

The Electronic Communications Act contains provisions stating that suppliers of publicly available electronic communications services are to retain certain data generated or processed in connection with providing such services so that these data can be used for law enforcement purposes. Our remit has been to propose the changes deemed appropriate to strengthen the protection of privacy with respect to these regulations.

The Data Collection Act regulates the powers of the Police Authority, the Swedish Security Service and the Swedish Customs to access such information. The Inquiry has had instructions to survey and evaluate the application of the Act in practice and to consider whether it should be changed. Another purpose of our remit has been to analyse the Swedish Security Service's need for special powers to collect data about some forms of criminal activity that are not covered by the general rule in the Data Collection Act and to present proposals on how such a need should be met and the balance to be struck with the interests of privacy.

Background

Protection of private life etc.

In the background section of the report, we describe the rules on the protection of individuals' private lives contained in the Swedish Instrument of Government, the European Convention for the Protection of Human Rights and Fundamental Freedoms and the EU Charter of Fundamental Rights. This section also discusses certain provisions on the protection of individuals' personal data.

In addition, it describes the activities of the various law enforcement authorities and the provisions regulating these authorities' powers to demand access to certain information about electronic communications that they need in their activities.

Data retention

The Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC) aimed to harmonise EU Member States' regulations on the obligations of suppliers of publicly available electronic communications services or of public communications networks to retain certain data about electronic communications to ensure that the data is available for detecting, investigating and prosecuting serious crime. The provisions implementing the Directive in Swedish law are contained in the Electronic Communications Act.

On 8 April 2014 the Court of Justice of the European Union delivered its judgment in joined cases C 293/12 and C 594/12, Digital Rights Ireland et al., concerning the validity of the Data Retention Directive. In its judgment, the Court declared the Directive invalid. The Court noted that the Directive entailed a wide-ranging and particularly serious interference in the right to respect for private life and the protection of personal data. However, the Court found that an obligation to retain data is an effective measure for achieving the purpose of fighting serious crime and maintaining public safety. Nonetheless, since the Directive did not lay down clear and precise rules governing the scope of the interference in the rights at issue, the Court considered that the interference was not limited to what was strictly necessary to achieve its purpose. In its judgment, the Court identified certain circumstances to which particular attention was paid in assessing whether the Directive satisfied the requirements of proportionality. On balance, the Court found that the legislative assemblies of the European Union had exceeded their authority when the Directive was adopted, since it does not satisfy the principle of proportionality with regard to the rights concerned.

Which categories of data should be retained?

The obligation to retain data is regulated in Swedish law by provisions in the Electronic Communications Act and Ordinance. These provisions require suppliers of electronic communications networks and communications services to retain certain data concerning telephone calls, internet traffic, message processing and other matters. The obligation applies for six months calculated from the date on which the communications concluded.

The obligation to retain this data is a measure that infringes on rights that are guaranteed to individuals in accordance with the Instrument of Government, the European Convention for the Protection of Human Rights and Fundamental Freedoms and the EU Charter of Fundamental Rights. For such a measure to be acceptable, it must be objectively appropriate for achieving the measure's purpose and it must be proportionate.

It is evident from information obtained from the police that all the categories of data retained under current rules are of great importance for law enforcement activities. Our assessment is therefore that the data retention obligation does not cover anything other than what is strictly necessary to achieve the purpose of the regulations. Consequently, no changes should be made in the categories of data that are to be retained.

Requirement for retention within the EU?

According to the Court of Justice, control by an independent authority is a fundamental component of the protection provided to individuals in connection with the processing of personal data. In the data retention judgment, the Court pointed out that one deficiency in the Data Retention Directive was that it could not be held that the Directive fully ensured the control by an independent authority of compliance with the requirements of protection and security. According to the Court, this was a consequence of the fact that the Directive did not require the data to be retained within the European Union.

Against this backdrop, we considered whether a prohibition should be introduced against data that is retained under Swedish rules being transferred to a third country for storage there. However, we

found that the way in which the Swedish regulations are designed enables the supervisory authority, the Swedish Post and Telecom Authority, to conduct active and effective supervision even of suppliers that choose to store data outside the EU. We have also taken into consideration that personal data may only be transferred to a third country if the country concerned ensures an adequate level of protection for the data. The adequate protection requirement means, among other things, that the third country must have established control mechanisms that monitor compliance with the country's rules on protection of personal data. Our assessment is therefore that control by an independent authority is guaranteed in Swedish law even with regard to suppliers that might choose to store data outside the EU. Moreover, we have found that a requirement in national law for retention within the EU or the EEA is incompatible with other EU regulations in the area and with Sweden's commitments under the Data Protection Convention.

Against this backdrop, our assessment is that no general prohibition should be introduced against data that is retained under Swedish data retention rules being transferred to a third country for storage there.

Collection of subscription data

One of the deficiencies in the Data Retention Directive that the Court of Justice pointed out in its judgment was that the Directive did not give any objective criteria for limiting the access of the national authorities to the retained data or their use of that data. The Court also noted that the Directive did not require that access to data was made dependent on a prior review carried out by a court or by an independent body tasked with ensuring that access is limited to what is strictly necessary.

Subscription data retained under the Swedish data retention rules may be released to law enforcement authorities without any requirement that the crime for which the data are released is of any particular degree of severity. Moreover, data may be collected following a decision of the law enforcement authority, without prior control by an independent body.

Against this backdrop, we have considered several different measures that could contribute to strengthening controls over the application by the law enforcement authorities of the rules on collecting subscription data. For example, we have considered whether a supervisory body ought to be instructed to exercise supervision specifically focused on the application of these rules. However, our assessment is that the disadvantages of such a system outweigh the advantages. On the other hand, we propose that the authority to make decisions on collecting subscription data should be limited to certain specially designated officials at the authority requesting the data. In addition, we propose that decisions on collecting such data should be documented in a certain manner. The Inquiry considers that these measures could contribute to higher quality in the decision-making process and to more effective supervision by the Parliamentary Ombudsmen, the Chancellor of Justice, the Data Inspection Board and the Swedish Commission on Security and Integrity Protection. We also present proposals on certain clarifications in the provision on collecting subscription data. The purpose of this will be to make it clear that the provision can be applied in the law enforcement authorities' intelligence activities.

Information covered by professional confidentiality

In its judgment, the Court of Justice underlined that one of the deficiencies of the Data Retention Directive was that it did not contain any exceptions to the data retention requirement, which meant that it applied even to persons whose communications are subject to confidentiality under national law.

We have therefore considered whether a prohibition should be introduced against collecting data concerning communications with persons subject to professional confidentiality. However, in Swedish law it is normally the contents of the data that determine whether it is subject to confidentiality. When collecting metadata, the authority collecting the data normally has no knowledge of the contents of the communications. Our assessment is therefore that a prohibition of this kind would be very difficult to apply. Moreover, in our view, it would have very little practical significance. This is because the principle of proportionality normally prevents data being collected

if the authorities, by way of exception, should be aware in advance that the communications are subject to confidentiality. On the other hand, we propose the introduction of rules requiring the data concerning such communications to be destroyed in cases where the authorities later learn that the communications are subject to such confidentiality.

Data Collection Act

Survey

Part of our remit was to survey the application of the Data Collection Act until now. The method that we chose to investigate this issue was an in-depth examination of a sample of intelligence cases in which the Data Collection Act had been applied by the Police Authority, the Swedish Security Service or Swedish Customs. In connection with the investigation, in each of the cases selected, the Inquiry studied the decision taken in the cases under the Data Collection Act and background written material. After that, a representative of the Inquiry interviewed the case officer responsible for the case. The purpose was to gain an in-depth understanding of the issues of benefit, need and interference in privacy.

The results of the survey are presented in detail in the report and were an important part of the material on which we based our analysis, assessments and proposals concerning the Data Collection Act. We found that the way in which the law enforcement authorities process cases under the Data Collection Act is essentially satisfactory. We also found that the Act is an important tool in the authorities' intelligence activities. In the vast majority of cases, the Act is applied so as to give the authorities access to relevant information that helps to advance the intelligence cases. There are therefore grounds for concluding that the Act is of considerable benefit for intelligence activities. However, it also leads to interference in the privacy of both the individuals concerned in the cases and those with whom they have been in contact.

Decision-making procedure in the Data Collection Act

The Court of Justice pointed out in the data retention judgment that the Directive did not prescribe that the access of the competent national authorities to retained data should be subject to prior review carried out by a court or an independent authority. Therefore, and in accordance with our terms of reference, we have considered whether a general court should be entrusted with taking decisions on collecting data. However, we have found that matters concerning the collection of data in intelligence activities are not particularly well-suited for review by a general court. The purpose of intelligence activities, which are separate from and precede a preliminary investigation, is to obtain material for processing and analysis through a broad collection of information and knowledge. The basic purpose of intelligence activities is to study and identify potential criminal activities in order to prevent the crime from being carried out. These activities are often part of a more wide-ranging approach. Since the activities, unlike a preliminary investigation, do not focus on any specific criminal act – and often not on any specifically identified person either – the interest of the parties does not play the same kind of role in intelligence activities as in a preliminary investigation. Consequently, in the intelligence phase the privacy aspect is characterised more by the perspective of citizens' interests than by the type of two party procedure that is well-suited for review by a general court. There is also reason to doubt whether the courts would be able to satisfy the need for speedy decisions.

We have also considered whether the decision-making powers under the Data Collection Act should be entrusted to a prosecutor or a new decision-making body, such as a special board. These options have the same weaknesses as a court review. There are also other disadvantages. In our assessment, for example, giving prosecutors the task of taking decisions to order collection of data would be difficult to reconcile with the role prosecutors have in the criminal law system. Given that the current decision-making procedure works well, our assessment is therefore that decisions under the Data Collection Act should be taken by the law enforcement authorities.

Measures within the framework of existing decision-making procedures

We have also considered certain measures that could be taken within the framework of existing decision-making procedures and that could contribute to strengthening controls over the application of these procedures. Among other things, we have considered whether it is possible to tighten up the possibility of delegating decision-making powers within the decision-making authority. However, we have found that the current provision on delegation is formulated as strictly as can reasonably be demanded. We therefore do not propose any changes in this provision.

Both the Police Authority and Swedish Customs now have centrally placed units that have a broad responsibility for creating standard guidelines for processing cases under the Data Collection Act and following up how these activities are managed within the authority. We consider that this is highly likely to help raise and guarantee the quality of the decision making process at these authorities. Furthermore, both the Police Authority and the Swedish Customs are now developing new systems for delegating decision-making powers under the Act. We believe we can assume that in this process, the authorities will ensure that decisions are taken at a sufficiently high level to guarantee a decision-making procedure that meets high standards of competence and legal certainty.

We have also considered whether it would be possible to take any measure or measures to improve the conditions for supervision by the Swedish Commission on Security and Integrity Protection. Our conclusion is that it should be prescribed that the authorities' obligation to inform the Commission of decisions taken under the Data Collection Act should be met by the authority concerned submitting the actual decision to the Commission. On the other hand, we do not consider it would be appropriate to change the requirements concerning the information the decisions must contain. We also do not consider it necessary to change the requirements concerning documentation in cases under the Data Collection Act. The reason for this is that it has emerged that the grounds for data collection decisions are generally documented in the cases and are therefore available to the Commission.

Finally, we have also considered whether there is reason to increase the possibilities for telecommunications operators to provide information to the Commission concerning the enforcement of decisions under the Data Collection Act. However, in our assessment, such a possibility would not lead to any improvement in the conditions for supervision by the Commission.

The need of the Swedish Security Service for special powers to collect information about certain criminal activities

According to the general rule in the Data Collection Act, data may be collected if the circumstances are such that the measure is of particular importance for preventing or detecting criminal activities that include crimes for which the law does not envisage a more lenient sentence than imprisonment for two years. The Act also contains a special time-limited provision allowing data to be collected concerning criminal activities that include certain crimes with lower minimum sentences than imprisonment for two years (Section 3). The crimes covered by this provision are the types of criminal activity that pose a threat to society and that are targeted by the Swedish Security Service. Part of our remit has been to analyse the extent to which the Swedish Security Service needs such an option and to present proposals on how this need should be met while striking a balance with the interests of privacy.

It has emerged from our review that the way in which the Data Collection Act has been applied has led to considerable benefits in connection with intelligence activities relating to criminal activities that include several of the crimes that are now covered by this section of the law. In our opinion, the possibility of collecting data concerning criminal activities that include these crimes should therefore be retained and should have permanent application in the future.

Moreover, it has emerged that the Swedish Security Service has a great need to be able to collect data concerning criminal activities that include state-sponsored industrial espionage and gross assault and unlawful deprivation of liberty committed with the intention of influencing public bodies or a person professionally engaged in news coverage or other journalism to take or refrain from taking a measure or to take revenge for a measure ('system-threatening

crime'). We therefore propose that the possibility of collecting data should also extend to these crimes.

1 Författningsförslag

1.1 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att 27 kap. 22 § rättegångsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

27 kap.

22 §[1]

Hemlig avlyssning av elektronisk kommunikation får inte avse telefonsamtal eller andra meddelanden där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram. Om det under avlyssningen kommer fram att det är fråga om ett sådant samtal eller meddelande, ska avlyssningen omedelbart avbrytas.

Hemlig rumsavlyssning får inte avse samtal eller annat tal där någon som angetts i första stycket talar. Om det under rumsavlyssningen kommer fram att det är fråga om ett sådant samtal eller tal, ska avlyssningen omedelbart avbrytas.

Upptagningar och uppteckningar ska omedelbart förstöras i de delar som de omfattas av förbud enligt första eller andra stycket.

Uppteckningar från hemlig övervakning av elektronisk kommunikation ska omedelbart förstöras i de delar innehållet avser uppgifter som, på grund av be-

[1] Senaste lydelse 2014:1419.

stämmelserna i 36 kap. 5 § andra–sjätte styckena, inte skulle ha kunnat inhämtas genom vittnesförhör i domstol.

Denna lag träder i kraft den 1 juli 2016.

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

Härigenom föreskrivs att 6 kap. 22 § lagen (2003:389) om elektronisk kommunikation ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
22 §[2]	
Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket ska på begäran lämna	
1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (2010:1932), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,	
2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet,	2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott *eller brottslig verksamhet* till en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet *eller den brottsliga verksamheten*,
3. uppgift som avses i 20 § första stycket 1 och 3 samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits till Polismyndigheten, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det finns fara för deras liv eller allvarlig risk för deras hälsa,	

[2] Senaste lydelse 2014:734.

4. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

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

6. uppgift som avses i 20 § första stycket 1 till Polismyndigheten, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

7. uppgift som avses i 20 § första stycket 1 till Polismyndigheten eller en åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och

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

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

Denna lag träder i kraft den 1 juli 2016.

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

Härigenom föreskrivs att 11 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

11 §[3]

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

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

Uppteckningar från hemlig övervakning av elektronisk kommunikation ska omedelbart förstöras i de delar innehållet avser uppgifter som, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat inhämtas genom vittnesförhör i domstol.

Denna lag träder i kraft den 1 juli 2016.

[3] Senaste lydelse 2012:286.

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

Härigenom föreskrivs att 44 kap. 4 § offentlighets- och sekretesslagen (2009:400) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	44 kap.
	4 §[4]
Rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer av	
1. 2 kap. 14 § första stycket 1 *och* 3 postlagen (2010:1045),	1. 2 kap. 14 § första stycket 1, 3 *och 4* postlagen (2010:1045),
2. 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation, när det är fråga om uppgift om innehållet i ett elektroniskt meddelande eller som annars rör ett särskilt sådant meddelande, och	
3. 6 kap. 21 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på grund av beslut av domstol, undersökningsledare eller åklagare eller om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.	

Denna lag träder i kraft den 1 juli 2016.

[4] Senaste lydelse 2012:288.

1.5 Förslag till lag om ändring i postlagen (2010:1045)

Härigenom föreskrivs att 2 kap. 14 § postlagen (2010:1045) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
2 kap.	
14 §	
Den som i postverksamhet har fått del av eller tillgång till någon av de uppgifter som anges i 1–*3* får inte obehörigen röja eller utnyttja vad han eller hon därigenom har fått veta. De uppgifter som omfattas av tystnadsplikten är	Den som i postverksamhet har fått del av eller tillgång till någon av de uppgifter som anges i 1–*4* får inte obehörigen röja eller utnyttja vad han eller hon därigenom har fått veta. De uppgifter som omfattas av tystnadsplikten är
1. uppgifter som rör ett särskilt brev som befordras inom verksamheten,	
2. andra uppgifter som rör en enskild persons förbindelse med verksamheten när det gäller befordran av brev, *eller*	2. andra uppgifter som rör en enskild persons förbindelse med verksamheten när det gäller befordran av brev,
3. uppgifter som handlar om att kvarhålla eller beslagta försändelser enligt 27 kap. rättegångsbalken.	3. uppgifter som handlar om att kvarhålla eller beslagta försändelser enligt 27 kap. rättegångsbalken, *eller*
	4. uppgifter som handlar om att undersöka, öppna, granska eller kvarhålla försändelser enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Tystnadsplikten enligt första stycket 1 och 2 gäller inte i förhållande till avsändaren och mottagaren av brevet.

För uppgifter om en enskild persons adress gäller tystnadsplikt endast om det kan antas att ett röjande av adressen skulle medföra fara för att någon utsätts för övergrepp eller annat allvarligt men.

Denna lag träder i kraft den 1 juli 2016.

1.6 Förslag till lag om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Härigenom föreskrivs i fråga om lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

dels att nuvarande 4–9 §§ ska betecknas 3–8 §§,

dels att 2, 5 och 8 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 §
Uppgifter får hämtas in om omständigheterna är sådana att	Uppgifter får hämtas in om omständigheterna är sådana att *åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar*
1. *åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar* brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, *och*	1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. *skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.*	*2. sabotage enligt 13 kap. 4 § brottsbalken,*
	3. kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,

4. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,

5. spioneri, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5 eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,

6. företagsspioneri enligt 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understödjs av en främmande makt eller av någon som agerar för en främmande makts räkning,

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

8. grov misshandel eller olaga frihetsberövande enligt 3 kap. 6 § eller 4 kap. 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.

Uppgifter får hämtas in bara om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

5 §

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

Säkerhets- och integritetsskyddsnämnden ska underrättas om ett beslut om inhämtning av uppgifter enligt denna lag. *Underrättelseskyldigheten ska fullgöras genom att beslutet* lämnas *till nämnden* senast en månad efter det att ärendet om inhämtning avslutades.

8 §

Uppteckningar av uppgifter ska granskas snarast möjligt.

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

Uppteckningar ska dock omedelbart förstöras i de delar innehållet avser uppgifter som, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat inhämtas genom vittnesförhör i domstol.

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

---

1. Denna lag träder i kraft den 1 juli 2016.

2. Genom lagen upphävs lagen (2012:279) om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

1.7 Förslag till förordning om ändring i förordningen (2003:396) om elektronisk kommunikation

Härigenom föreskrivs att det i förordningen (2003:396) om elektronisk kommunikation ska införas en ny paragraf, 36 b §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	36 b §
	Beslut om inhämtning av uppgifter enligt 6 kap. 22 § första stycket 2 lagen (2003:389) om elektronisk kommunikation fattas av den myndighet som ska ingripa mot brottet eller den brottsliga verksamheten. Myndighetschefen får delegera rätten att fatta beslut om inhämtning till annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Ett beslut om att delegera beslutsbefogenhet ska dokumenteras av myndigheten.
	Även utan särskild delegation enligt första stycket får förundersökningsledaren fatta beslut om sådan inhämtning av uppgifter som sker inom ramen för en förundersökning.
	I ett beslut om inhämtning av uppgifter enligt 6 kap. 22 § första stycket 2 lagen (2003:389) om elektronisk kommunikation ska det anges vem som har fattat beslutet samt vilket brott eller vilken brottslig verksamhet och vilka

abonnemangsuppgifter beslutet avser. Skälen för beslutet ska också anges.

Denna förordning träder i kraft den 1 juli 2016.

2 Utredningens uppdrag och arbete

2.1 Vårt uppdrag

Regeringen beslutade den 26 juni 2014 att ge en särskild utredare i uppdrag att utvärdera lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Enligt utredningens direktiv ska vi bl.a. kartlägga tillämpningen av lagen och analysera vilken nytta den har lett till i den brottsbekämpande verksamheten och vilken inverkan lagen har haft på enskildas personliga integritet. Med utgångspunkt i kartläggningen och analysen ska vi överväga om de rättssäkerhetsåtgärder och integritetsstärkande åtgärder som vidtogs när lagen infördes har varit tillräckliga eller om det finns behov av andra sådana åtgärder. Vi ska också analysera Säkerhetspolisens behov av en möjlighet enligt inhämtningslagen att hämta in uppgifter i underrättelseverksamhet avseende brottslig verksamhet som innefattar vissa samhällsfarliga brott och lämna förslag på hur detta behov bör tillgodoses och balanseras mot integritetsintresset. Slutligen ska vi också föreslå de förändringar som bedöms lämpliga för att stärka skyddet för den personliga integriteten i förhållande till reglerna om lagring av uppgifter enligt vissa bestämmelser i lagen om elektronisk kommunikation.

2.2 Utredningsarbetet

Utredaren har haft såväl möten som mer informella kontakter med experterna.

Vi har också samrått med företrädare för Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritets-

skyddsnämnden, Tullverket samt Post- och Telestyrelsen. Vidare har utredningen hållit ett möte med företrädare för leverantörer av elektroniska kommunikationstjänster.

För att kartlägga tillämpningen av inhämtningslagen har – vid sidan av de kontakter som nämnts ovan – uppgifter hämtats in från Polismyndigheten, Säkerhetspolisen och Tullverket i enskilda fall. Detta har skett genom att företrädare för utredningen har gått igenom handlingar i underrättelseärenden på plats hos myndigheterna samt intervjuat ett stort antal handläggare.

Utredningens kartläggning har genomförts i nära samarbete med Brottsförebyggande rådet. Sålunda har en forskare från Brå (tillika expert i utredningen) svarat för att gå igenom och hålla intervjuer i de ärenden som handlagts av Säkerhetspolisen. Samme forskare har även författat det avsnitt i betänkandet där kartläggningen av Säkerhetspolisens tillämpning redovisas. Vad avser Polismyndighetens och Tullverkets ärenden har motsvarande arbete utförts av en utredare från Brå (tillika expert i utredningen) tillsammans med utredningens sekreterare.

2.3 Betänkandets disposition

Betänkandet består, förutom av detta avsnitt och utredningens författningsförslag, av tio avsnitt. I avsnitt 3 beskrivs översiktligt de regler som gäller för skyddet för privatlivet och avseende personuppgiftsbehandling. Vidare innehåller avsnittet beskrivningar av de brottsbekämpande myndigheternas verksamhet och av de regler som gäller för inhämtning av uppgifter om elektronisk kommunikation i sådan verksamhet. Därefter följer i avsnitt 4 en beskrivning av det s.k. datalagringsdirektivet och den dom från april 2014 genom vilken EU-domstolen ogiltigförklarade direktivet. Avsnittet innehåller också en beskrivning av den analys av svensk rätts förhållande till EU-rätten som gjordes efter att domen meddelades (Ds 2014:23).

I avsnitt 5 gör vi vissa överväganden i fråga om vilka kategorier av uppgifter som bör lagras enligt de svenska reglerna. Nästa avsnitt, avsnitt 6, innehåller överväganden i fråga om det bör införas ett förbud mot att datalagrade uppgifter förs över till ett land utanför EU för lagring.

Avsnitt 7 innehåller överväganden och förslag i fråga om hur kontrollsystemet när det gäller inhämtning av uppgifter om abonnemang bör vara utformat. I avsnitt 8 finns vissa överväganden och förslag i fråga om skyddet för uppgifter som omfattas av yrkesmässig tystnadsplikt. Därefter följer i avsnitt 9 en redovisning av vad som kommit fram genom vår kartläggning av inhämtningslagen samt våra överväganden och förslag vad gäller den lagen.

I avsnitt 10 tar vi upp några övriga frågor som kommit upp under vårt arbete. Därefter behandlar vi i avsnitt 11 frågor om genomförande och konsekvenser, och i det avlutande avsnitt 12 finns kommentarer till författningsförslagen.

3 Bakgrund

3.1 Rätten till personlig integritet

3.1.1 Integritetsbegreppet

Det finns i svensk rätt inte någon allmängiltig definition av begreppet personlig integritet. Olika utredningar (se t.ex. Tvångsmedelskommitténs betänkande Tvångsmedel – Anonymitet – Integritet, SOU 1984:54 s. 42) har med utgångspunkt i bl.a. de grundläggande fri- och rättigheterna i regeringsformens andra kapitel försökt klargöra begreppet genom att skilja mellan den rumsliga integriteten (hemfriden), den materiella integriteten (egendomsskyddet), den kroppsliga integriteten (skydd för liv och hälsa samt mot ingrepp i eller mot kroppen), den personliga integriteten i fysisk mening (skyddet för den personliga friheten och rörelsefriheten) och den personliga integriteten i ideell mening (skyddet för privatlivet och för personligheten inklusive den privata ekonomin). Ett annat sätt att bestämma begreppet personlig integritet är att ange vilka handlingar som utgör kränkningar av densamma. Enligt denna modell kan kränkningarna delas in i tre huvudgrupper: 1) intrång i en persons privata sfär i fysisk eller annan mening; 2) insamlande av uppgifter om en persons privata förhållanden; 3) offentliggörande eller annan användning (t.ex. som bevisning i rättegång) av uppgifter om en persons privata förhållanden (se prop. 2006/07:63 s. 61).

Utformningen av integritetsskyddet i svensk rätt synes inte i praktiken ha tagit sin utgångspunkt i en viss definition av begreppet, utan skyddet har i stället kommit att bestämmas av summan av ett stort antal skyddsregler av varierande slag (se SOU 2007:22 s. 52). I förarbetena till regeringsformen (RF) och personuppgiftslagen (1998:205) har lagstiftaren dock försökt att beskriva kärnan i vad som avses skyddas av lagstiftningen genom att slå fast att kränkningar av den personliga integriteten utgör intrång i den fredade sfär

som enskilde bör vara tillförsäkrad och där ett oönskat ingrepp bör kunna avvisas (prop. 2005/06:173 s. 15 och prop. 2009/10:80 s. 175). Denna beskrivning ligger också väl i linje med den definition av begreppet som ges i t.ex. Nationalencyklopedins ordbok; rätten att ha ett visst eget område som är skyddat mot intrång.

3.1.2 Skyddsintressen

Det är viktigt i en rättsstat att den offentliga maktutövningen är bunden av förutsebara normer och underkastad vissa begränsningar. Detta gäller inte minst de metoder som används i statens brottsbekämpande verksamhet. Den som är misstänkt för ett brott har rätt att ställa krav på att staten respekterar hans eller hennes berättigade krav på respekt för de grundläggande fri- och rättigheterna samt skydd mot godtycke.

Samtidigt har var och en som vistas i Sverige även rätt att göra anspråk på att staten vidtar effektiva åtgärder för att skydda hans eller hennes säkerhet. I detta ligger bl.a. att staten måste anstränga sig för att se till att brott förebyggs och utreds och att gärningsmän ställs till svars för sina brottsliga handlingar. Staten har alltså ett ansvar för att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda. Till exempel innebär artikel 8 i Europakonventionen inte bara ett skydd mot ingrepp i privatlivet från statens sida, utan ålägger också staten att vidta positiva åtgärder för att skydda den enskildes privatsfär. Även utan att det förekommit något ingripande från en myndighet eller en offentlig tjänsteman kan staten således bryta mot artikel 8 genom att tolerera en existerande situation eller genom att inte skapa tillräckligt rättsligt skydd. Staten kan då bli ansvarig för sin underlåtenhet trots att det specifika övergrepp som visat att det rättsliga skyddet var otillräckligt har utförts av en enskild person, för vars handlande staten inte i och för sig är ansvarig. Vad som i huvudsak kan förväntas är att staten utfärdar lagar som ger ett tillfredsställande skydd åt privatliv, familjeliv, hem och korrespondens och att de rättsvårdande myndigheterna håller kontroll över att dessa lagar respekteras.[1] En förutsättning för att staten ska kunna leva

[1] Danelius, Hans, Mänskliga rättigheter i Europeisk praxis, Norstedts Juridik, 4 uppl. 2012, s. 347.

upp till kraven på att upprätthålla rättstryggheten för enskilda är att staten har en välfungerande och effektiv brottsbekämpning.

3.1.3 Regleringen av skyddet för privatlivet

3.1.3.1 Grundläggande bestämmelser

Grundläggande bestämmelser som har betydelse för det allmännas ansvar att skydda enskildas privatliv och integritet finns i bl.a. regeringsformen (RF). Av målsättningsstadgandet i 1 kap. 2 § framgår att den offentliga makten ska utövas med respekt för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv. Enligt 2 kap. 6 § första stycket RF gäller vidare att var och en gentemot det allmänna är skyddad mot undersökning av förtroliga brev och andra förtroliga försändelser samt mot hemlig avlyssning eller upptagning av telefonsamtal eller andra förtroliga meddelanden. 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.

Europakonventionen och konventionens samtliga ändrings- och tilläggsprotokoll utom ändringsprotokoll 15 och tilläggsprotokoll 12 och 16 har ratificerats av Sverige. Konventionen, med de ändringar och tillägg som gjorts genom dessa protokoll, gäller sedan den 1 januari 1995 som svensk lag (lagen [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna). Av 2 kap. 19 § RF följer att lag eller annan författning inte får meddelas i strid med Sveriges åtaganden enligt konventionen. Detta innebär att en föreskrift som står i strid med konventionen i princip också kommer i konflikt med grundlagen.

Av artikel 8 i Europakonventionen följer att var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Begreppet privatliv tolkas i Europadomstolens praxis vitt. Domstolen har flera gånger framhållit att det inte är möjligt att definiera begreppet genom en uttömmande beskrivning av olika aspekter som rör den enskildes privata förhållanden (se t.ex. *S. och Marper mot Förenade kungariket* [GC], nr 30562/04, § 66 och *Gillberg mot Sverige* [GC], nr 41723/06, § 66). Begreppet täcker

olika aspekter av en enskild individs såväl fysiska som psykiska integritet. Det omfattar bl.a. uppgifter om den enskildes identitet, inklusive namn och kön, uppgifter om hälsa och sexuell läggning och information som rör den personliga utvecklingen och relationer till andra individer. Respekten för privatlivet omfattar inte enbart skydd av rent privata relationer utan kan även omfatta relationer och aktiviteter som är relaterade till den enskildes yrkesliv (se t.ex. *Rotaru mot Rumänien* [GC], nr 28341/95, § 43). Till privatlivet hör vidare en rätt till skydd mot angrepp av den enskildes ära och ryktbarhet och mot spridning av information som rör privata förhållanden (se t.ex. *K.U. mot Finland*, nr 2872/02, §§ 42 och 43, och *von Hannover mot Tyskland*, nr 59320/00, § 50). Vidare omfattar rätten till respekt för privatlivet ett skydd mot registrering och utlämnande av uppgifter ur allmänna register (se t.ex. *Leander mot Sverige*, nr 9248/81, § 48 och *Segerstedt-Wiberg m.fl. mot Sverige*, nr 62332/00, § 72).

En bestämmelse om rätt till respekt för bl.a. privatlivet finns också i artikel 7 Europeiska unionens stadga om de grundläggande rättigheterna av den 7 december 2000, anpassad den 12 december 2007 i Strasbourg (rättighetsstadgan). Av artikel 52.3 i stadgan följer att i den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen ska de ha samma innebörd och räckvidd som enligt konventionen. Rättighetsstadgan riktar sig till medlemsstaterna endast när de tillämpar unionsrätten (artikel 51.1). Av EU-domstolens praxis framgår att detta innebär att rättigheterna i stadgan måste iakttas inte bara vid tillämpningen av nationell lagstiftning som genomför EU-rätt, utan så snart nationell lagstiftning omfattas av unionens tillämpningsområde (se t.ex. *Åkerberg Fransson*, C-617-10, punkt 21).

Frågor om skydd för privatlivet tilldrar sig stort intresse runt om i världen. Detta gäller inte minst i förhållande till frågor om övervakning av elektronisk kommunikation. Exempelvis har ett stort antal organisationer som arbetar för integritetsfrågor tillsammans arbetat fram ett antal principer som stater uppmanas att följa vid sådan övervakning.[2] Dessa principer innehåller bl.a. uppmaningar om att övervakningsåtgärder ska regleras i lag och endast vara tillåtna när det är nödvändigt, lämpligt och proportionerligt i förhållande till ett legitimt ändamål. Vidare ska åtgärderna beslutas av en behörig

[2] Principerna finns att läsa på https://en.necessaryandproportionate.org/

rättslig myndighet. Den som utsätts för åtgärderna ska underrättas om dem. Staterna ska också inrätta kontrollmekanismer som ska säkerställa transparens och ansvar för åtgärderna.

3.1.3.2 Inskränkningar i skyddet får göras

Rätten till skydd av privatlivet och den personliga integriteten är inte absolut. En individ som lever i ett samhälle och sålunda ingår i en gemenskap med andra människor kan inte göra gällande något absolut anspråk på att i alla situationer få leva i fred för andra individer eller ostört av samhällets organ. I syfte att tillförsäkra medborgarna ökad trygghet och säkerhet mot yttre och inre hot kan det i bland vara nödvändigt med vissa inskränkningar av integritetsskyddet. Regler som syftar till att skydda den enskildes personliga integritet måste sålunda förses med olika, i skilda situationer mer eller mindre vittgående undantag eller på annat sätt begränsas till sin giltighet, så att andra människors och samhällets intressen i övrigt inte träds för när.

Det är en svår uppgift att avväga integritetsintresset mot nödvändigheten av att se till att myndigheterna har effektiva metoder till sin hjälp för att bedriva den verksamhet de är skyldiga att utföra. En viktig utgångspunkt är att myndigheterna inte får ges sådana befogenheter att medborgarnas tilltro till dem påverkas negativt. Förtroendet kan skadas om medborgarna upplever att det finns risk för att myndigheterna utan deras vetskap samlar information om enskilda och deras privatliv utan att detta motiveras av tungt vägande allmänna intressen. Medborgarnas bild av det allmännas verksamhet påverkas dock också av i vilken utsträckning myndigheterna ges förutsättningar att använda effektiva arbetsmetoder. Myndigheterna är samhällsorgan som ytterst har till uppgift att värna medborgarna. Om medborgarna upplever att myndigheterna inte har förmåga eller tillräckliga medel för att hantera hot mot samhället och enskilda kan även detta leda till minskat förtroende.

Enligt 2 kap. 20 § RF får det integritetsskydd som följer av regeringsformen endast begränsas genom lag. En begränsning får göras endast för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle. En begränsning får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och får inte heller sträcka sig så långt att den utgör ett hot mot den fria

åsiktsbildningen såsom en av folkstyrelsens grundvalar (2 kap. 21 § RF). En begränsning måste alltså vara proportionerlig.

På liknande sätt får rättigheter enligt artikel 8 i Europakonventionen inskränkas endast genom lag. Kravet på lagstöd är inte endast formellt. Det krävs även att den rättighetsbegränsande lagen uppfyller rimliga anspråk på rättssäkerhet och skydd mot godtycke. Den måste vara tillgänglig för allmänheten, och den måste vara utformad med tillräcklig precision, så att inskränkningarna i den grundläggande konventionsrättigheten kan i rimlig utsträckning förutses. En nationell lag som ger de rättstillämpande organen ett tolkningsutrymme och en rätt till skönsmässig prövning är emellertid inte i och för sig oförenlig med kravet på förutsebarhet, under förutsättning att gränserna för den skönsmässiga bedömningen är tillräckligt klara för att ge individen skydd mot godtyckliga ingrepp.[3]

När det gäller dolda spaningsåtgärder innebär kravet på förutsebarhet visserligen inte att en person bör kunna veta på förhand t.ex. när myndigheterna sannolikt avlyssnar dennes samtal, så att han eller hon kan anpassa sitt beteende därefter. Lagstiftningen om sådana åtgärder måste däremot vara så tydlig att den ger medborgarna en tillräcklig indikation om vilka omständigheter som krävs för att myndigheterna ska få använda sig av åtgärderna. Europadomstolen har utarbetat en minimistandard som ställer följande krav på lagstiftning om dolda spaningsåtgärder (se t.ex. Europadomstolens dom den 2 september 2010 i målet Uzun mot Tyskland, p. 61 med hänvisningar):

- Arten av de brott som skulle kunna leda till en begäran om avlyssning måste framgå.
- Det ska finnas en definition av de personkategorier som skulle kunna riskera att t.ex. få sin telefon avlyssnad.
- Avlyssningens varaktighet ska vara begränsad.
- Det måste finnas förfaranderegler för undersökning, användning och lagring av de uppgifter som inhämtas.
- Försiktighetsåtgärder vid överföring av information till andra parter ska vidtas.

[3] Danelius, a.a. s. 351.

- De omständigheter under vilka inspelningarna kan eller måste raderas ska anges.

Det kan dock konstateras att den grad av förutsebarhet som krävs varierar beroende på vilken typ av spaningsåtgärd som lagstiftningen avser och hur ingripande åtgärden är. I det ovan nämnda målet Uzun mot Tyskland, vilket rörde övervakning via GPS av förflyttningar på offentliga platser, uttalade domstolen att de relativt strikta krav som minimistandarden ställer har utarbetats i mål om telefonavlyssning. Domstolen fann att dessa krav inte var tillämpliga i målet eftersom övervakning av en persons rörelser med hjälp av GPS-utrustning, i jämförelse med telefonavlyssning, utgjorde ett mindre intrång i dennes privatliv. En rimlig slutsats är att verksamhet och åtgärder som utgör större intrång i privatlivet borde tillhandahållas med tydligare bemyndiganden och bli föremål för fler restriktioner än verksamhet som utgör mindre sådana intrång.

Europadomstolen har också slagit fast att nationell lagstiftning om dolda spaningsåtgärder måste innehålla kontrollmekanismer för att skydda mot missbruk av den prövningsrätt som finns. Vad som krävs i det avseendet beror på omständigheter som åtgärdernas karaktär, räckvidd och varaktighet, vilka motiv som krävs för att besluta, utföra och övervaka dem samt vilken typ av rättsmedel som finns i den nationella lagstiftningen. Beträffande telefonavlyssning har Europadomstolen ansett att beslutet normalt sett ska kontrolleras av domstol, åtminstone i sista instans.[4] Den nationella lagstiftningen måste också, såvitt avser telefonavlyssning, innehålla tillfredsställande mekanismer för att övervaka vad som sker med överskottsinformation. När det gäller mindre ingripande åtgärder ställer konventionen däremot lägre krav. Som ett exempel på detta kan nämnas Europadomstolens dom den 25 september 2001 i målet *P.G. och J.H. mot Storbritannien*. I målet uttalade domstolen att vad som krävs i fråga om skyddsåtgärder beror, åtminstone i viss utsträckning, på det aktuella intrångets natur och omfattning. Domstolen fann att de brittiska reglerna om telefonövervakning innehöll tillräckliga garantier mot missbruk, trots att det saknades lagregler

[4] Frågan om det är förenligt med Europakonventionen att beslut om vissa former av avlyssning kan fattas av ett annat organ än domstol är f.n. föremål för Europadomstolens prövning i målen Máté SZABÓ och Beatrix VISSY mot Ungern (37138/14) och Roman ZAKHAROV mot Ryssland (47143/06)

(i motsats till interna riktlinjer för polisen) om lagring och förstörande av den information som samlades in.

Det kan sägas att domstolen i det aktuella målet satte en låg standard för ”med stöd av lag” eftersom det inte fanns något uttryckligt bemyndigande för hemlig övervakning av elektronisk kommunikation i det brittiska systemet. Uppfattningen har också framförts att det är mycket sannolikt att Europadomstolen i framtiden kommer att kräva någon form av system för efterföljande kontroll av hemlig övervakning av elektronisk kommunikation om och när den konfronteras med denna fråga igen.[5]

En inskränkning i rättigheter som skyddas av artikel 8 får vidare göras endast 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. Av Europadomstolens praxis följer att en inskränkning måste kunna motiveras av ett angeläget samhälleligt behov och den måste stå i rimlig proportion till det syfte som ska tillgodoses genom inskränkningen. Konventionsstaterna har visst utrymme – *margin of appreciation* – att själva avgöra om en inskränkning är nödvändig. Europadomstolen förbehåller sig dock rätten att övervaka om staternas avvägningar uppfyller konventionens krav på proportionalitet. Domstolens kontroll i detta avseende varierar beroende bl.a. på vilka ändamål som utgör grund för inskränkningen och är typiskt sett något mindre strikt när en stats vitala intressen motiverar en inskränkning eller när det saknas en enhetlig europeisk rättsuppfattning om hur en fråga ska bedömas.[6]

När det gäller unionsrätten följer av artikel 52.1 i rättighetsstadgan att varje begränsning i utövandet av de fri- och rättigheter som erkänns i stadgan måste vara föreskriven i lag och vara förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, göras endast om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter. Enligt EU-domstolens fasta praxis kräver proportionalitetsprincipen att unionsinstitutionernas

[5] Se Cameron, Expertrapport åt Polismetodutredningen, SOU 2010:103 s. 547 f.
[6] Danelius, a.a. s. 351.

åtgärder, för att vara godtagbara, för det första måste vara ägnade att uppnå de legitima mål som eftersträvas. För det andra får åtgärderna inte gå utöver vad som är lämpligt och nödvändigt för att uppnå de eftersträvade målen. Utrymmet för unionslagstiftaren att bedöma om proportionalitetsprincipens krav är uppfyllda kan begränsas på grund av omständigheter som t.ex. vilken rättighet som begränsas, hur omfattande och allvarlig ingreppet är, vilket syfte ingreppet har etc.[7] Ju mer långtgående ett ingrepp är, desto mer strikt blir EU-domstolens kontroll av att proportionalitetsprincipens krav följs.

3.2 Skyddet för personuppgifter

3.2.1 EU:s primärrätt

Bestämmelser om skydd av personuppgifter finns i unionsrättens primärrätt och sekundärrätt. I artikel 8.1 i rättighetsstadgan slås fast att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Enligt artikel 8.2 i stadgan ska personuppgifter behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har vidare rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem. Av artikel 8.3 i stadgan följer att en oberoende myndighet ska kontrollera att dessa regler efterlevs. Begränsningar i rätten till skydd av personuppgifter får – i likhet med vad som gäller för andra fri- och rättigheter enligt stadgan – göras på de grunder som anges i artikel 52 (se föregående avsnitt).

Rätten till skydd för enskilda personer med avseende på behandlingen av personuppgifter kommer till uttryck även i artikel 16 i fördraget om Europeiska unionens funktionssätt (FEUF) där den rättsliga grunden för lagstiftningsåtgärder inom unionsrättens tillämpningsområde slås fast. I artikel 16.2 FEUF anges att oberoende myndigheter ska kontrollera att de bestämmelser som Europaparlamentet och rådet antar följs. En särskild rättslig grund för lagstiftning på området för den gemensamma utrikes- och säkerhetspolitiken finns i

[7] Jfr Europadomstolens resonemang i *S. och Marper mot Förenade kungariket.*

artikel 39 FEUF. Även där slås fast att oberoende myndigheter ska kontrollera att bestämmelserna följs.

3.2.2 Dataskyddsdirektivet

En allmän reglering om skydd av personuppgifter inom EU finns i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet). Det är ett fullharmoniseringsdirektiv som har antagits med stöd av fördragens bestämmelser om inre marknadens upprättande och funktion. Direktivet omfattar inte juridiska personer utan gäller bara i fråga om uppgifter som direkt eller indirekt kan hänföras till fysiska personer.

Dataskyddsdirektivet syftar dels till att skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter, dels till att säkerställa det fria flödet av personuppgifter mellan medlemsstaterna (artikel 1). I direktivet regleras ett antal allmänna principer om uppgifternas kvalitet och godtagbara grunder för behandling av personuppgifter i allmänhet och vissa särskilda uppgiftsslag i synnerhet (artiklarna 6–8). Vidare finns i direktivet bestämmelser om enskildas rätt till information och tillgång till uppgifter för att kunna ta till vara sin rätt (artiklarna 10–12), om rätt att motsätta sig behandlingen (artikel 14) och om krav på en nationell reglering rörande skadestånd och sanktioner vid överträdelser av de nationella genomförandebestämmelserna (artiklarna 23 och 24). Räckvidden av principerna om uppgiftsskydd och de rättigheter som slås fast för enskilda får enligt direktivet begränsas genom undantag i nationell rätt. Begränsningar får göras bl.a. om det är nödvändigt med hänsyn till statens säkerhet, allmän säkerhet eller förebyggande, undersökning, avslöjande av brott eller åtal för brott (artikel 13).

När det gäller kraven på säkerhet vid behandlingen av personuppgifter följer av direktivet att registeransvariga ska genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt

om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling. Dessa åtgärder ska åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som är förknippade med behandlingen och arten av de uppgifter som ska skyddas (artikel 17.1). Åtgärderna ska väljas med beaktande av såväl de tekniska möjligheter som finns för att åstadkomma en lämplig säkerhetsnivå som de kostnader som är förenade med att genomföra åtgärderna. Om den registeransvarige anlitar en registerförare – någon som utför behandlingen för den registeransvariges räkning – förutsätts att registerföraren kan ge tillräckliga garantier för att nödvändiga organisatoriska och tekniska säkerhetsåtgärder inrättas och följs (artikel 17.2). Några möjligheter att i nationell rätt göra undantag från dessa krav finns inte.

Regleringen i dataskyddsdirektivet begränsar förutsättningarna för överföring av personuppgifter till tredje land, dvs. till en stat som varken ingår i EU eller är ansluten till EES. Sådan överföring av personuppgifter är som regel tillåten bara om tredje landet, med beaktande av bl.a. uppgifternas art, behandlingens ändamål och varaktighet och de rättsregler och regler för yrkesverksamhet och säkerhet som gäller i det landet, kan anses säkerställa en adekvat skyddsnivå för uppgifterna (artikel 25). Det finns dock ett visst utrymme för avsteg från kravet på adekvat skyddsnivå i överföringslandets lagstiftning, bl.a. om den registeransvarige ställer tillräckliga garantier för att enskilda personers grundläggande fri- och rättigheter skyddas och för utövningen av motsvarande rättigheter. Sådana garantier kan framgå t.ex. av lämpliga klausuler i bindande avtal (artikel 26). De kan också skapas genom bindande företagsinterna regler inom en koncern.

Den registeransvarige bestämmer normalt själv för vilka ändamål personuppgifter ska få behandlas. Om den registeransvarige avtalar med någon annan att t.ex. lagra uppgifter för den registeransvariges räkning, får uppdragstagaren som utgångspunkt behandla uppgifterna – t.ex. lämna ut dessa – endast i enlighet med instruktion från den registeransvarige. Biträdet är dock skyldig att också utföra annan behandling, om detta följer av en förpliktelse enligt lag (artikel 16).

Varje medlemsstat ska enligt artikel 28.1 i dataskyddsdirektivet utse en eller flera myndigheter som har till uppgift att inom dess territorium övervaka tillämpningen av de bestämmelser som med-

lemsstaterna antar till följd av direktivet. Dessa myndigheter ska fullständigt oberoende utöva de uppgifter som åläggs dem.

3.2.3 Personuppgiftslagen

Dataskyddsdirektivet har genomförts i svensk rätt genom framför allt personuppgiftslagen (1998:204). Lagen är i första hand tillämplig på personuppgiftsansvariga (registeransvariga) som är etablerade i Sverige (4 §). Det innebär att lagen tillämpas på sådana fysiska eller juridiska personer som ensamma eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter och som har en effektiv och faktisk verksamhet med en stabil struktur i Sverige (se skäl 19 i ingressen till direktivet).

Lagen, som i huvudsak följer direktivets text och disposition, omfattar all automatiserad behandling av personuppgifter och manuell behandling av personregister. Rent privat användning av personuppgifter är dock undantagen. Det görs även undantag med hänsyn till offentlighetsprincipen och tryck- och yttrandefriheten. Särregler i annan lagstiftning tar över bestämmelserna i personuppgiftslagen.

Lagen innehåller bestämmelser om när behandling av personuppgifter är tillåten och när sådana uppgifter får föras över till en stat utanför EES (se vidare nedan avsnitt 3.2.5). För behandling av känsliga personuppgifter gäller särskilt stränga regler. Även vissa grundläggande krav på den som behandlar personuppgifter regleras, t.ex. att personuppgifter som samlats in för ett ändamål inte får behandlas för något annat oförenligt ändamål. Det finns i lagen vidare bestämmelser om information till de registrerade, om korrigering av personuppgifter och om säkerheten vid behandlingen. Den enskilde har, i fråga om s.k. automatiserade beslut, rätt att på begäran få manuell omprövning av beslutet och information om den automatiserade behandling som ligger bakom det. Automatiserad behandling av personuppgifter måste i princip anmälas till en tillsynsmyndighet, men omfattande undantag från denna anmälningsskyldighet medges, t.ex. när den ansvarige för behandlingen har tillsatt ett s.k. personuppgiftsombud med uppgift att självständigt kontrollera den ansvariges behandling. Den som bryter mot lagen kan drabbas av ingripanden från tillsynsmyndigheten, t.ex. ett vitesföreläggande,

eller skadestånd och straff. Lagen innehåller också bestämmelser om säkerhet vid behandlingen.

Av 2 § personuppgiftsförordningen (1998:1191) framgår att Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen. Det uppdraget utövas på ett sätt som är oberoende i förhållande till andra myndigheter. Att varken någon annan myndighet eller riksdagen får bestämma hur inspektionen ska besluta i ett särskilt fall som rör myndighetsutövning mot någon enskild eller mot en kommun eller som rör tillämpningen av lag följer av 12 kap. 2 § RF.

3.2.4 Polisdatalagen

Polisdatalagen (2010:361) gäller vid behandling av personuppgifter i brottsbekämpande verksamhet vid bl.a. Polismyndigheten och i Ekobrottsmyndighetens polisiära verksamhet. Lagen gäller i stället för personuppgiftslagen, men hänvisar till ett antal bestämmelser i personuppgiftslagen som alltså gäller vid behandling av personuppgifter i polisens brottsbekämpande verksamhet. Till exempel gäller, enligt 2 kap. 2 § polisdatalagen, personuppgiftslagens bestämmelser om information till den registrerade, om rättelse, om säkerhet vid behandlingen, om skadestånd vid felaktig behandling och om överklagande. För den personuppgiftsbehandling som inte avser brottsbekämpande verksamhet, exempelvis tillståndsgivning eller mer renodlad övervakning och ordningshållande verksamhet, gäller personuppgiftslagen. Polismyndigheten är enligt 2 kap. 4 § polisdatalagen personuppgiftsansvarig för den behandling av personuppgifter som myndigheten utför och den behandling som utförs i polisiär verksamhet vid Ekobrottsmyndigheten.

I polisdatalagen anges för vilka ändamål personuppgifter får behandlas i polisens brottsbekämpande verksamhet. Ändamålen delas in i primära och sekundära, där de primära avser behandling av personuppgifter för att tillgodose de behov som finns inom polisens brottsbekämpande verksamhet och de sekundära anger när personuppgifter, som får behandlas i polisens brottsbekämpande verksamhet, får användas i andra delar av polisens verksamhet eller lämnas ut till andra myndigheter eller organisationer för dessas behov. De primära ändamålen är uttömmande angivna i 2 kap. 7 § polisdatalagen. Personuppgifter får enligt den bestämmelsen behandlas om de behövs för

att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller beivra brott eller fullgöra förpliktelser som följer av internationella åtaganden.

De sekundära ändamålen regleras i 2 kap. 8 § polisdatalagen. Enligt den bestämmelsen får personuppgifter behandlas om det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket, eller hos utländsk myndighet eller mellanfolklig organisation. Personuppgifter får vidare behandlas om det är nödvändigt för att tillhandahålla information som behövs i polisens handräckningsverksamhet eller, om det finns särskilda skäl, att tillhandahålla information i annan verksamhet som polisen ansvarar för. Personuppgifter får även behandlas om det är nödvändigt för att tillhandahålla information som behövs i verksamhet hos Kriminalvården för att förebygga brott och upprätthålla säkerheten, eller i en myndighets verksamhet i övrigt, om polisen är skyldig att bistå myndigheten med viss uppgift, eller informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott. Uppgifter som behandlas för ett primärt ändamål får även behandlas om det är nödvändigt för att lämna information till riksdagen och regeringen samt, i den utsträckning det finns en uppgiftsskyldighet i lag eller förordning, till andra. I ett enskilt fall får personuppgifter behandlas genom att lämnas ut även för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in (finalitetsprincipen). Uppgifter om en person får inte behandlas enbart på grund av vad som är känt om personens ras eller etniska ursprung, politiska åsikter, religiösa eller filosofiska övertygelse, medlemskap i fackförening, hälsa eller sexualliv (2 kap. 10 §). Om uppgifter om en person behandlas på annan grund får de kompletteras med sådana uppgifter när det är absolut nödvändigt för syftet med behandlingen. Tillgången till personuppgifter ska begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter (2 kap. 11 §).

För uppgifter som görs eller har gjorts gemensamt tillgängliga i polisens brottsbekämpande verksamhet finns särskilda och mer begränsande regler i 3 kap. polisdatalagen. Avgörande för om uppgifter ska anses gemensamt tillgängliga är hur många personer som har rätt att ta del av dem. Uppgifter som endast ett fåtal personer

har rätt att ta del av anses inte som gemensamt tillgängliga (3 kap. 1 §). Vid bedömning av om en uppgift har gjorts gemensamt tillgänglig saknar det betydelse hur många personer som rent faktiskt tar del av de aktuella uppgifterna. Säkerhetspolisen, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket får medges direktåtkomst till personuppgifter i polisens brottsbekämpande verksamhet som gjorts gemensamt tillgängliga.

Personuppgifter får inte bevaras under längre tid än vad som behövs för något eller några av de i lagen angivna ändamålen (2 kap. 12 §). Vidare gäller följande för uppgifter i ärenden om utredning eller beivrande av brott som har gjorts gemensamt tillgängliga. Om en brottsanmälan avskrivs på grund av att den påstådda gärningen inte utgör brott, får personuppgifterna i anmälan inte längre behandlas i polisens brottsbekämpande verksamhet. Om en brottsanmälan i annat fall inte har lett till förundersökning eller annan motsvarande utredning, får personuppgifterna inte behandlas i polisens brottsbekämpande verksamhet när åtal inte längre får väckas för brottet (3 kap. 10 §). Om en förundersökning har lett till åtal eller annan domstolsprövning, får personuppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år efter utgången av det kalenderår då domen, eller det beslut som meddelades med anledning av talan, vann laga kraft. Om en förundersökning har lagts ned eller avslutats på annat sätt än genom åtal, får personuppgifterna i förundersökningen inte behandlas i polisens brottsbekämpande verksamhet när det har förflutit fem år efter utgången av det kalenderår då åklagarens eller förundersökningsledarens beslut meddelades (3 kap. 11 §).

Uppgifter som inte har gjorts gemensamt tillgängliga eller behandlas i särskilda register ska, om de behandlas i ett ärende, normalt gallras senast ett år efter det att ärendet avslutades. Om de inte kan hänföras till ett ärende ska uppgifterna gallras senast ett år efter det att de behandlades automatiserat första gången (2 kap. 13 §). Detta gäller dock inte personuppgifter i ärenden om utredning eller beivrande av brott. I fråga om uppgifter i sådana ärenden tillämpas i stället arkivlagens (1990:782) bestämmelser om gallring (prop. 2009/10:85 s. 328).

I 5 kap. polisdatalagen finns bestämmelser om behandling av personuppgifter i Säkerhetspolisens brottsbekämpande verksamhet. Dessa bestämmelser reglerar framför allt ändamålen för Säkerhets-

polisens personuppgiftsbehandling, vilka delvis avviker från regleringen för den övriga polisen. De primära ändamålen för behandlingen anges i 5 kap. 1 §. Bestämmelsen innebär att personuppgifter får behandlas i Säkerhetspolisens brottsbekämpande verksamhet, om det behövs för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott mot rikets säkerhet, tryckfrihetsbrott och yttrandefrihetsbrott med rasistiska eller främlingsfientliga motiv eller vissa former av terroristbrottslighet.

De sekundära ändamålen för Säkerhetspolisens behandling regleras i 5 kap. 2 §. Enligt den bestämmelsen får personuppgifter som behandlas enligt 1 § även behandlas när det är nödvändigt för att tillhandahålla information som behövs i brottsbekämpande verksamhet hos Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Kustbevakningen och Skatteverket, eller hos utländsk myndighet eller mellanfolklig organisation. Personuppgifter får vidare behandlas om det är nödvändigt för att tillhandahålla information som behövs i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst, om det finns särskilda skäl att tillhandahålla informationen, eller i en myndighets verksamhet i övrigt, om informationen tillhandahålls inom ramen för myndighetsöverskridande samverkan mot brott. Personuppgifter som behandlas enligt 1 § får även behandlas, om det är nödvändigt för att tillhandahålla information till riksdagen och regeringen samt, i den utsträckning skyldighet att lämna uppgifter följer av lag eller förordning, till andra. I ett enskilt fall får personuppgifter behandlas genom att lämnas ut även för något annat ändamål, under förutsättning att ändamålet inte är oförenligt med det ändamål för vilket uppgifterna samlades in.

Det finns även särskilda bestämmelser om bevarande och gallring av personuppgifter som behandlas av Säkerhetspolisen. Enligt 5 kap. 12 § första stycket ska uppgifter som har gjorts gemensamt tillgängliga som huvudregel gallras senast tio år efter utgången av det kalenderår då den senaste registreringen avseende personen gjordes. Om det finns särskilda skäl får dock Säkerhetspolisen besluta att personuppgifter får bevaras längre tid, om uppgifterna fortfarande behövs för det ändamål för vilket de behandlas (tredje stycket).

När det gäller behandlingen av känsliga uppgifter, utlämnande av personuppgifter och uppgiftsskyldighet gäller samma bestämmelser som för polisen i övrigt. Säkerhetspolisen är enligt 5 kap. 5 § person-

uppgiftsansvarig för den personuppgiftsbehandling som Säkerhetspolisen utför.

3.2.5 Överföring av personuppgifter till tredje land

3.2.5.1 Den EU-rättsliga regleringen

Regleringen i dataskyddsdirektivet begränsar förutsättningarna för överföring av personuppgifter till ett s.k. tredje land, dvs. till en stat som varken ingår i EU eller är ansluten till EES. Enligt artikel 25.1 i direktivet ska medlemsstaterna föreskriva att överföring av personuppgifter till tredje land endast får ske om det tredje landet säkerställer en adekvat skyddsnivå för uppgifterna. Bedömningen av om skyddsnivån är adekvat ska ske på grundval av alla de förhållanden som har samband med en överföring eller en grupp av överföringar av uppgifter. Härvid ska särskilt beaktas uppgifternas art, den eller de avsedda överföringarnas ändamål och varaktighet, ursprungslandet och det slutliga bestämmelselandet, de allmänna respektive särskilda rättsregler som gäller i det tredje landet liksom de regler för yrkesverksamhet som gäller där (artikel 25.2). Det finns dock ett visst utrymme för avsteg från kravet på adekvat skyddsnivå i överföringslandets lagstiftning, bl.a. om den registrerade har samtyckt till överföringen eller om den registeransvarige ställer tillräckliga garantier för att enskilda personers grundläggande fri- och rättigheter skyddas och för utövningen av motsvarande rättigheter (artikel 26). Sådana garantier kan framgå t.ex. av lämpliga klausuler i bindande avtal. De kan också skapas genom bindande företagsinterna regler inom en koncern.

Enligt artikel 25.6 i dataskyddsdirektivet kan EU-kommissionen besluta att ett tredje land genom sin interna lagstiftning eller på grund av sina internationella åtaganden har en skyddsnivå som är adekvat i den mening som avses i artikeln. Medlemsstaterna ska i sådana fall vidta de åtgärder som är nödvändiga för att följa kommissionens beslut. Kommissionen har fattat ett antal sådana beslut, bl.a. avseende Andorra, Argentina, Israel, Nya Zealand, Schweiz och Uruguay. Vidare har kommissionen i förhållande till USA beslutat att de s.k. Safe Harbour Privacy Principles, tillämpade i enlighet med den vägledning som ges i de frågor och svar som utfärdats av Förenta staternas handelsministerium, ska anses utgöra en adekvat skyddsnivå för

personuppgifter som överförs från gemenskapen till organisationer som är etablerade i Förenta staterna. Överföring av uppgifter till organisationer som har åtagit sig att följa dessa principer är följaktligen tillåtet. Överföring till Kanada är också tillåten, om mottagaren omfattas av landets lagstiftning om skydd för personuppgifter. Tillämpningen av dessa beslut har dock ifrågasatts av bl.a. Europaparlamentet som i kölvattnet av avslöjandena om den amerikanska försvarsunderrättelsemyndigheten NSA:s (National Security Agency) övervakning av elektronisk kommunikation har antagit en resolution som uppmanar kommissionen att omedelbart upphäva Safe Harbour-beslutet och överväga detsamma när det gäller besluten rörande Kanada och Nya Zealand.[8]

3.2.5.2 Dataskyddskonventionen

Europarådets konvention från 1981 om skydd för enskilda vid automatisk behandling av personuppgifter (CETS 108) trädde i kraft den 1 oktober 1985. Konventionen syftar till att säkerställa den enskildes rätt till personlig integritet i samband med behandling av personuppgifter och till att förbättra förutsättningarna för ett fritt informationsflöde över gränserna.

Dataskyddskonventionen innehåller principer för dataskydd som de konventionsanslutna staterna ska iaktta i sin nationella lagstiftning. Personuppgifter som är föremål för automatiserad behandling ska hämtas in och behandlas på ett korrekt sätt för särskilt angivna ändamål. Vidare ska uppgifterna vara relevanta för ändamålen och får inte senare användas på ett sätt som är oförenligt med dessa. Uppgifterna måste också vara riktiga och aktuella och de får inte bevaras längre än vad som är nödvändigt för ändamålen.

Av artikel 12.2 i konventionen följer som huvudregel att en konventionsstat inte av integritetsskyddsskäl får hindra att personuppgifter förs över till en annan konventionsstat för att användas där. En konventionsstat har rätt att göra undantag från den bestämmelsen om statens lagstiftning innehåller särskilda bestämmelser för vissa kategorier av personuppgifter eller automatiserade personregister på grund av uppgifternas eller registrens natur (artikel 12.3).

[8] Europaparlamentets resolution den 12 mars 2014, P7_TA-PROV (2014)0230.

Sådana undantag får dock göras bara när den andra partens föreskrifter inte ger ett likvärdigt skydd.

Europarådets ministerkommitté antog år 2001 ett tilläggsprotokoll till dataskyddskonventionen. Det innehåller bestämmelser om tillsynsmyndigheter och överföring av personuppgifter till länder som inte är bundna av konventionen. Tilläggsprotokollet trädde i kraft den 1 juli 2004.

Konventionen har ratificerats av samtliga medlemsstater i EU, samt flera andra stater, t.ex. Albanien, Azerbajdzjan, Island, Norge, och Ryssland.

3.2.5.3 Den svenska regleringen

Artikel 25 i dataskyddsdirektivet har genomförts i svensk rätt genom bestämmelsen i 33 § personuppgiftslagen. Av den bestämmelsen framgår att det som huvudregel är förbjudet att föra över personuppgifter som är under behandling till ett tredje land om landet inte har en adekvat skyddsnivå för uppgifterna. Frågan om skyddsnivån är adekvat ska bedömas med hänsyn till samtliga omständigheter varvid särskild vikt ska läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredje landet. Det är alltså fråga om en individuell bedömning som i princip ska göras för varje enskild överföring eller grupp av överföringar. I förarbetena framhålls att frågan om skyddsnivån i ett visst land är adekvat kan bedömas på olika sätt beroende på omständigheterna i det enskilda fallet, och att det mycket väl tänkas att ett land har adekvat skyddsnivå på vissa områden men inte på andra (prop. 1999/2000:11 s. 15).

Trots förbudet är det enligt 34 § personuppgiftslagen tillåtet att föra över personuppgifter till tredje land, om den registrerade har gett sitt samtycke till överföringen eller om överföringen är nödvändig för att den registrerades rättigheter ska kunna tas till vara eller skyddas. Det är också tillåtet att föra över personuppgifter för användning enbart i en stat som har anslutit sig till dataskyddskonventionen.

Regeringen eller den myndighet som regeringen bestämmer får enligt 35 § personuppgiftslagen under vissa förutsättningar meddela

undantag från förbudet att föra över personuppgifter till tredje land. Enligt samma bestämmelse får regeringen meddela föreskrifter om att överföring av personuppgifter till tredje land är tillåten, om överföringen regleras av ett avtal som ger tillräckliga garantier till ett skydd för de registrerades rättigheter. Regeringen har bemyndigat Datainspektionen att meddela föreskrifter om sådana undantag (14 § personuppgiftsförordningen [1998:1191]).

3.3 Elektronisk kommunikation

3.3.1 Allmänt om elektronisk kommunikation

Elektronisk kommunikation innebär överföring av signaler i elektronisk form. Elektronisk kommunikation omfattar telefoni, datakommunikation samt utsändningar till allmänheten genom radio och TV. Gradvis växer dessa tre delar samman. Denna utveckling har framför allt möjliggjorts genom den s.k. digitaliseringen och den tekniska standardiseringen genom framväxten av internet. Detta innebär att olika infrastrukturer och tekniker för överföring av kommunikation och tjänster som tidigare kunde tillhandahållas genom endast en teknik nu kan tillhandahållas genom flera. Det gör att det exempelvis är möjligt att ringa via datorn, använda internet via tv:n och se på tv i mobiltelefonen (jfr prop. 2002:03:110 s. 58).

Via elektroniska kommunikationsnät överförs ständigt en mycket stor mängd information. Där förmedlas bl.a. telefonsamtal, telefaxmeddelanden, elektronisk post, datakommunikation och annan kommunikation som innehåller meddelanden, dvs. information i form av text, bild eller ljud.

3.3.2 Integritetsskydd och tystnadsplikt vid elektronisk kommunikation

Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation) innehåller regler som syftar till att harmonisera medlemsstaternas bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, i synner-

het rätten till integritet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation. De syftar även till att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom unionen. Direktivets bestämmelser preciserar och kompletterar dataskyddsdirektivet och är därutöver avsedda även att skydda berättigade intressen för de abonnenter som är juridiska personer (artikel 1).

Bestämmelser om säkerhet vid behandlingen av uppgifter finns i artikel 4 i direktivet. Enligt artikel 4.1 ska leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten i sina tjänster, om nödvändigt tillsammans med leverantören av det allmänna kommunikationsnätet när det gäller nätsäkerhet. Dessa åtgärder ska säkerställa en säkerhetsnivå som är anpassad till den risk som föreligger, med beaktande av dagens tillgängliga teknik och kostnaderna för att genomföra åtgärderna. Om det föreligger särskilda risker för brott mot nätsäkerheten, ska leverantören enligt artikel 4.2 informera abonnenterna om sådana risker och, om risken ligger utanför tillämpningsområdet för de åtgärder som tjänsteleverantören ska vidta, om hur de kan avhjälpas, inbegripet en uppgift om de sannolika kostnader som detta kan medföra.

Enligt artikel 5 ska medlemsstaterna genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. Medlemsstaterna ska särskilt förbjuda avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller andra metoder som andra metoder som innebär att kommunikationen och de därmed förbundna trafikuppgifterna kan fångas upp eller övervakas av andra personer än användarna utan de berörda användarnas samtycke, utom när de har laglig rätt att göra detta i enlighet med direktivet.

I artikel 6 finns bestämmelser om för vilka begränsade ändamål trafikuppgifter får behandlas och krav på begränsningar i fråga om tillgången till uppgifter för dem som behöver det för att utföra vissa närmare angivna arbetsuppgifter. Som huvudregel ska trafikuppgifter om abonnenter och användare som behandlas och lagras av en leverantör utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra kommunikation. Trafikuppgifter som krävs för abonnentfakturering och betalning av samtrafikavgifter

får dock behandlas. Om abonnenten har samtyckt till det får uppgifter också behandlas för vissa marknadsföringsändamål.

Vidare finns i artikel 15 ett stöd för medlemsstaterna att – för vissa närmare specificerade ändamål – föreskriva undantag från de skyddsregler som finns i bl.a. artiklarna 5 och 6. Bland annat får undantag göras om det i ett demokratiskt samhälle är nödvändigt, lämpligt och proportionerligt för att skydda nationell säkerhet, försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott.

Direktivet om integritet och elektronisk kommunikation har genomförts i svensk rätt främst genom bestämmelser som tagits in i lagen (2003:389) om elektronisk kommunikation (LEK).

3.3.3 Lagen om elektronisk kommunikation

Lagen om elektronisk kommunikation trädde i kraft i juli 2003 och syftade bl.a. till att genomföra flera EG-direktiv om elektronisk kommunikation. Lagen är en i huvudsak näringsrättslig lagstiftning som syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer och största möjliga utbyte vad gäller urvalet av elektroniska kommunikationstjänster samt deras pris och kvalitet.

Lagen om elektronisk kommunikation gäller elektroniska kommunikationsnät och kommunikationstjänster med tillhörande installationer och tjänster samt annan radioanvändning (1 kap. 4 § första stycket). Elektroniskt kommunikationsnät definieras i lagen som system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier oberoende av vilken typ av information som överförs (1 kap. 7 §). Med elektronisk kommunikationstjänst avses i lagen en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät (1 kap. 7 §).

Bestämmelser om säkerhet vid tillhandahållande av allmänt tillgänglig elektroniska kommunikationstjänster finns i 6 kap. 3–4 b §§ LEK. Dessa bestämmelser genomför regleringen i artikel 4 i direktivet om integritet och elektronisk kommunikation. Konfidentialiteten

enligt artikel 5 i direktivet säkerställs bl.a. genom bestämmelser om förbud mot avlyssning i 6 kap. 17 § LEK och bestämmelser om tystnadsplikt i 20 § samma kapitel. I 20 § föreskrivs således att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till vissa närmare angivna uppgifter som rör ett meddelande inte obehörigen får föra vidare eller utnyttja det han eller hon har fått del av eller tillgång till. Tystnadsplikten omfattar uppgift om abonnemang, innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande. Enligt lagen har operatörerna dessutom tystnadsplikt för uppgift som hänför sig till användning av vissa hemliga tvångsmedel, nämligen hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, kvarhållande av försändelser samt inhämtning av uppgifter enligt inhämtningslagen (6 kap. 21 §). Ett obehörigt röjande eller utnyttjande av sådana uppgifter i strid med denna bestämmelse är straffsanktionerat som brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

Vidare innehåller LEK bestämmelser om under vilka förutsättningar trafikuppgifter får behandlas (6 kap. 5–8 §§). Som utvecklas närmare i avsnitt 4 finns även bestämmelser i lagen som anger att vissa uppgifter måste lagras under en närmare angiven tidsperiod för att de ska finnas tillgängliga för brottsbekämpande ändamål (6 kap. 16 a–f §§).

Vissa bestämmelser i LEK knyter an till rättegångsbalkens regler om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation. I 6 kap. 19 § LEK regleras anpassningsskyldigheten för operatörerna. Den innebär att vissa verksamheter ska bedrivas så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas under sådana former att verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade meddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand.

I lagen finns dessutom bestämmelser som ger såväl de brottsbekämpande som andra myndigheter möjligheter att utan domstolsprövning få tillgång till vissa uppgifter (6 kap. 22 §). Reglerna innebär bl.a. att operatörerna i vissa fall är skyldiga att på begäran lämna ut uppgifter om abonnemang, dvs. uppgifter som identifierar

en abonnent eller ett abonnemang, framför allt namn, titel, adress och abonnentnummer.

Enligt 2 § förordningen om elektronisk kommunikation är Post- och telestyrelsen (PTS) tillsynsmyndighet enligt lagen om elektronisk kommunikation.

3.4 Brottsbekämpande verksamhet

3.4.1 Brottsutredande verksamhet

Till polisens uppgifter hör bl.a. att förebygga brott och att bedriva spaning och utredning i fråga om brott som hör under allmänt åtal. Polisen har således – tillsammans med åklagaren – en brottsutredande funktion. Även vissa andra myndigheter, däribland Tullverket, har vissa självständiga brottsutredande uppgifter.

Förfarandet vid den utredning som föregår ett beslut om åtal, förundersökningen, regleras i rättegångsbalken och i förundersökningskungörelsen (1947:948). Förundersökning ska, enligt 23 kap. 1 § rättegångsbalken, inledas så snart det på grund av angivelse eller av annat skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats. Beslut att inleda förundersökning fattas oftast av Polismyndigheten eller av åklagare. Om förundersökning har inletts av Polismyndigheten eller annan och saken inte är av enkel beskaffenhet, ska ledningen av förundersökningen övertas av åklagare så snart någon är skäligen misstänkt för brottet eller om det finns särskilda skäl. Så är bl.a. fallet om det blir aktuellt att använda sig av hemliga tvångsmedel.

Förundersökningen har enligt 23 kap. 2 § rättegångsbalken huvudsakligen två syften. Det ena syftet är att utreda om brott har begåtts, vem som skäligen kan misstänkas för brottet och att skaffa tillräckligt material för bedömning av frågan om åtal ska väckas. Det andra syftet är att bereda målet så att bevisningen kan förebringas i ett sammanhang vid en huvudförhandling i domstol. Utifrån detta brukar förundersökningen indelas i ett spanings- respektive ett utredningsstadium.

De i lagen angivna syftena understryker förundersökningens förberedande karaktär och klargör att den primära uppgiften för polisens brottsutredande verksamhet är att ge åklagaren underlag för sitt åtalsbeslut. Huruvida åklagaren kan väcka åtal är helt bero-

ende av vad som har kommit fram under förundersökningen. Därför blir resultatet av förundersökningen i praktiken helt avgörande för utgången av målet.[9]

3.4.2 Underrättelseverksamhet

De brottsbekämpande myndigheternas underrättelseverksamhet beskrivs utförligt i Polismetodutredningens betänkande *En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen* (SOU 2009:1 s. 48 ff.).

3.4.2.1 Allmänt om underrättelseverksamhet

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

Det första ledet i underrättelseprocessen där information förädlas till underrättelser är planeringsfasen. I planeringsfasen tas ställning t.ex. till vilka områden som är prioriterade för underrättelseverksamheten och vilka uppgifter som ska inhämtas.

Information kan inhämtas från olika källor. Det kan t.ex. ske genom rutinmässig rapportering, spaning eller användning av över-

[9] Bring, Thomas och Diesen, Christian, Förundersökning, Norstedts Juridik, 4 uppl., 2009, s. 65.

skottsinformation från hemliga tvångsmedel. Information kan inhämtas även genom nationell och internationell samverkan samt från tipsare och informatörer. En annan källa för inhämtning är information som publicerats i tidningar eller på internet.

När informationen inhämtats bearbetas den genom att informationen struktureras, systematiseras och värderas, t.ex. genom jämförelser med sedan tidigare tillgängliga uppgifter. Därefter vidtar den avgörande fasen i underrättelseprocessen – analysen. Genom analysen tydliggörs sammanhang och den bearbetade informationen tillförs mervärden. Det kan handla om t.ex. hot- och riskanalys, analys av brottsmönster samt kartläggning av mer eller mindre löst sammansatta kriminella nätverk och grupperingar.

Efter inhämtning, bearbetning och analys delges informationen lämpliga mottagare. Det framtagna underrättelsematerialet kan läggas till grund för t.ex. beslut om att inleda förundersökning eller beslut om att vidta särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. Det kan alltså handla om allt från en redovisning till berörda chefer till att gå ut i media för att förebygga ett visst brottsligt tillvägagångssätt. En annan form av förebyggande verksamhet är att de berörda personerna kontaktas och därigenom blir medvetna om den brottsbekämpande myndighetens intresse, vilket många gånger leder till att den brottsliga verksamhet som var i görningen aldrig kommer till stånd.

Genom att slutligen utvärdera resultatet av vidtagna åtgärder och underrättelsernas betydelse i sammanhanget kan verksamheten tillföras ny kunskap för det fortsatta arbetet.

3.4.2.2 Polisens underrättelseverksamhet

Polismyndighetens underrättelseverksamhet utgör en del av beslutsstödprocessen inom den brottsbekämpande verksamheten. Arbetet beskrivs i termer av planera, inhämta, bearbeta, analysera och delge information. Resultatet är underrättelser, rapporter eller andra underlag, som syftar till att möjliggöra proaktiva och kunskapsbaserade beslut, planering och verksamhet i övrigt – strategisk, operativ och taktisk – på alla nivåer i polisorganisationen.

Till skillnad från Polismyndighetens utredande verksamhet fokuserar inte underrättelseverksamheten på enskilda brott, utan på

brottslig verksamhet. Utredande verksamhet i form av en förundersökning eller primärutredning är att betrakta som bakåtblickande, då utredningen avser ett specifikt brott som har begåtts. Underrättelseverksamheten är framåtblickande, då den förutser viss brottslighet, brottsutveckling eller ett visst fenomen. Material i förundersökning syftar vanligtvis till bevisföring. Information som hanteras i underrättelseverksamheten syftar oftast till att användas som underlag för bedömningar och analys avseende kommande brottslighet, brottsutveckling eller fenomen.

I enlighet med underrättelseprocessen bearbetar och registrerar Polismyndighetens underrättelsetjänst inkommen eller inhämtad information i kriminalunderrättelseregistret och i så kallade särskilda uppgiftssamlingar. Information kommer bland annat direkt från allmänheten i form av tips, från särskilda informatörer, i form av underrättelseuppslag från enskilda poliser, från andra myndigheter i Sverige, från polisens sambandsmän i andra länder samt från Europol och Interpol.

Inhämtad information bedöms för registrering i kriminalunderrättelseregistret och de särskilda uppgiftssamlingarna. Genom analys länkas uppgifter samman och sammanhang, nätverk och skeenden värderas. Resultatet blir ett underlag för strategiska och operativa beslut i polisverksamheten som sedan delges berörd beslutsfattare. Genom att utvärdera resultatet av vidtagna operativa åtgärder och underrättelsernas betydelse för dessa tillförs verksamheten ny kunskap som kan användas i framtiden.

Polisens underrättelseverksamhet bedrivs i huvudsak vid Polismyndighetens underrättelsetjänst. Underrättelsetjänsten är verksam på alla nivåer i organisationen.

På nationell nivå finns en underrättelseenhet vid Nationella operativa avdelningen, NOA. Underrättelseenheten vid NOA har processansvaret för polisens underrättelseverksamhet, ansvar för en nationell underrättelsebild, polisens underrättelsemodell och samordning samt beslutar om inriktningen för underrättelseverksamhet i hela polisorganisationen. Underrättelseverksamhet vid nationella underrättelseenheten är huvudsakligen inriktad mot organiserad brottslighet på nationell och internationell nivå. Inom vissa prioriterade områden bedrivs långsiktiga operativa underrättelseprojekt samt strategiska projekt.

Underrättelseenheten vid NOA innefattar Nationellt underrättelsecentrum, NUC, som samordnar myndigheters underrättelsearbete mot organiserad brottslighet på nationell nivå. I centret ingår Polismyndigheten, Ekobrottsmyndigheten, Kriminalvården, Kronofogdemyndigheten, Kustbevakningen, Skatteverket, Säkerhetspolisen, Tullverket, Åklagarmyndigheten, Försäkringskassan, Migrationsverket och Arbetsförmedlingen.

På regional nivå finns underrättelseenheter som ska bedriva underrättelseverksamhet med strategiskt och operativt fokus. Förutom bearbetning av underrättelseinformation ska enheterna också tillhandahålla strategiska och operativa analyser. De regionala enheterna ska upprätthålla en regional lägesbild.

De regionala enheterna innefattar även myndighetsgemensamma regionala underrättelsecenter, RUC. I likhet med NUC samordnar RUC myndigheters underrättelsearbete men på regional nivå.

På polisområdesnivå finns underrättelseenheter som ska bedriva underrättelseverksamhet med operativt och taktiskt fokus samt ha en arbetsprocess som stödjer inhämtning, bearbetning och delgivning på lokalpolisområdesnivå och regional nivå.

På lokalpolisområdena ska det finnas kontaktfunktioner gentemot underrättelseenheten i polisområdet för att säkerställa underrättelseprocessen såväl lokalt som regionalt och nationellt.

3.4.2.3 Säkerhetspolisens underrättelseverksamhet

Säkerhetspolisen har i uppdrag att leda och bedriva polisverksamhet för att förebygga och avslöja brott mot rikets säkerhet, bekämpa terrorism samt fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Med säkerhetsskydd avses skydd mot bl.a. spionerі liksom mot terroristbrott. Säkerhetspolisen har också i uppdrag att leda och bedriva det bevaknings- och säkerhetsarbete som avser den centrala statsledningen eller som har samband med statsbesök och liknande händelser.

Uppdraget att förebygga och avslöja brott mot rikets säkerhet innebär att Säkerhetspolisen ska motverka olaglig eller oanmäld underrättelseverksamhet som bedrivs i Sverige. Likaså ska Säkerhetspolisen förhindra att organisationer, grupper, nätverk eller enskilda individer bedriver säkerhetshotande verksamhet som syftar till att

hota eller störa det demokratiska styrelseskicket eller enskildas rätt att utöva sina demokratiska rättigheter. Uppdraget att bekämpa terrorism innebär att Säkerhetspolisen ska minska risken för att terroristbrott begås i Sverige och utomlands samt motverka att Sverige och svenska förhållanden utnyttjas som bas för stöd till terroristverksamhet. När det gäller skyddet av den centrala statsledningen ska Säkerhetspolisen verka för att den och de personer i övrigt som omfattas av Säkerhetspolisens personskyddsverksamhet ska kunna utföra sina åtaganden under trygga och säkra former. Säkerhetspolisens uppdrag är således i allt väsentligt brottsförebyggande. Den brottsutredande verksamheten kommer härigenom i andra hand och utgör en mycket begränsad del av uppdraget. Detta avspeglar sig också tydligt i Säkerhetspolisens resursfördelning mellan brottsförebyggande och brottsutredande arbete.

För att Säkerhetspolisen ska kunna fullgöra sitt uppdrag måste myndighetens verksamhet inriktas utifrån den hotbild som finns mot de företeelser som Säkerhetspolisen ska skydda. Det är dels fråga om en strategisk hotbild för att inrikta verksamheten långsiktigt, dels hotbilder som är knutna till en viss person, en viss händelse eller vissa företeelser. Hotbilden bestäms utifrån en bedömning av vilken avsikt och förmåga som en aktör har när det gäller att begå aktuella brott.

Säkerhetspolisens underrättelseverksamhet syftar i allt väsentligt till att lägga grunden för hotbildsbedömningarna och därigenom det brottsförebyggande arbetet. Tillförlitliga hotbilder och relevanta skyddsåtgärder förutsätter att underrättelseverksamheten kan följa olika aktörer och fånga upp varningssignaler redan innan en viss person vidtagit konkreta åtgärder för att begå ett brott. Det kan handla om att kartlägga utländsk underrättelseverksamhet i Sverige eller grupper som tydligt manifesterat en vilja att hota eller begå andra brott för att störa personer i syfte att få dem att sluta bedriva en viss politik. Det kan naturligtvis förekomma att Säkerhetspolisen får uppgifter som gör att en förundersökning ska inledas. Syftet med underrättelseverksamheten är dock inte att få fram uppgifter till underlag för en sådan bedömning.

Säkerhetspolisen tillämpar i princip samma modell som den övriga polisen för att styra underrättelsearbetet. Modellen innebär i korthet att ett väl definierat underrättelsebehov leder till en beställning av uppgifter. Beställningen resulterar i att olika inhämtningsåtgärder

vidtas. De inhämtade uppgifterna bearbetas och analyseras varefter resultatet rapporteras till beställaren. Resultatet ligger sedan till grund för beslut om fortsatta åtgärder. Genom att tillämpa modellen blir inhämtningen aldrig slumpartad. Underrättelseverksamheten är tydligt avgränsad och det finns ett väl definierat mål för arbetet.

Liksom beträffande den öppna polisen sätter de allmänna principer för polisingripande som anges i 8 § polislagen (1984:387) den yttre ramen för verksamheten. Säkerhetspolisen har alltså att beakta såväl behovs- som proportionalitetsprincipen innan en åtgärd beslutas. Säkerhetspolisens inhämtningsmetoder skiljer sig härigenom inte från de metoder som används inom polisen i övrigt. Det kan exempelvis vara fråga om inhämtning genom fysisk spaning, liksom genom öppna eller egna källor. Även såväl nationell som internationell samverkan med andra myndigheter har stor betydelse för underrättelseverksamheten.

3.4.2.4 Tullverkets underrättelseverksamhet

Underrättelseverksamhet i Tullverket utgör ett stöd för den brottsbekämpande verksamheten genom att tillföra aktuell och bearbetad information om förväntad eller pågående brottslig verksamhet samt kunskap om och förståelse av brottslig verksamhet.

Underrättelseverksamhet i Tullverket bedrivs genom insamling/inhämtning, bearbetning och analys av uppgifter. Syftet är att förhindra eller upptäcka brottslig verksamhet.

Resultatet av underrättelseverksamhet, de slutsatser eller produkter som tas fram, delges beslutsfattare på olika nivåer och ingår som beslutsunderlag dels vid beslut om inriktning och prioriteringar av Tullverkets brottsbekämpande verksamhet (strategisk underrättelse), dels vid beslut om direkt operativa åtgärder (operativ underrättelse).

Det finns fyra kärnområden för Tullverkets underrättelseverksamhet.

- Att utarbeta och löpande uppdatera profiler på objekt i de olika trafikflöden som från smugglingssynpunkt bör kontrolleras. Arbetet bygger bl.a. på återrapporter och iakttagelser från kontrollerande personal, på uppgifter i tillgängliga register och på uppgifter från samverkansmyndigheter.

- Att utarbeta underlag för beslut om direkt operativ åtgärd mot viss person eller grupp eller för beslut om att påbörja tullkriminalärende eller förundersökning. Detta sker genom inhämtning och bearbetning av uppgifter som kan förknippas med brottslig verksamhet.
- Att utarbeta underlag för beslut om inriktning och prioritering på något längre sikt av brottsbekämpande åtgärder. Dessa underlag kan avse visst trafikflöde, viss typ av transportmedel eller visst geografiskt område. Underlagen bygger på inhämtning och bearbetning av uppgifter som kan förknippas med brottslig verksamhet.
- Att löpande inhämta, kvalitetssäkra och systematisera uppgifter om misstänkt brottslighet.

I begreppet ”förhindra eller upptäcka” ligger att underrättelseverksamhet inte avser åtgärd mot ett redan begånget konkret brott utan i stället avser att söka avslöja om viss brottslighet har förekommit, pågår eller kan förutses. Man kan säga att verksamheten ofta börjar med en låg misstankegrad (anledning anta) om viss brottslig verksamhet. Genom riktad inhämtning och bearbetning av ytterligare uppgifter kan man antingen verifiera och komplettera till en högre misstankegrad, identifiera misstänkta och ett mer konkret brott eller avskriva den ursprungliga misstanken. Ju tidigare man kan komma fram till en grundad uppfattning i dessa avseenden desto bättre.

3.5 Uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

3.5.1 Allmänt om straffprocessuella tvångsmedel

Rättegångsbalken innehåller inte någon definition av vad ett straffprocessuellt tvångsmedel är. Det rör sig dock om åtgärder som har en funktion inom straffprocessen men som inte utgör straff eller andra sanktioner. Åtgärderna företas i myndighetsutövning och innebär intrång i en persons rättssfär utan att personen har lämnat

sitt samtycke. Vanligtvis – men inte beträffande alla tvångsmedel – innefattar användningen tvång mot person eller egendom.[10]

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

Bland de straffprocessuella tvångsmedlen intar de hemliga tvångsmedlen en särställning. Dessa är hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, kvarhållande (och kontroll) av försändelse samt hemlig rumsavlyssning. Även inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen, IHL) utgör ett hemligt tvångsmedel (prop. 2011/12:55 s. 111). Den berörde är inte medveten om dessa åtgärder, men det antas att de äger rum mot hans eller hennes vilja. De intrång i den personliga integriteten som åtgärderna innebär medför att de, även i avsaknad av tvång, betecknas som tvångsmedel.[11]

En grundläggande förutsättning för att använda straffprocessuella tvångsmedel är normalt att en förundersökning har inletts. Användningen ska då ytterst ha till syfte att utreda eller lagföra ett visst brott. Regleringen ger dock stöd även för att i vissa fall använda hemliga tvångsmedel för att förebygga, avslöja eller förhindra brottslig verksamhet utan att förundersökning har inletts, dvs. i underrättelseverksamhet.

När lagstiftaren har preciserat i vilka fall en viss myndighet ska ha rätt att få tillgång till en viss typ av uppgifter gäller enligt tolkningsprincipen om lex specialis att de begränsningar som följer av denna reglering inte ska kunna kringgås genom att myndigheten väljer att tillämpa t.ex. de allmänna bestämmelserna om husrannsakan och beslag. Regeringen har mot den bakgrunden uttalat att uppgifter som angår ett särskilt elektroniskt meddelande som finns hos en leverantör inte kan inhämtas med stöd av ett editionsföre-

[10] Se t.ex. Lindberg, Straffprocessuella tvångsmedel, 3 uppl. 2012, s. 5 f. samt Ekelöf, Rättegång, tredje häftet, 7 uppl. 2006, s. 38 f.
[11] Ekelöf, s. 42.

läggande eller husrannsakan i förening med beslag i fall där annars andra regler för utfående av sådana uppgifter gäller (prop. 2002/03:74 s. 45 f.).

Villkoren för att använda de olika tvångsmedlen skiljer sig åt beroende på vilken slags åtgärd som avses och för vilket ändamål den vidtas. För all användning av tvångsmedel gäller dock – vid sidan av kravet på uttryckligt lagstöd (legalitetsprincipen) – tre allmänna principer: ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Dessa principer innebär kortfattat att en myndighets befogenheter att använda tvångsmedel ska vara bundna till de ändamål för vilket tvångsmedlet har beslutats (ändamålsprincipen). Tvångsmedel ska bara få användas när det finns ett påtagligt behov av det och en mindre ingripande åtgärd inte är tillräcklig (behovsprincipen). En tvångsmedelsåtgärd måste vidare, när det gäller åtgärdens art, styrka, räckvidd och varaktighet, stå i rimlig proportion till vad som står att vinna med åtgärden (proportionalitetsprincipen).

3.5.2 Hur används uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet?

Vid bedömningen av hur långtgående inskränkningar i enskildas fri- och rättigheter som kan tolereras i ett demokratiskt samhälle för att förebygga och utreda brott är det av vikt att klargöra vilken betydelse en åtgärd som innebär intrång i en skyddad rättighet kan ha för att uppnå målet att förhindra och lagföra brott. En proportionalitetsavvägning måste därefter göras mellan åtgärdens betydelse för det eftersträvande ändamålet (samhällsnyttan) å ena sidan och den grad av intrång i enskildas skyddade rättigheter – t.ex. rätten till yttrande- och informationsfrihet eller rätten till självbestämmande och personlig integritet – som åtgärden innebär å andra sidan. När utformningen av regler som innebär intrång i enskildas personliga integritet övervägs är det därför viktigt att undersöka hur reglerna används i den brottsbekämpande verksamheten och vilka behov av reglerna som finns.

För att de brottsbekämpande myndigheterna ska kunna fullgöra sina uppgifter att förebygga, förhindra och utreda brott har myndigheterna behov av information. Detta behov kan vara olika stort beroende på vilken brottslighet och vilka aktörer det är fråga om. Brottsbekämparna kan använda olika metoder för att skaffa sig

relevant information, t.ex. spaning och förhör samt kontakter med anmälare och tipsare. Behovet av information i såväl utredningsverksamheten som i underrättelseverksamheten innefattar ett behov av uppgifter om elektronisk kommunikation.

Det kan inte längre råda någon som helst tvekan om att uppgifter om elektronisk kommunikation har mycket stor betydelse i nästan all verksamhet som rör utredning av allvarlig brottslighet. Beredningen för rättsväsendets utveckling (BRU) konstaterade redan 2005 i betänkandet *Tillgång till elektronisk kommunikation i brottsutredningar m.m.* (SOU 2005:38 s. 323 f.) att trafikuppgifter ofta utgjorde den information som var viktigast för att föra utredningar om grövre brott framåt och att sådana uppgifter också används i princip i varje utredning rörande grova brott som t.ex. mord, människorov, grovt rån, grov mordbrand, allmänfarlig ödeläggelse, grov våldtäkt, människohandel för sexuella ändamål, grovt barnpornografibrott och grovt narkotikabrott samt brott som faller inom Säkerhetspolisens område. Trafikuppgifterna är ofta av stor betydelse redan i utredningsarbetets inledningsskede, då en kontroll av de trafikuppgifter som har genererats i anslutning till en brottsplats och sådana uppgifter som kan knytas till ett brottsoffer eller en eventuell misstänkt person kan användas tillsammans med annan information för att föra utredningen framåt.

Trafikuppgifterna kan svara på frågor om vilka nummer som haft kontakt med varandra, hur intensiv kommunikationen har varit och var användarna av t.ex. mobiltelefoner eller annan kommunikationsutrustning har befunnit sig. Vid användning av anonyma tjänster, som t.ex. förbetalda kontantkort som saknar registrerad användare, kan informationen vara av stor betydelse i ett senare skede i utredningen då ett beslag av en mobiltelefon från en misstänkt person kan avslöja vilka kontakter den personen har haft och var han eller hon har befunnit sig vid olika tidpunkter i samband med att ett brott har begåtts. BRU konstaterade även att uppgifterna i många fall kan få till följd att personer avförs från utredningen genom att misstankarna mot dem visar sig sakna substans.

När det gäller planeringsskedet av ett brott är det genom tillgången till trafikuppgifter ofta möjligt att ta reda på t.ex. hur gärningsmännen har sammanträffat och hur de har rekognoserat vid gömställen, längs flyktvägar och vid brottsplatsen samt hur de införskaffat brottsverktyg eller stulit flyktbilar (SOU 2005:38 s. 324). Genom

tillgången till historiska trafik- och lokaliseringsuppgifter kan de brottsbekämpande myndigheterna således klarlägga händelser som anknyter såväl till själva brottstillfället som till planläggningen och flykten. Dessa uppgifter kan t.ex. leda till att gömställen upptäcks, att stulna pengar, flyktbilar eller annat gods påträffas och att bortförda personer eller döda kroppar hittas.

Vid utredningen av internetrelaterad brottslighet är trafikuppgifter ofta helt avgörande information för att möjliggöra identifiering av en misstänkt gärningsman. Möjligheten till anonymitet och begränsningen av forensisk bevisning för att utreda brott medför därför att trafikuppgifter i många fall inte kan undvaras vid utredning om internetrelaterad brottslighet, om sådan brottslighet alls ska kunna bekämpas. Från de brottsbekämpande myndigheterna har i flera sammanhang också framhållits att tillgången till trafikuppgifter i brottsutredningarna fått allt större betydelse i takt med den ökade användningen av kryptering, som innebär att innehållet i meddelanden inte blir åtkomligt för myndigheterna vid hemlig avlyssning av elektronisk kommunikation.

Det bör i sammanhanget även noteras att trafikuppgifternas betydelse i brottsutredningar också hänger samman med att den information som kommer fram vid hemlig övervakning och hemlig avlyssning av elektronisk kommunikation ofta bedöms ha ett betydande bevisvärde i rättegångar som rör grov allvarlig och organiserad brottslighet.

I Åklagarmyndighetens redovisning av användningen av vissa hemliga tvångsmedel under 2013 (ÅM-A-2013/1962) ges några exempel på situationer där hemlig övervakning av elektronisk kommunikation har varit till nytta för brottsutredningar:

> Under utredning av ett rån på allmän plats kan med hjälp av positionering av den misstänktes telefon fastslås att telefonen varit på platsen för brottet. Med hjälp av uppgifter om vilka samtal eller meddelanden som skett vid tiden för brottet eller i nära anslutning till denna kan utredas om det är den misstänkte som just vid tillfället förfogat över telefonen. Dessa uppgifter har stor betydelse vid förhör med den misstänkte för att ställas mot dennes eventuella förnekande av att ha varit på platsen. Uppgifterna kan också ha stor betydelse som bevisning vid en rättegång.

> Vid utredning av grov kvinnofridskränkning kan det vara av stor betydelse att med hjälp av samtalslistor kunna visa på omfattningen av och tidpunkterna för en misstänkt mans kontakter med sin tidigare hustru.

När det gäller underrättelseverksamheten anges i Åklagarmyndighetens redovisning att den typiskt sett vanligaste nyttan med inhämtade uppgifter om elektronisk kommunikation är att underrättelser om hantering av stora mängder narkotika vid ett flertal tillfällen på olika orter i och utanför Sverige, i kombination med inhämtade uppgifter om elektronisk kommunikation, lett till att förundersökningar kunnat inledas efter att rörelsemönster och kontakter mellan inblandade kunnat kartläggas samt att brottsmisstankar kunnat verifieras. Därefter har användning av andra hemliga tvångsmedel i kombination med spaning och utredningsarbete lett till frihetsberövanden och beslag av stora mängder narkotika. Inte sällan har samverkan skett mellan polisen och Tullverket samt med andra länders brottsbekämpande myndigheter.

Enligt redovisningen har Rikspolisstyrelsen och Tullverket kunnat konstatera att information om elektronisk kommunikation är väsentlig för myndigheternas underrättelseverksamhet och att de inhämtningsmöjligheter som inhämtningslagen medger har varit avgörande för att inleda förundersökning avseende en lång rad grova brott. Uppgifter om elektronisk kommunikation redan på underrättelsestadiet anges ofta vara avgörande för att koppla samman aktörer, platser och tidpunkter samt stärka misstankar så att en väl grundad förundersökning kan inledas.

Åklagarmyndighetens redovisning innehåller också några konkreta exempel på fall där inhämtade uppgifter om elektronisk kommunikation har använts i underrättelseverksamheten. Några av dessa återges nedan:

> Underrättelser avseende leveranser av stora mängder narkotika, från Malmö till Stockholm, ledde i kombination med uppgifter om elektronisk kommunikation till att en person greps på Stockholms Central. Initialt togs 15 kg marijuana i beslag. Slutligen dömdes tio personer till närmare 40 års fängelse och ca 50 kg olika cannabispreparat togs i beslag.

> Underrättelser gjorde gällande att personer hemmahörande i Skåne, tidigare dömda för narkotikabrott, sysslade med framställning av cannabis i stor skala. Framställningen skulle ske i antingen Danmark eller

Sverige. Underrättelserna tillsammans med inhämtning av uppgifter om elektronisk kommunikation ledde till att två personer greps då de transporterade 10 kg narkotika från Danmark till Sverige.

Inhämtning av uppgifter om elektronisk kommunikation, i kombination med underrättelser avseende omfattande hantering av narkotika i Stockholmsområdet, ledde till att ett kriminellt nätverk kunde kartläggas. Förundersökning kunde inledas och efter en tids spanings- samt utredningsåtgärder greps personerna varvid ett mycket stort parti narkotika kunde beslagtas.

Inhämtning av uppgifter om elektronisk kommunikation i kombination med underrättelser avseende att en utpekad person förfogade över stora mängder förfalskade tusenkronorssedlar ledde i kombination med annan spaning till inledande av förundersökning. Tre personer frihetsberövades och dömdes till fängelse för en rad olika brott. Avancerad utrustning för penningförfalskning togs i beslag.

Efter underrättelser avseende att ett stort antal bränder tidigare inträffat, utan att dessa anmälts och därmed inte heller förundersökning kunnat inledas, inhämtades uppgifter om elektronisk kommunikation i syfte att upptäcka och förhindra fortsatt brottslighet. Inhämtningsbeslutet ledde i sin tur till att förundersökning kunde inledas och inriktas mot en misstänkt person. Därefter kunde ytterligare beslut om hemliga tvångsmedel enligt rättegångsbalken användas.

Säkerhetspolisen har framfört till utredningen att analys av telefontrafik – oavsett verksamhetsområde – bedöms vara av ovärderlig vikt för myndighetens arbete. Exempelvis har Säkerhetspolisens spaningsresurser i vissa ärenden kunnat användas mer effektivt efter en telefonanalys som visat användarens dygnsmönster och geografiskt återkommande platser. I underrättelsesyfte bidrar telefontrafikdata också med mycket värdefull information bl.a. för att kartlägga aktörer och nätverk som har en avsikt och förmåga att begå brott som är allvarliga för rikets säkerhet. Lagstiftningen möjliggör således att på ett tidigt stadium fånga upp eventuella grupperingar, skeenden och modus i syfte att förhindra sådan brottslighet.

3.5.3 Regleringen av tillgången till uppgifter

3.5.3.1 Abonnemangsuppgifter, trafikuppgifter och lokaliseringsuppgifter

Av regleringen i 6 kap. LEK följer att trafikuppgifter som lagras av en leverantör med stöd av den tvingande regleringen i 16 a § i nämnda kapitel (se vidare avsnitt 4.2.2) får behandlas – vid sidan av själva lagringen och den efterföljande raderingen – endast för att lämnas ut enligt 6 kap. 22 § första stycket 2 LEK (abonnemangsuppgifter), 27 kap. 19 § rättegångsbalken och enligt inhämtningslagen. Villkoren för denna inhämtning av uppgifter, som alltså är uppdelad på tre olika regelverk, berörs mer ingående nedan.

Det kan nämnas att uppgifter som inte lagrats med stöd av den tvingande regleringen i 6 kap. 16 a § LEK ändå kan finnas tillgängliga hos leverantören exempelvis för att denne behöver uppgifterna för sin fakturering. Sådana uppgifter kan också hämtas in av de brottsbekämpande myndigheterna enligt gällande regelverk. Uppgifter som inte lagras enligt de tvingande reglerna kan i vissa situationer också lämnas ut enligt andra regelverk än de som nämns ovan. Ett exempel på det är reglerna om informationsföreläggande enligt 53 c § lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk.

Vidare finns, när det gäller andra uppgifter som rör leverantörernas kunder än de uppgifter som lagras enligt 6 kap. 16 a § LEK, bestämmelser som genombryter leverantörens tystnadsplikt i situationer som omfattar utlämnande för bl.a. delgivning i vissa fall, efterforskning av försvunna personer, identifiering vid olyckor och dödsfall samt underrättelse av vårdnadshavare till en underårig som misstänks för brott (6 kap. 22 § första stycket 1, 3, 6 och 7 LEK). I dessa fall genombryts tystnadsplikten – med ett undantag – enbart i fråga om uppgifter om abonnemang. För ändamålet att eftersöka försvunna personer ska även andra uppgifter som angår ett elektroniskt meddelande, t.ex. lokaliseringsuppgifter, på begäran lämnas ut.

Med uppgifter om abonnemang i 6 kap. 20 § LEK avses t.ex. uppgifter om abonnentens nummer, namn, titel och adress (prop. 1992/93:200 s. 310). Sådana uppgifter finns ofta tillgängliga i elektronisk form i abonnentförteckningar som leverantörerna upprättar. För att uppgifter om en fysisk person ska tas in i en abonnentförteckning som görs allmänt tillgänglig krävs att den enskilde lämnat sitt samtycke till det (6 kap. 16 § LEK). I den utsträckning uppgifter

finns tillgängliga i sådana allmänt tillgängliga förteckningar omfattas de, till följd av abonnentens samtycke, i praktiken inte av tystnadsplikten. Bestämmelserna om skyldighet att lämna ut uppgifter om abonnenter får därför betydelse i första hand i fråga om uppgifter som rör abonnenter som inte har lämnat sitt samtycke till att uppgifterna offentliggörs och när det gäller nummer som normalt inte offentliggörs, t.ex. ip-adresser.

En ip-adress (Internet Protocol Address) är en unik adress som en dator eller ett lokalt nätverk tilldelas för att datapaket ska kunna skickas och tas emot över internet genom det tekniska kommunikationsprotokollet Internet Protocol. Den kan därför liknas med en postadress för vanliga brevförsändelser. Ip-adressen är en teknisk uppgift som behövs för att ett datapaket ska nå sin destination på internet och ingår därför som en del av dessa datapaket.

En ip-adress kan vara fast eller dynamisk och tilldelas en användare via t.ex. en internetleverantör. Av praktiska skäl tilldelas privatpersoner vanligen dynamiska ip-adresser. Dessa är inte konstant knutna till specifika datorer eller annan utrustning som kommunicerar över internet utan tilldelas olika datorer beroende på vilka enheter som vid varje given tidpunkt är uppkopplade mot internet. Eftersom ip-adressen hänför sig till internetuppkopplingen som sådan och inte uteslutande rör ett visst elektroniskt meddelande kan ip-adressens huvudsakliga syfte sägas vara att identifiera abonnenten. Mot den bakgrunden anses ip-adressen, oberoende av om den är fast eller dynamisk, vara en uppgift om abonnemang (prop. 2011/12:55 s. 101).

Med trafikuppgifter avses i detta sammanhang enkelt uttryckt de uppgifter som behövs för att förmedla ett elektroniskt meddelande i ett elektroniskt kommunikationsnät eller för att fakturera ett sådant meddelande (6 kap. 1 § LEK). De trafikuppgifter som genereras vid elektronisk kommunikation kan avslöja t.ex. vilken typ av kommunikation som förekommit, vilken utrustning som har använts, vilka nummer eller adresser som har kommunicerat med varandra och hur länge kommunikationen har pågått. Utanför begreppet trafikuppgifter faller information som avslöjar meddelandets innehåll. Vid sidan av begreppet trafikuppgifter används även uttrycket lokaliseringsuppgifter för att beteckna uppgifter som genereras vid elektronisk kommunikation och som är knutna till

lokaliseringen av den kommunikationsutrustning som används vid överföringen av ett elektroniskt meddelande.

En uppgift om vilket abonnentnummer som har använts för att skicka eller ta emot ett visst meddelande utgör en trafikuppgift då uppgifterna behövs för att överföra meddelandet. En uppgift om vem som innehar detta nummer är däremot en abonnemangsuppgift. Dessa uppgifter finns normalt tillgängliga i leverantörernas kund- och faktureringssystem under den tid som de behövs för att fakturera för utnyttjade tjänster, erbjuda andra mervärdestjänster eller övervaka nätsäkerheten.

3.5.3.2 Tidigare regler om tillgången till trafikuppgifter

Lagen om elektronisk kommunikation trädde i kraft i juli 2003 och ersatte telelagen (1993:597) och lagen (1993:599) om radiokommunikation.

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

Tidigare kunde brottsbekämpande myndigheter få tillgång till historiska trafikuppgifter enligt två olika regelverk; bestämmelserna om hemlig teleövervakning (numera hemlig övervakning av elektronisk kommunikation) i rättegångsbalken och utlämnande av uppgifterna från leverantörer enligt lagen om elektronisk kommunikation. Myndigheterna kunde då få i princip samma uppgifter oavsett vilka bestämmelser som tillämpades. Förutsättningarna för att få ut uppgifter skiljde sig dock åt en del. För hemlig teleövervakning krävdes bl.a. att det fanns en skäligen misstänkt person, att åtgärden var av synnerlig vikt för utredningen, att åtgärden avsåg en teleadress med viss anknytning till den misstänkte och att åtgärden beslutades av domstol. Vidare krävde hemlig teleövervakning att misstanken avsåg antingen ett brott med minimistraff fängelse i minst sex månader eller ett sådant brott som pekades ut särskilt i bestämmelserna om hemlig teleövervakning.

För att få tillgång till uppgifter enligt LEK krävdes att misstanken avsåg brott med lägsta minimistraff fängelse i två år. I detta avseende var alltså kravet i LEK strängare än i rättegångsbalken. Däremot saknade reglerna i LEK motsvarigheter till de övriga kraven i rättegångsbalken. LEK ställde t.ex. inte upp några krav på att det skulle finnas en skäligen misstänkt person, att åtgärden skulle vara av någon viss vikt för utredningen, att åtgärden bara fick avse vissa teleadresser eller att den skulle beslutas av domstol. Det fanns inte heller några krav på att enskilda skulle underrättas om inhämtningen eller att Säkerhets- och integritetsskyddsnämnden skulle utöva tillsyn.

I samband med att reglerna i LEK om utlämnande av trafikuppgifter vid misstanke om vissa brott upphävdes uttalade regeringen att den aktuella regleringen i LEK inte framstod som ändamålsenligt utformad och att den inte heller i tillräcklig grad uppfyllde de krav på rättssäkerhet och integritetsskydd som måste ställas på sådana integritetskänsliga åtgärder (prop. 2011/12:55 s. 66). Enligt regeringen borde trafikuppgifter få inhämtas i förundersökningar endast efter beslut om hemlig övervakning av elektronisk kommunikation. Befogenheten att inhämta uppgifter i underrättelseverksamhet skulle däremot regleras i en ny lag (inhämtningslagen).

3.5.3.3 Tillgången till abonnemangsuppgifter

En leverantör som har fått del av eller har tillgång till uppgifter om abonnemang, innehållet i ett elektroniskt meddelande och andra uppgifter som angår ett särskilt elektroniskt meddelande har – med vissa undantag i förhållande till innehavaren av ett abonnemang och den som tagit del i utväxlingen av meddelandet – tystnadsplikt för dessa uppgifter (6 kap. 20 § LEK). Uppgifter som angår ett särskilt elektroniskt meddelande anses enligt praxis vara uppgifter om vilka som har deltagit i utväxlingen av ett elektroniskt meddelande, uppgifter om när och under hur lång tid utväxlingen ägde rum och uppgifter om positionen hos den utrustning som använts vid kommunikationen. Tystnadsplikten omfattar i förekommande fall även t.ex. information om att uppgifter i hemlighet har inhämtats av de brottsbekämpande myndigheterna (6 kap. 21 § LEK).

En åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller annan myndighet som ska ingripa mot brott (Tullverket, Kustbevak-

ningen och Skatteverket) har trots tystnadsplikten rätt att få tillgång till abonnemangsuppgifter, om uppgiften gäller misstanke om brott som myndigheten ska ingripa mot (6 kap. 22 § första stycket 2 LEK). Regleringen innebär att de brottsbekämpande myndigheterna i princip har rätt att inhämta abonnemangsuppgifter för att beivra alla typer av brott utom sådana brott som åtalas enbart av målsäganden. En begränsning av tillgången följer dock av ändamåls-, behovs- och proportionalitetens krav. Inhämtning av uppgifter om abonnemang enligt LEK anses inte vara hemlig tvångsmedelsanvändning (se prop. 2013/14:237 s. 134).

Fram till den 1 juli 2012 gällde att tystnadsplikten för abonnemangsuppgifter genombröts bara om fängelse var föreskrivet för brottet och det enligt myndighetens bedömning kunde föranleda annan påföljd än böter. På grund av denna begränsning kunde abonnemangsuppgifter i realiteten inte hämtas in för många brott av normalgraden med böter i straffskalan. I förarbetena till 2012 års ändring i lagen om elektronisk kommunikation konstaterade regeringen bl.a. att det hade skett en betydande teknisk utveckling och förändring av i vilken omfattning enskilda använder bl.a. datorer och mobiltelefoner (prop. 2011/12:55 s. 102). Trakasserier via internet av olika slag, nätmobbning och förtal, liksom vuxnas kontakter med barn i sexuella syften (grooming) bedömdes ha blivit ett allt större problem. Det framhölls att när sådant beteende misstänktes utgöra brott hade de brottsutredande myndigheterna ofta begränsade möjligheter att utreda brotten, bl.a. eftersom möjligheterna att identifiera den som stått bakom kommunikationen många gånger var små på grund av begränsningarna i rätten att få tillgång till abonnemangsuppgifter. Detsamma ansågs gälla i fråga om de reella möjligheterna för polisen att ingripa mot internetrelaterade immaterialrättsbrott. Vid bedömningen av det intrång som ett enskilt utlämnande av uppgifter om en abonnent innebär beaktade regeringen särskilt att privatpersoner vanligen använder dynamiska ip-adresser. Möjligheterna till kartläggning av en abonnents kontakter via internet vid andra tillfällen bedömdes därmed bli begränsade vid ett enstaka utlämnande. Vidare menade regeringen att de brottsbekämpande myndigheternas intresse av tillgång till uppgifter om abonnemang hade förändrats på grund av utvecklingen av den internetrelaterade brottsligheten. Regeringen ansåg att intresset av att lämna ut abonnemangsuppgifter för att bekämpa brott vägde tyngre än det mot-

stående intresset av att skydda enskildas integritet och föreslog därför att kravet på fängelse i straffskalan och det särskilda kravet i fråga om brottets straffvärde skulle tas bort (prop. 2011/12:55 s. 103). Riksdagen ställde sig bakom denna bedömning (bet. 2011/12:JuU8, rskr. 2011/12:212).

3.5.3.4 Hemlig övervakning av elektronisk kommunikation

Hemlig övervakning av elektronisk kommunikation innebär att uppgifter i hemlighet hämtas in om meddelanden som i ett elektroniskt kommunikationsnät överförs eller har överförts till eller från ett telefonnummer eller annan adress (t.ex. en ip-adress), vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område (s.k. basstationstömning), eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits (27 kap. 19 § första stycket rättegångsbalken). De uppgifter som kan hämtas in genom tvångsmedlet är alltså s.k. trafikuppgifter och lokaliseringsuppgifter. Tvångsmedlet ger inte tillgång till uppgifter om innehållet i meddelanden. Hemlig övervakning av elektronisk kommunikation omfattar såväl inhämtning av uppgifter från telefoni- och internetoperatörer som inhämtning genom egna tekniska medel som de brottsbekämpande myndigheterna förfogar över. Tvångsmedlet kan användas också för att hindra meddelanden som överförs i ett elektroniskt kommunikationsnät från att nå fram.

Hemlig övervakning av elektronisk kommunikation får enligt 27 kap. 19 § tredje stycket rättegångsbalken användas vid förundersökning om brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader, vid förundersökning som avser dataintrång, barnpornografibrott som inte är ringa eller narkotikabrott eller narkotikasmuggling av normalgraden. Därutöver får tvångsmedlet användas vid förundersökning om vissa samhällsfarliga brott som bekämpas av Säkerhetspolisen, t.ex. sabotage, spionerі och vissa former av terroristbrottslighet. Tvångsmedlet får också användas vid förundersökning om försök, förberedelse eller stämpling till nämnd brottslighet i den mån sådana förstadier till brott är straffbelagda.

En förutsättning för att hemlig övervakning av elektronisk kommunikation ska få användas vid förundersökning är att åtgärden är

av synnerlig vikt för utredningen. Som huvudregel krävs även att det finns någon som är skäligen misstänkt för brottet. Sedan den 1 juli 2012 kan tillstånd till tvångsmedlet emellertid meddelas även utan att det finns en skäligen misstänkt person om syftet med övervakningen är att utreda vem som skäligen kan misstänkas för brottet. Det krävs då att förundersökningen avser brott som kan leda till hemlig avlyssning av elektronisk kommunikation. Det ska alltså vara fråga om

- ett brott vars minimistraff är fängelse i minst två år,
- vissa särskilt angivna samhällsfarliga brott som bekämpas av Säkerhetspolisen,
- försök, förberedelse eller stämpling till sådana brott om detta är straffbart, eller
- ett annat brott om brottets straffvärde med hänsyn till omständigheterna kan antas överstiga två års fängelse

När hemlig övervakning av elektronisk kommunikation används för att hämta in uppgifter om meddelanden i syfte utreda vem som skäligen kan misstänkas för ett brott får övervakningen bara innebära inhämtning av uppgifter i förfluten tid (27 kap. 20 § andra stycket rättegångsbalken).

Hemlig övervakning av elektronisk kommunikation som avser en skäligen misstänkt person får endast avse ett telefonnummer, en annan adress eller en elektronisk kommunikationsutrustning som innehas eller har innehafts eller annars kan antas ha använts eller komma att användas av den misstänkte under den tid tillståndet till övervakning gäller (27 kap. 20 § första stycket 1 rättegångsbalken).

Tvångsmedlet får enligt huvudregeln användas endast efter förhandsprövning och beslut av domstol. Tingsrätten prövar frågan efter ansökan av åklagare (27 kap. 21 § rättegångsbalken). Om det kan befaras att det skulle innebära en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd, får tillstånd ges interimistiskt av åklagaren i avvaktan på domstolens prövning. Ett sådant beslut ska utan dröjsmål anmälas till rätten som skyndsamt ska pröva om det finns skäl för åtgärden. Om domstolen vid sin prövning bedömer att det inte finns skäl för åtgärden ska den upphäva beslutet. I sådana fall får uppgifter som redan har inhämtats

med stöd av det interimistiska beslutet inte användas i en förundersökning till nackdel för den som har omfattats av övervakningen (27 kap. 21 a § rättegångsbalken).

I ett beslut att tillåta hemlig övervakning av elektronisk kommunikation ska det anges vilken tid åtgärden avser. Tiden får inte bestämmas längre än nödvändigt och får, när det gäller tid som infaller efter beslutet, inte överstiga en månad. Tiden kan dock förlängas genom ett nytt beslut. I beslutet ska också anges vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område tillståndet avser (27 kap. 21 § rättegångsbalken).

Möjligheterna att använda uppgifter som kommit fram vid hemlig övervakning av elektronisk kommunikation för att inleda förundersökning om ett annat brott än det som legat till grund för beslutet (s.k. överskottsinformation) är begränsade på så sätt att brott som kan antas leda till enbart en bötespåföljd normalt inte får användas (27 kap. 23 a § rättegångsbalken). Uppgifterna får dock alltid användas för att förhindra förestående brott.

I vissa fall får hemlig övervakning av elektronisk kommunikation användas också utan att en förundersökning pågår, då i syfte att förhindra vissa särskilt allvarliga brott. Enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (lagen om preventiva tvångsmedel) får tillstånd till bl.a. hemlig övervakning av elektronisk kommunikation meddelas om det finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar vissa särskilt angivna brott. Det rör sig främst om sådan samhällsfarlig brottslighet som bekämpas av Säkerhetspolisen, t.ex. sabotage, spionerі och terroristbrottslighet, men även vissa våldsbrott och brott mot frihet och frid som begås i syfte att påverka offentliga organ eller journalister (s.k. systemhotande brottslighet). I övrigt gäller i huvudsak samma regler för tvångsmedlen som när de används under en förundersökning. Till exempel krävs att åtgärden är av synnerlig vikt för att förhindra den brottsliga verksamheten och att den är proportionerlig.

3.5.3.5 Inhämtning av uppgifter enligt inhämtningslagen

Inhämtningslagen reglerar Polismyndighetens, Säkerhetspolisens och Tullverkets möjligheter att hämta in uppgifter om elektronisk kommunikation i underrättelseverksamhet. Lagen reglerar enbart inhämtning från den som enligt LEK tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, och ger alltså inte stöd för de brottsbekämpande myndigheterna att hämta in uppgifter med hjälp av egna tekniska hjälpmedel. Inhämtning av uppgifter enligt lagen utgör definitionsmässigt ett hemligt tvångsmedel (prop. 2011/12:55 s. 111).

De uppgifter som får hämtas in med stöd av lagen är

1. historiska uppgifter om meddelanden,
2. uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område (s.k. basstationstömning), och
3. uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits (1 §).

Uppgifter får hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott vilka har ett straffminimum på fängelse minst två år (2 §). Enligt en särskild bestämmelse (3 §) är inhämtning av uppgifter också möjlig vid brottslig verksamhet som innefattar vissa särskilt angivna samhällsfarliga brott inom Säkerhetspolisens ansvarsområde vilka har lägre straffminimum, t.ex. sabotage och spioneri. Denna bestämmelse är tidsbegränsad och gäller till utgången av 2016.

Beslut om inhämtning enligt lagen fattas av myndigheten själv och är inte föremål för någon utomstående förhandskontroll (4 §). Det är myndighetschefen eller annan person som har fått uppgiften delegerad till sig som fattar beslutet. Myndighetschefen får delegera uppgiften att fatta beslut bara till sådana personer som har den särskilda kompetens, utbildning och erfarenhet som behövs. Den som enligt delegation har fått rätt att hämta in uppgifter får inte fatta beslut om inhämtning i sådan operativ verksamhet som han eller hon deltar i. Beslutet ska vara preciserat och tiden för beslutet

får, när det gäller tid som infaller efter beslutet, inte överstiga en månad (5 §).

Säkerhets- och integritetsskyddsnämnden (SIN) utövar tillsyn över de brottsbekämpande myndigheternas användning av lagen (se vidare avsnitt 3.5.4.2). Nämnden ska också underrättas om samtliga beslut som fattas enligt lagen. Underrättelsen ska lämnas senast en månad efter det att ärendet om inhämtning avslutades (6 §). Nämnden är vidare skyldig att på begäran av enskild kontrollera om han eller hon har varit föremål för inhämtning enligt lagen.

Så kallad överskottsinformation som kommit fram om annan brottslighet får användas för att förhindra brott (7 §). Om uppgifter som kommit fram vid inhämtning ska användas i en förundersökning, krävs ett tillstånd till hemlig övervakning av elektronisk kommunikation (8 §). Ett sådant tillstånd ges av domstol.

3.5.4 Kontrollmekanismer

3.5.4.1 Förhandskontroll

De brottsbekämpande myndigheternas tillgång till trafik- och lokaliseringsuppgifter i en förundersökning om brott – och i vissa fall även tillgången till sådana uppgifter i Säkerhetspolisens och polisens underrättelseverksamhet – förutsätter som regel att tingsrätten, efter prövning av en ansökan från åklagaren, har meddelat tillstånd till inhämtningen (27 kap. 21 § rättegångsbalken). Vid denna prövning har domstolen att kontrollera om de villkor som gäller för övervakningen av elektronisk kommunikation är uppfyllda, bl.a. vilken typ av gärning som brottsmisstanken avser, vilka telefonnummer och andra adresser som ska övervakas, om övervakningen avser en person som är skäligen misstänkt eller i stället syftar till att klarlägga vem som skäligen kan misstänkas för brottet, om åtgärden är av synnerlig vikt för utredningen etc. Prövningen görs med utgångspunkt i ett konkret brott, och en bedömning görs normalt även av om omständigheterna i det enskilda fallet med tillräcklig grad av styrka (skälig misstanke) talar för att en viss person kan misstänkas för brottet.

Genom en förhandskontroll av domstol inrymmer systemet ett inslag som skapar starka garantier för att de åtgärder som brottsbekämpande myndigheter vidtar i varje enskilt fall uppfyller lagens

stränga begränsningar och skyddsregler. De brottsbekämpande myndigheterna tvingas noga motivera behovet av åtgärden för att övertyga domstolen om att övervakningsåtgärden ska tillåtas.

Som argument för att kräva förhandskontroll när det gäller åtgärder som inte är så resurskrävande för de offentliga organen kan också framhållas att resursargumenten, som annars i praktiken ofta är av stor betydelse för verksamheten (se t.ex. SOU 2012:44 s. 648) i sådana fall inte får någon påtaglig återhållande effekt. Vidare kan konstateras att en tillsyn som sker i efterhand normalt måste genomföras utifrån några slags urvalskriterier och knappast kan bli heltäckande.

För att förhandsprövningen ska kunna vara ett effektivt kontrollinstrument vid tvångsmedelsanvändning är det emellertid också viktigt att komma ihåg att domstolens prövning bygger på att de motstående intressen som ska balanseras mot varandra – brottsbekämpningsintresset och integritetsintresset – på något sätt kan relateras till varandra. En förhandskontroll av de brottsbekämpande myndigheternas underrättelsearbete kan således knappast inrymma annat än en ganska övergripande prövning av om myndigheterna har fog för sin misstanke att viss brottslig verksamhet planeras eller pågår, och bedömningen av integritetsintresset kan inte göras på ett lika konkret sätt, utifrån ett partsperspektiv, som i en förundersökning om brott. Betydelsen, effektiviteten och behovet av förhandskontroll kan därför variera beroende bl.a. på vilket typ av aktivitet som de brottsbekämpande myndigheterna ägnar sig åt och hur väl en efterhandskontroll – liksom regler om skadestånd och ansvar för tjänstefel – kan verka avhållande och disciplinerande i den brottsbekämpande verksamheten.

3.5.4.2 Efterhandskontroll

Tillsyn

Tillsynen över polisens och övriga brottsbekämpande myndigheters tillämpning av lagar och andra författningar i den brottsbekämpande verksamheten delas mellan flera myndigheter.

Säkerhets- och integritetsskyddsnämnden har i uppdrag att utöva tillsyn bl.a. över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel, däribland hemlig övervakning av elektronisk

kommunikation (1 § lagen [2007:980] om tillsyn över viss brottsbekämpande verksamhet). Tillsynen omfattar även verksamhet hos dessa myndigheter som hänger samman med själva tvångsmedelsanvändningen. Det innebär att tillsynen ska avse även den vidare hanteringen av inhämtade uppgifter hos myndigheterna, bl.a. när det gäller hantering av överskottsinformation. SIN:s uppdrag omfattar också tillsyn över polisens och Säkerhetspolisens behandling av personuppgifter enligt polisdatalagen (2010:361) och lagen (2010:362) om polisens allmänna spaningsregister.

SIN bedriver sin verksamhet genom inspektioner och andra utredningar som sker på eget initiativ (2 §). Till grund för tillsynsverksamheten ligger bl.a. de anmälningar som de brottsbekämpande myndigheterna gör om inhämtning enligt inhämtningslagen (6 § inhämtningslagen) och om de fall då underrättelse till enskilda som varit föremål för en övervakningsåtgärd har underlåtits på grund av sekretess (14 b § förundersökningskungörelsen [1947:948] och förordningen [2007:1144] om fullgörande av underrättelseskyldighet enligt lagen [2007:979] om åtgärder för att förhindra vissa särskilt allvarliga brott). Urvalet av tillsynsärenden görs med utgångspunkt i nämndens bedömning av var risken för felaktig rättstillämpning hos de granskade myndigheterna är som störst och tillsynsmetodiken är i huvudsak tematisk (se t.ex. SIN:s årsredovisning för 2013, dnr 7-2014, s. 10). 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.

SIN:s tillsyn avseende användningen av hemliga tvångsmedel har på senare tid särskilt inriktats på ärenden i vilka åklagare beslutat att underlåta underrättelse till enskild, frågor om förstöring av upptagningar och uppteckningar efter hemlig tvångsmedelsanvändning, dokumentationsfrågor samt beslut om inhämtning enligt inhämtningslagen. Under 2013 omfattande tillsynen även anmälningar till nämnden om interimistiska beslut enligt den nu upphävda lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott samt tillämpningen av 20 § förundersökningskungörelsen när det gäller protokollföringen av uppgifter som rör användningen av hemliga tvångsmedel. Tillsynen har enligt nämndens redovisningar visat att de brottsbekämpande myndigheterna överlag har bedrivit sin verksamhet i enlighet med lag och andra författningar. Brister har dock uppmärksammats, bl.a. har nämnden påpekat att åklagar-

nas rättstillämpning av de regler som styr underrättelseskyldigheten till enskild inte förefaller vara enhetlig, att förstöringen av upptagningar och uppteckningar från hemliga tvångsmedel i vissa fall har dröjt för länge och att dokumentationen över vidtagna åtgärder brustit. När brister har upptäcks har nämnden följt upp frågan, och normalt har det då visat sig att den aktuella myndigheten har vidtagit åtgärder för att komma till rätta med problemet (se SOU 2012:44 s. 667).

När det gäller tillsynen över tillämpningen av inhämtningslagen framgår av SIN:s redovisning av tillsynsverksamheten under år 2013 (nämndens uttalande den 22 maj 2014 i ärende med dnr 891-2014) att nämnden under året fått en god bild av hur polismyndigheterna och Tullverket hanterar ärenden enligt lagen. Granskningen har enlig nämnden visat att myndigheterna i de flesta fallen handlägger inhämtningsärendena på ett tillfredsställande sätt. I ett tidigare initiativärende, som avsåg samtliga underrättelser som kom in till nämnden under år 2012, har nämnden bl.a. konstaterat att det i några underrättelser antingen angetts att den brottsliga verksamheten innefattat ett brott som inte omfattas av inhämtningslagen eller inte tydligt framgått vilken brottsrubricering som avsetts. Vid granskningen av de underrättelser som kom in till nämnden under år 2013 har inte några sådana brister iakttagits. Enligt nämnden har dock granskningen även detta år visat att hanteringen har vissa brister. I ett stort antal fall har nämnden underrättats om beslut enligt inhämtningslagen för sent. I flera fall har dröjsmålet uppgått till närmare ett år.

Under senare tid har SIN även gjort några uttalanden om tillämpningen av reglerna i inhämtningslagen i vissa specifika fall. I ett av dessa fann nämnden att flera lagliga förutsättningar för att tillämpa inhämtningslagen hade saknats, att de inhämtade uppgifterna hade använts i förundersökning utan lagstöd, att det fanns brister i dokumentationen, att beslut om förstöring hade fattats för sent avseende vissa uppgifter och att det beträffande andra uppgifter var oklart om och när dessa förstörts (nämndens uttalande den 11 september 2014 i ärende med dnr 156-2014). Enligt uppgift från SIN har detta ärende också anmälts till åklagare.

I ett annat ärende konstaterade nämnden att dokumentationen i de granskade inhämtningsärendena var undermålig, men hade därutöver inget att anmärka mot vad som kommit fram (nämndens

uttalande den 9 oktober 2014 i ärende med dnr 158-2014). I ytterligare ett fall fann nämnden att två olika polismyndigheter hade fattat beslut om inhämtning av lokaliseringsuppgifter för en tid som överstigit en månad från dagen för besluten (nämndens uttalande den 9 oktober 2014 i ärenden med dnr 895-2014 och 896-2014). Nämnden framhöll dock i uttalandet att det inte fanns något som motsade att de felaktiga besluten hade sin grund i rena förbiseenden (inhämtningsperioden var en månad eller kortare, däremot rymdes inte beslutsdatumet inom denna period).

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen. Myndighetens tillsynsansvar omfattar all behandling av personuppgifter som är helt eller delvis automatiserad eller som ingår i manuella register. Datainspektionen och SIN har således delvis överlappande tillsynsansvar när det gäller polisens och Säkerhetspolisens behandling av personuppgifter. Frågan om hur tillsynen ska inrättas i framtiden när det gäller dessa myndigheter är för närvarande under utredning och hänger delvis samman med den pågående omorganisationen av polisen, se Polisorganisationskommitténs (Ju2010:09) betänkande Tillsyn över polisen (SOU 2013:42) och kommitténs tilläggsdirektiv från februari 2014 (dir. 2014:17). Övriga brottsbekämpande myndigheters behandling av personuppgifter står under tillsyn enbart av Datainspektionen. Datainspektionens och SIN:s tillsyn inriktas i första hand på att myndigheterna följer de föreskrifter som gäller för behandlingen av personuppgifter.

Därtill kommer att tillsyn över att statliga förvaltningsmyndigheter följer lagar och andra författningar samt i övrigt fullgör sina skyldigheter utövas även av Riksdagens ombudsmän (JO) och Justitiekanslern (JK).

JO:s arbete styrs av lagen (1986:765) med instruktion för Riksdagens ombudsmän. JO ska särskilt se till att de grundläggande fri- och rättigheterna inte överträds i den offentliga verksamheten, men också verka för att brister i lagstiftningen avhjälps. JO får därför göra framställningar till riksdag och regering om författningsändringar. Ombudsmännens tillsyn baseras på anmälningar som allmänheten skickar in samt på initiativärenden och inspektioner. I sin tillsyn får JO närvara vid en myndighets överläggningar och ha tillgång till myndighetens protokoll och handlingar. Myndigheter och tjänstemän är också skyldiga att lämna de upplysningar och yttranden som JO begär.

JO avgör ärenden genom beslut. I ett beslut kan JO uttala sig om en åtgärd av en myndighet eller en befattningshavare strider mot lag eller annan författning eller annars är felaktig eller olämplig, en s.k. erinran. JO har inte befogenhet att själv meddela straffrättsliga sanktioner eller disciplinära påföljder. JO är inte heller någon besvärsmyndighet och får därför inte överpröva eller på annat sätt ändra de granskade besluten. Beslut i JO:s ärenden är inte rättsligt bindande. I formellt hänseende är besluten inte något annat än ett uttryck för ombudsmannens personliga uppfattning i de behandlade frågorna. JO får även göra uttalanden som avser att främja enhetlighet och ändamålsenlig rättstillämpning. Enligt sin instruktion kan JO överlämna ett ärende till en annan myndighet för handläggning, om ärendet är av sådan karaktär att det är lämpligt att det utreds och prövas av någon annan myndighet än JO, och den myndigheten inte tidigare prövat saken. Överlämnanden av detta slag sker ofta till tillsynsmyndigheter.

JK har i likhet med JO tillsyn över myndigheter och deras tjänstemän. Tillsynen har till syfte att kontrollera att lagar och andra författningar följs. JK:s tillsyn är, i jämförelse med JO:s, mer övergripande och främst inriktad på att upptäcka systematiska fel i den offentliga verksamheten (se SOU 2013:42 s. 87).

Som regel initieras JK:s granskning av en anmälan från en enskild eller en myndighet. Ett tillsynsärende kan också påbörjas i samband med en inspektion eller genom att JK på eget initiativ tar upp ett ärende. I de ärenden som JK handlägger föreligger en skyldighet för enskilda befattningshavare och myndigheter att lämna den information och de yttranden som JK begär.

JK kan inte ge direktiv om hur ett ärende hos en förvaltningsmyndighet ska handläggas eller avgöras. Inte heller kan JK ompröva beslut som har fattats av andra myndigheter eller ändra deras avgöranden i sak. Som särskild åklagare har JK dock rätt att väcka åtal mot befattningshavare som begått brottslig handling genom att ha åsidosatt vad som ålegat henne eller honom i tjänsten. Vidare får JK göra en anmälan om disciplinpåföljd, avsked eller avstängning och har också rätt att föra talan i domstol om ändring av en myndighets beslut i sådana frågor.

Underrättelseskyldighet och kontroll på begäran av enskild

Den som har varit utsatt för hemliga tvångsmedel enligt rättegångsbalken ska som huvudregel underrättas om detta så snart det kan ske utan men för utredningen, dock senast inom en månad efter att förundersökningen avslutades (27 kap. 31 § rättegångsbalken). Det finns dock vissa möjligheter att skjuta upp underrättelsen om de uppgifter som den ska innehålla omfattas av vissa former av sekretess (27 kap. 33 § första stycket). Om sekretess fortfarande gäller ett år efter att förundersökningen avslutades behöver underrättelse inte lämnas. I sådana fall ska dock SIN underrättas om beslutet att underlåta underrättelse (14 b § andra stycket förundersökningskungörelsen). Vissa brott som faller inom Säkerhetspolisens ansvarsområde är också helt undantagna från underrättelseskyldighet (33 § tredje stycket rättegångsbalken). Motsvarande regler om underrättelseskyldighet gäller även för den öppna polisens tillämpning av lagen om åtgärder för att förhindra vissa särskilt allvarliga brott (16–18 §§). Däremot gäller inte någon underrättelseskyldighet enligt inhämtningslagen.

Som ett komplement till bestämmelserna om underrättelse till enskilda som utsatts för användning av hemliga tvångsmedel finns vidare en reglering som ålägger SIN en skyldighet att på begäran av en enskild kontrollera om han eller hon har utsatts för ett hemligt tvångsmedel och om användningen av detta tvångsmedel har skett i enlighet med lag eller annan författning. En sådan begäran får också avse frågan om polisens personuppgiftsbehandling varit författningsenlig. Den enskilde ska underrättas om att kontrollen har utförts (3 § lagen om tillsyn över viss brottsbekämpande verksamhet). Om nämnden bedömer att det förekommit felaktigheter som kan medföra skadeståndsansvar för staten gentemot den enskilde, anmäls sådana ärenden till JK som kan tillerkänna den enskilde ersättning för den skada och kränkning som en felaktig hantering av uppgifter eller en felaktig tillämpning av hemliga tvångsmedel inneburit. Om SIN i stället bedömer att det förekommit felaktigheter som innefattar misstanke om brott, ska ärendet anmälas till åklagare. Vidare ska nämnden, om den finner omständigheter som Datainspektionen bör uppmärksammas på, anmäla det till inspektionen (20 § förordningen [2007:1141] med instruktion för Säkerhets- och integritetsskyddsnämnden).

Antalet kontrollärenden på begäran av enskilda har varierat över åren. Under åren 2011 och 2012 inkom omkring 50 framställningar per år. År 2013 inkom 411 framställningar medan antalet ökade till 1 946 år 2014. Av SIN:s årsredovisning för 2014 (dnr 9-2015) framgår att den huvudsakliga förklaringen till det ökande antalet kontrollärenden är den uppmärksamhet som nämnden fick i samband med kritiken mot Polismyndigheten i Skånes behandling av personuppgifter i det s.k. Kringresanderegistret.

Av de kontrollärenden som avslutades under 2014 har något fler än hälften avslutats med att den enskilde underrättats om att det vid kontrollen inte framkommit något som talar för att hantering skett i strid med lag eller annan författning. I fem ärenden har den enskilde underrättats om iakttagna brister utan att någon anmälan skett till annan myndighet. Anledningen var att nämnden bedömde att bristerna inte var sådana att de kunde medföra skadeståndsansvar för staten eller annan åtgärd.

Under år 2011–2013 överlämnade SIN sammanlagt åtta ärenden till JK för prövning av om det förekommit felaktigheter som kan medföra skadeståndsansvar för staten gentemot den enskilde. År 2014 överlämnades 914 sådana ärenden till JK. I 912 av dessa bestod felaktigheten i att personen varit registrerad i Kringresanderegistret. JK har i ett principbeslut fastställt att den som har varit föremål för personuppgiftsbehandling i Kringresanderegistret har rätt till ersättning av staten med 5 000 kr.[12]

Av de tio ärenden under år 2011–2014 som inte avsett registrering i Kringresanderegistret är det endast ett ärende som ännu inte är avslutat. Två ärenden har skrivits av utan åtgärd. I tre fall har JK beviljat ersättning för kränkning av artikel 8 i Europakonventionen på den grunden att personuppgifter inte gallrats ur Säkerhetspolisens register i föreskriven ordning (i likhet med vad som i några fall förekommit i Segerstedt-Wiberg m.fl. mot Sverige). I ett fall har JK beviljat ersättning eftersom personuppgifter inte gallrats ur en polismyndighets register i enlighet med polisdatalagen (2010:361) I tre fall har kränkning av artikel 8 Europakonventionen konstaterats på grund av att upptagningar från hemlig teleavlyssning bevarats under längre tid än vad som medgetts i lag, dvs. utan stöd i lag. I dessa tre fall har JK bedömt att konstaterandet av en rättighetskränkning

[12] JK:s beslut den 7 maj 2014, diarienummer 1441-14-47.

ansetts vara tillräcklig gottgörelse för den ideella skada kränkningen inneburit. År 2012 överlämnades också ett ärende till Åklagarmyndigheten.

Parlamentarisk kontroll

En parlamentarisk kontroll av tillämpningen av reglerna om hemliga tvångsmedel utövas av riksdagen på grundval av en årlig skrivelse från regeringen. Skrivelsen omfattar de brottsbekämpande myndigheternas tillämpning av reglerna om hemlig avlyssning och övervakning av elektronisk kommunikation, hemlig kameraövervakning samt inhämtning av uppgifter enligt inhämtningslagen. De tillstånd som avser Säkerhetspolisens ärenden redovisas dock inte. Regeringen har nyligen också föreslagit att redovisningen ska omfatta även hemlig rumsavlyssning och tillämpningen av lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (prop. 2013/14:237 s. 133 f.). I skrivelsen redovisar regeringen bl.a. antalet tillstånd till respektive tvångsmedel, vilka brott som tillstånden avsett samt uppgifter om vilken nytta tvångsmedelsanvändningen har bedömts leda till.

4 Datalagring

4.1 Datalagringsdirektivet

4.1.1 Direktivets syfte och tillämpningsområde

Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (datalagringsdirektivet) antogs den 15 mars 2006. Direktivet syftade enligt artikel 1.1 till att harmonisera medlemsstaternas bestämmelser om skyldighet att lagra vissa uppgifter om elektronisk kommunikation för att på så sätt säkerställa att uppgifterna är tillgängliga för avslöjande, utredning och åtal av allvarliga brott. I direktivet definierades uppgifter som trafik- och lokaliseringsuppgifter samt de uppgifter som behövs för att identifiera en abonnent eller användare (artikel 2.2 a).

Direktivet gällde, enligt artikel 1.2, trafik- och lokaliseringsuppgifter om såväl fysiska som juridiska personer samt uppgifter som är nödvändiga för att kunna identifiera abonnenten eller den registrerade användaren.

4.1.2 Lagringsskyldighetens omfattning

Artikel 3 i direktivet ålade medlemsstaterna att anta åtgärder för att säkerställa lagring av sådana uppgifter som specificerades i artikel 5. Lagringsskyldigheten omfattade uppgifter som genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät vid leverans av kommunikationstjänster, i den utsträckning det sker inom statens territorium.

Medlemsstaterna ålades enligt artikel 6 att säkerställa att uppgifterna lagras under en period av minst sex månader och högst två år från det datum kommunikationen ägde rum.

De uppgifter som omfattades av lagringsskyldigheten angavs i artikel 5. Bestämmelsen var uppdelad utifrån olika ändamål för vilka uppgifterna skulle lagras. Det rörde sig om uppgifter som är nödvändiga för att spåra och identifiera en kommunikationskälla och för att identifiera slutmålet för kommunikationen. Lagringsskyldigheten omfattade dessutom uppgifter om datum, tidpunkt och varaktighet för kommunikationen, typen av kommunikation samt vilken utrustning som använts. Slutligen omfattade lagringsskyldigheten uppgifter som är nödvändiga för att identifiera lokalisering av mobil kommunikationsutrustning vad avser kommunikationens början. I anslutning till respektive ändamål angavs i detalj de kategorier av uppgifter som skulle lagras för respektive kommunikationssätt.

Inga uppgifter som avslöjar kommunikationens innehåll fick lagras enligt direktivet. Av skäl 13 i ingressen framgick att lagringen också borde ske på ett sådant sätt att man undviker att uppgifter lagras mer än en gång.

4.1.3 Hanteringen av lagrade uppgifter

Enligt artikel 4 i direktivet skulle medlemsstaterna vidta åtgärder för att säkerställa att lagrade uppgifter görs tillgängliga endast för behöriga nationella myndigheter i vissa närmare angivna fall. De närmare förutsättningarna för när och under vilka förutsättningar uppgifterna får lämnas ut skulle fastställas i respektive medlemsstat. I skäl 25 i ingressen klargjordes att direktivet inte påverkade hur medlemsstaterna reglerar frågan om de nationella myndigheternas tillgång till och användning av trafikuppgifter. I skäl 17 i ingressen framhölls dock att medlemsstaterna måste anta lagstiftning som säkerställer att lagrade uppgifter är tillgängliga bara för behöriga nationella myndigheter i enlighet med nationell lagstiftning och som respekterar grundläggande rättigheter för berörda personer fullt ut.

Medlemsstaterna skulle säkerställa att de lagrade uppgifterna på begäran kan överföras till behöriga myndigheter utan dröjsmål (artikel 8).

Frågan om uppgiftsskydd och datasäkerhet reglerades i artikel 7 i direktivet. Där angavs att varje medlemsstat, utan att det påverkar tillämpningen av de bestämmelser som antagits i enlighet med direktiv 95/46 och direktiv 2002/58, ska säkerställa att leverantörerna som lagrar uppgifter enligt direktivet som ett minimum respekterar vissa principer om datasäkerhet. Dessa var närmare angivna så att de lagrade uppgifterna dels skulle vara av samma kvalitet och föremål för samma säkerhet och skydd som uppgifterna i nätverket, dels skulle omfattas av lämpliga tekniska och organisatoriska åtgärder som säkerställer att de skyddas mot förstöring, förlust, ändring eller olaglig lagring, behandling av, tillgång till eller avslöjande av uppgifterna samt som säkerställer att tillgång ges endast till bemyndigad personal. Vidare angavs att uppgifterna skulle förstöras vid slutet av lagringstiden, utom de uppgifter för vilka tillgång har medgetts och som har bevarats. I artikel 9 angavs vidare att varje medlemsstat skulle utse en eller flera oberoende myndigheter för att övervaka leverantörernas tillämpning av artikel 7.

I skäl 16 i ingressen erinrades om tjänsteleverantörernas skyldigheter att vid behandlingen garantera uppgifternas kvalitet, sekretess och säkerhet i enlighet med dataskyddsdirektivet. Enligt artikel 13 i datalagringsdirektivet skulle medlemsstaterna också se till att de nationella åtgärder som genomför bestämmelserna om rättslig prövning, ansvar och sanktioner i dataskyddsdirektivet blir tillämpliga även på de uppgifter som avsågs i datalagringsdirektivet. Den rätt till ersättning som enligt dataskyddsdirektivet tillkommer varje person som lidit skada till följd av otillåten behandling eller någon annan handling som är oförenlig med de nationella bestämmelser som genomför direktivet skulle enligt skäl 19 i datalagringsdirektivet gälla även för personuppgifter enligt det sist nämnda direktivet.

Medlemsstaterna ålades vidare att införa sanktioner för att beivra otillåten avsiktlig tillgång till eller överföring av lagrade trafikuppgifter (artikel 13). Europarådskonventionen om IT-brottslighet från 2001 (CETS 185) liksom dataskyddskonventionen skulle också omfatta uppgifter som lagras i enlighet med direktivet om lagring av trafikuppgifter (skäl 20).

4.2 Den svenska regleringen

4.2.1 Genomförandeprocessen

Datalagringsdirektivet genomfördes i svensk rätt genom lag- och förordningsändringar som trädde i kraft den 1 maj 2012. Bestämmelserna om lagring finns i 6 kap. 16 a–f §§ LEK (prop. 2010/11:46, bet. 2011/12:JuU28, rskr. 2011/12:165–166). Kompletterande bestämmelser finns i 37–46 §§ förordningen om elektronisk kommunikation.

Till grund för genomförandet fanns förslag från Trafikuppgiftsutredningen som hade överlämnat sitt betänkande *Lagring av trafikuppgifter för brottsbekämpning* (SOU 2007:76) i november 2007.

När riksdagen under våren 2011 behandlade regeringens proposition återförvisades förslaget med stöd av 2 kap. 22 § RF till justitieutskottet för att där vila i minst ett år. När förslaget togs upp för förnyad behandling i kammaren den 21 mars 2012 bifölls det med kvalificerad majoritet. Riksdagen beslutade även på eget initiativ att de föreskrifter om skyddsåtgärder som regeringen bemyndigades att meddela snarast skulle underställas riksdagen för prövning (8 kap. 6 § RF). Detta skedde genom att en proposition underställdes riksdagen där det föreslogs att riksdagen skulle godkänna regeringens föreskrifter om särskilda tekniska och organisatoriska åtgärder för att skydda de lagrade trafikuppgifterna vilka hade förts in i förordningen om elektronisk kommunikation (prop. 2011/12:146, bet. 2011/12:JuU26, rskr. 2011/12:288–289). Riksdagen biföll förslaget den 19 juni 2012.

4.2.2 Lagringsskyldighetens omfattning

Den centrala bestämmelsen avseende lagringsskyldighetens omfattning finns i 6 kap. 16 a § LEK. Lagringsskyldiga är enligt den bestämmelsen de som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § samma lag. Därigenom omfattas leverantörer av allmänt tillgängliga kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning och av allmänt tillgängliga elektroniska kommunikationstjänster. Lagringsskyldigheten omfattar uppgifter som anges som nödvändiga för vissa preciserade syften. Dessa är formulerade som uppgifter som är nödvändiga för att kunna spåra och

identifiera en kommunikationskälla, slutmålet för kommunikationen, datum, tid och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning. Lagringsskyldigheten omfattar uppgifter som leverantören genererar eller behandlar i sin verksamhet. Det innebär att leverantören inte har någon skyldighet att skapa uppgifter som denne annars inte genererar eller behandlar. Lagringsskyldigheten är närmare strukturerad i vissa teknikslag. Dessa är angivna som telefoni, meddelandehantering, internetåtkomst och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform). I 39–43 §§ förordningen om elektronisk kommunikation anges på en mer tekniskt detaljerad nivå vilka uppgifter som ska lagras inom respektive teknikslag. PTS får också meddela närmare föreskrifter om de uppgifter som ska lagras (44 §).

Av 6 kap. 16 a § LEK följer vidare att den svenska regleringen på två punkter går längre än vad direktivet krävde. Lagringsskyldigheten omfattar nämligen även uppgifter som behövs för att lokalisera mobil kommunikationsutrustning vid kommunikationens slut samt uppgifter som genererats eller behandlats vid misslyckad uppringning.

En lagringsskyldig leverantör får enligt 6 kap. 16 a § tredje stycket LEK uppdra åt någon annan att utföra själva lagringen. Enligt 6 kap. 16 b § kan en leverantör, om det finns synnerliga skäl för det, undantas från lagringsskyldigheten.

Lagringsskyldigheten gäller enligt 6 kap. 16 d § LEK under sex månader från den dag då kommunikationen avslutades. Därefter ska uppgifterna omedelbart utplånas, om det inte är så att de har begärts utlämnade men ännu inte hunnit lämnas ut. I sådana fall ska uppgifterna i stället utplånas så snart de har lämnats ut.

4.2.3 Utlämnande av uppgifter

Som framgår ovan omfattas bl.a. uppgifter om abonnemang och andra uppgifter som angår ett särskilt elektroniskt meddelande som huvudregel av tystnadsplikt hos den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. De uppgifter som lagras enligt 6 kap. 16 a § LEK får, enligt 6 kap. 16 c §, lämnas ut till brottsbekämpande myndigheter endast

enligt 22 § första stycket 2 i samma kapitel (abonnemangsuppgifter), 27 kap. 19 § rättegångsbalken eller inhämtningslagen (för en närmare redogörelse för dessa regler, se avsnitt 3.5.3). De lagringsskyldiga leverantörerna ska enligt 6 kap. 16 f § LEK bedriva sin verksamhet så att uppgifterna kan lämnas ut utan dröjsmål och så att det inte röjs att uppgifterna lämnats ut. Uppgifterna ska också göras tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand av de brottsbekämpande myndigheterna.

De kostnader som uppstår vid utlämnande av lagrade trafikuppgifter ska leverantören få ersättning för av den myndighet som begärt ut uppgifterna (6 kap. 16 e § LEK). Enligt 46 § förordningen om elektronisk kommunikation får PTS, efter att ha hört Polismyndigheten, Säkerhetspolisen och Tullverket, meddela föreskrifter om ersättningen. PTS har meddelat sådana föreskrifter (PTSFS 2013:5). Övriga kostnader för lagring, säkerhet och anpassning av tekniska system m.m. ska leverantörerna själva stå för.

4.2.4 Säkerheten för lagrade uppgifter

Vid genomförandet av direktivet i Sverige konstaterades att det i lagen om elektronisk kommunikation redan fanns regler om såväl driftsäkerhet (5 kap. 6 a §) som integritetsskydd (6 kap. 3 §). Sist nämnda bestämmelse, som genomför artikel 4.1 i direktiv 2002/58/EG, reglerar leverantörernas skyldighet att vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna, är anpassad till risken för integritetsintrång. Detta grundskydd ansågs dock inte tillräckligt för uppgifter som skulle lagras enligt datalagringsdirektivet (prop. 2010/11:46 s. 54). Det angavs, mot bakgrund av det nya syfte för vilket uppgifter skulle lagras samt den mängd uppgifter det rörde sig om, att kravet på säkerheten borde höjas samt att säkerhetsnivån borde preciseras. Resultatet blev att det infördes en ny bestämmelse i 6 kap. 3 a § LEK av vilken det framgår att den som är lagringsskyldig enligt 6 kap. 16 a § samma lag ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. I förarbetena angavs att det därav följer att bestämmelsen, till skillnad

från vad som gäller enligt 6 kap. 3 § LEK, inte lämnar något utrymme att bestämma säkerhetsnivån genom en avvägning mellan teknik, kostnader och risken för integritetsintrång (prop. 2010/11:46 s. 75).

I 6 kap. 3 a § andra stycket LEK bemyndigas regeringen eller den myndighet regeringen bestämmer att komplettera lagbestämmelsen med ytterligare föreskrifter om säkerheten. Detta har regeringen gjort i 37 § förordningen om elektronisk kommunikation. Av bestämmelsen, som har godkänts av riksdagen, framgår att den som är lagringsskyldig ska vidta åtgärder för att säkerställa att de lagrade uppgifterna är av samma kvalitet och föremål för samma säkerhet och skydd som vid den behandling som skett före lagringen. Vidare framgår att åtgärder ska vidtas för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring samt för att förhindra otillåten lagring, behandling av eller tillgång till och otillåtet avslöjande av uppgifterna. Slutligen får uppgifterna göras tillgängliga endast för personal med särskild behörighet. PTS får efter att ha hört Polismyndigheten, Säkerhetspolisen och Datainspektionen meddela närmare föreskrifter om de åtgärder som ska vidtas.

PTS har med stöd av 37 § i förordningen meddelat sådana föreskrifter (PTSFS 2012:4). Dessa går i korthet ut på att den lagringsskyldige ska bedriva ett kontinuerligt och systematiskt säkerhetsarbete med beaktande av de särskilda risker lagringsskyldigheten medför (3 §). Rutiner ska finnas som säkerställer att bara personal med särskild behörighet har tillgång till lagrade uppgifter och de system som hanterar uppgifterna (4 §). Den utrustning som används för att lagra uppgifter ska också placeras i ett särskilt skyddat utrymme för att förhindra förlust av eller otillåten tillgång till uppgifterna (5 §). Vidare ska all behandling av lagrade uppgifter loggas i krypterad form och på ett sådant sätt att det går att följa upp vem som har haft tillgång till uppgifterna och vid vilken tidpunkt (6 §). Lagrade uppgifter ska också säkerhetskopieras (7 §).

PTS fick därutöver i uppdrag att utöva tillsyn över leverantörernas lagring av trafikuppgifter. Det ansågs att myndighetens befintliga tillsynsbefogenheter var ändamålsenliga och tillräckliga (prop. 2010/11:46 s. 55 f.). Av dessa följer att myndigheten bl.a. har rätt att förelägga en leverantör som bedriver verksamhet som omfattas av LEK att tillhandahålla myndigheten upplysningar och handlingar som behövs för att kontrollera lagens efterlevnad, att meddela före-

lägganden och förbud som får förenas med vite och, om ingen rättelse sker, återkalla ett tillstånd att bedriva verksamhet. De tillsynsbeslut som PTS fattar får överklagas hos allmän förvaltningsdomstol. När det gäller behandlingen av personuppgifter utövar även Datainspektionen tillsyn.

Vad slutligen gäller frågan om hanteringen av lagrade uppgifter vid lagringstidens slut anges i 6 kap. 6 d § LEK att den lagringsskyldige vid denna tidpunkt genast ska utplåna uppgifterna. Om uppgifterna har begärts utlämnade före utgången av lagringstiden men innan uppgifterna har hunnit lämnas ut, följer dock av bestämmelsen att leverantören ska fortsätta lagra uppgifterna till dess ett utlämnande har skett. Därefter ska leverantören genast utplåna dem.

4.3 EU-domstolens dom

EU-domstolen meddelade den 8 april 2014 dom i de förenade målen C-293/12 och C-594/12, Digital Rights Ireland m.fl., angående giltigheten av datalagringsdirektivet med anledning av begäran av förhandsavgöranden från nationella domstolar i Irland respektive Österrike. EU-domstolen förklarade i domen datalagringsdirektivet ogiltigt.

EU-domstolen konstaterade att de uppgifter som ska lagras enligt direktivet sammantaget gör det möjligt att dra mycket precisa slutsatser om enskildas privatliv, bl.a. om deras vanor i vardagslivet, om dagliga förflyttningar och sociala relationer (punkt 27). Domstolen slog fast att redan lagringsskyldigheten i fråga om de aktuella uppgifterna avseende personers privatliv och kommunikationer utgör ett ingrepp i de rättigheter som skyddas enligt artikel 7 i rättighetsstadgan (punkt 34). Ett ytterligare ingrepp i denna rättighet görs när nationella myndigheter medges tillgång till lagrade uppgifter (punkt 35). Det kunde alltså konstateras att det här rörde sig om två olika former av ingrepp i rätten till respekt för privatlivet. Eftersom direktivet föreskrev en behandling av personuppgifter innefattade regleringen också ett ingrepp i den i artikel 8 i rättighetsstadgan skyddade rättigheten (punkt 36).

Domstolen slog fast att direktivet innebar ett långtgående och synnerligen allvarligt ingrepp i rätten till privatliv och skyddet av personuppgifter. Domstolen noterade i samband med det bl.a. att

lagringen och den senare användningen kan ge berörda personer en känsla av att deras privatliv står under ständig övervakning (punkt 37). Domstolen konstaterade trots det att skyldigheten för leverantörer av allmänt tillgängliga kommunikationstjänster eller allmänna kommunikationsnät att lagra uppgifter och de nationella myndigheternas tillgång till dessa uppgifter inte kränkte det väsentliga innehållet i de skyddade rättigheterna och att datalagringsdirektivets materiella syfte – tillgängliggörandet av uppgifter för bekämpning av allvarlig brottslighet – motsvarade ett mål av allmänt samhällsintresse som erkänns av unionen (punkterna 39–42). Var och en har enligt stadgan rätt inte bara till frihet utan även till personlig säkerhet. Kravet att en inskränkning av en rättighet faktiskt måste svara mot ett allmänt samhällsintresse var därmed enligt EU-domstolen uppfyllt (punkt 44).

EU-domstolen gjorde därefter en noggrann prövning av om direktivet levde upp till den unionsrättsliga proportionalitetsprincipen. Domstolen konstaterade inledningsvis att lagringen är ägnad att nå det eftersträvade målet eftersom de nationella myndigheternas tillgång till lagrade trafikuppgifter innebär att myndigheterna ges ytterligare ett värdfullt verktyg för att klara upp brott (punkt 49). För att lagringen skulle kunna anses vara en proportionerlig åtgärd för bekämpningen av brott noterade domstolen att en sådan inskränkning av de grundläggande friheterna enligt fast praxis måste begränsas till vad som är strikt nödvändigt (punkt 52). Det innebar enligt domstolen att unionslagstiftningen måste föreskriva tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden och som uppfyller vissa minimikrav för att möjliggöra ett effektivt skydd mot riskerna för missbruk och otillåten tillgång och användning av enskildas personuppgifter (punkt 54).

De förhållanden som domstolen särskilt uppmärksammade vid sin proportionalitetsbedömning var för det första att det i direktivet inte fanns några generella begränsningar i lagringsskyldigheten då det i fråga om de uppgifter som skulle lagras inte gjordes någon åtskillnad eller några undantag som tog sin utgångspunkt i syftet att bekämpa brott (punkterna 57–59). Lagringskravet enligt direktivet omfattade nästintill all kommunikation – alla personer, alla kommunikationsmedel och alla trafikuppgifter – mellan enskilda i hela Europa. Domstolen konstaterade för det andra att det i direktivet inte angavs några objektiva kriterier för att avgränsa de nationella myndigheternas tillgång till och användning av de lagrade upp-

gifterna för bekämpning av brott som kunde anses vara av tillräckligt allvarligt slag för att motivera det aktuella ingreppet. Det lämnades i stället till medlemsstaterna att själva bestämma vad som utgjorde allvarlig brottslighet i detta sammanhang (punkt 60). Inte heller reglerades i direktivet vilka formella och materiella villkor som skulle gälla och vilka krav som skulle ställas på förfarandet för tillgång till uppgifterna. Domstolen noterade också att tillgången till uppgifter inte var underkastad någon förhandskontroll av en domstol eller oberoende myndighet som har till uppgift är att se till att tillgången begränsas till vad som är strikt nödvändigt (punkterna 61 och 62). Domstolen pekade vidare på att direktivet inte innehöll några bestämmelser som innebar att en åtskillnad skulle göras i fråga om lagringstiden för olika slags trafikuppgifter utifrån den nytta dessa har för att tillgodose syftet med lagringen och att det inte heller föreskrevs att lagringstiden måste bestämmas utifrån objektiva kriterier för att säkerställa att den inte går utöver vad som är strikt nödvändigt (punkterna 63 och 64). Slutligen uppmärksammade domstolen att det i direktivet saknades specifika regler om skydd av och säkerhet för lagrade personuppgifter som anpassade kraven till såväl mängden och arten av uppgifter som riskerna för otillåten tillgång till dessa. Domstolen menade i detta sammanhang att det inte fanns några garantier för att leverantörerna inte tar ekonomiska hänsyn när de bestämmer säkerhetsnivån eller för att uppgifterna förstörs när lagringstiden har gått ut. Domstolen ansåg också att kravet på en oberoende tillsyn inte kan garanteras om uppgifterna lagras utanför EU (punkterna 66–68).

Domstolen fann vid en samlad bedömning av nämnda förhållanden att EU:s lagstiftande församlingar överskridit sina befogenheter då direktivet antogs eftersom regleringen inte ansågs leva upp till proportionalitetsprincipen mot bakgrund av artiklarna 7, 8 och 52.1 i rättighetsstadgan (punkt 69).

EU-domstolens dom i det aktuella målet har tillbakaverkande (retroaktiv) effekt. Det innebär att domen får till följd att rättsläget numera är detsamma som om datalagringsdirektivet aldrig hade funnits. Detta gäller om inte domstolen i det enskilda fallet beslutar att ogiltigförklaringen inte ska få omedelbar och tillbakaverkande effekt. Innebörden av att domen får tillbakaverkande effekt är inte att nationella genomförandeåtgärder också omedelbart blir ogiltiga.

Däremot bortfaller med retroaktiv verkan medlemsstaternas unionsrättsliga skyldighet att lojalt genomföra unionsrättsakten.

4.4 Analysen

4.4.1 Analysens utgångspunkter

Den 29 april 2014 gav chefen för Justitiedepartementet en utredare[1] i uppdrag att biträda departementet med att, i ljuset av EU-domstolens dom, bl.a. grundligt analysera reglerna om lagring av uppgifter enligt 6 kap. 16 a–f §§ LEK, samt övriga bestämmelser om tillgång till och behandling av sådana uppgifter, och deras förhållande till unionsrätten. Analysen redovisades den 13 juni 2014 (Ds 2014:23).

Analysen är upplagd på samma sätt som EU-domstolens dom vilket innebär att svensk rätt analyserades i förhållande till de omständigheter som domstolen pekade särskilt på i domen. I analysen betonades att domstolens slutsats – att direktivet står i strid med rättigheter som garanteras av stadgan – bygger på en samlad bedömning av alla de behandlade frågorna. Domen ansågs alltså inte kunna tolkas så att domstolen presenterade en lista som i alla delar måste vara uppfylld för att regleringen inte ska anses oproportionerlig, utan det är först vid den sammantagna bedömningen som svensk rätts förenlighet med EU-rätten fullt ut kan avgöras. På samma sätt som EU-domstolen avslutades analysen därför med en samlad bedömning av om den svenska regleringen är proportionerlig och förenlig med Europarätten och EU-rätten. Det konstaterades därvid att det kan finnas skäl att överväga några närmare angivna frågor och vidta några åtgärder som skulle verka för att ytterligare stärka rättssäkerheten och integritetsskyddet i den svenska regleringen. Den samlade bedömningen var emellertid att det svenska regelverket avseende lagring av uppgifter samt övriga bestämmelser om tillgång till och behandling av sådana uppgifter, även utan sådana åtgärder, inte strider mot unionsrätten eller europarätten.

Slutsatserna i analysen redovisas närmare i det följande.

[1] F.d. justitierådet och ordföranden i Högsta förvaltningsdomstolen Sten Heckscher.

4.4.2 Lagringsskyldighetens omfattning

4.4.2.1 Generellt om lagringsskyldigheten

EU-domstolen konstaterade i sin dom (punkterna 56–59) att omfattningen av den lagringsskyldighet som följer av artikel 3 och 5 i direktivet innebär att trafikuppgifter lagras för alla personer och alla elektroniska kommunikationssätt, utan att någon urskillning görs av de uppgifter som kan tänkas vara relevanta för att uppnå målet att bekämpa allvarlig brottslighet. Man kan därmed säga att den inskränkning i de grundläggande rättigheter som följer av artiklarna 7 och 8, som lagringen av domstolen konstaterades innebära, omfattar hela Europas befolkning. Domstolen angav att lagringsskyldigheten som följer av direktivet således omfattade även personer som inte misstänks ha någon koppling till allvarlig brottslighet och utan någon möjlighet till undantag ens för de yrkeskategorier vars kommunikation enligt nationella regler omfattas av tystnadsplikt. Inte heller ställdes det i direktivet upp några tidsmässiga eller geografiska begränsningar och/eller begränsningar till en viss grupp av människor som gjorde att lagringsskyldigheten bara omfattade sådana uppgifter som av något skäl kan antas ha relevans för att förhindra, utreda eller åtala allvarliga brott.

Som framgår ovan innehåller direktiv 2002/58/EG regler om i vilka situationer och för vilka syften trafikuppgifter får behandlas. Tidigare följde av artikel 11 i datalagringsdirektivet att artikel 15.1 i direktiv 2002/58/EG inte skulle tillämpas på de uppgifter som specifikt måste lagras enligt datalagringsdirektivets bestämmelser. I det lagstiftningsärende som behandlade genomförandet av datalagringsdirektivet gjordes en sådan prövning i förhållande till artikel 15.1 följaktligen endast beträffande de uppgiftskategorier som skulle lagras utan att det fanns ett krav i datalagringsdirektivet.

I analysen framhölls att när datalagringsdirektivet förklarats ogiltigt måste det prövas om lagringen av alla de aktuella trafikuppgifterna kan anses vara en lämplig och proportionerlig åtgärd för att skydda allmän säkerhet och/eller för att förebygga, undersöka, avslöja och lagföra brott. Det kunde därvid konstateras att uppgifter om elektronisk kommunikation är av stort värde för att kunna upptäcka och utreda brott, inte minst vad gäller grov och organiserad brottslighet. Det framhölls att för viss typ av internetrelaterad brottslighet, som exempelvis barnpornografibrott, trafikuppgifter

också är av avgörande betydelse för att kunna identifiera en misstänkt gärningsman.

I denna del inhämtades uppgifter från polisen om behovet av de uppgifter som omfattas av lagringskravet enligt de svenska reglerna. Det framkom då att ingen lagrad information som i dag kan hämtas in kan anses som oviktig. Som extremt viktiga angavs uppgifter om lokaliseringen av var en telefon eller internetsession kopplat upp och riktningen till basstationen vara. Dessa uppgifter används för att positionera offer och misstänkta, kontrollera alibin och för att hitta vittnen eller misstänkta i ett område. Några få uppgifter bedömdes som mindre viktiga. Dessa var, såvitt avser telefoni, uppgifter om s.k. IMSI-nummer (del av 40 § punkten 1 förordningen om elektronisk kommunikation) eftersom denna information går att få fram genom SIM-kortets telefonnummer, uppgifter om den första aktiveringen av en förbetald anonym tjänst (del av 40 § punkten 3 förordningen om elektronisk kommunikation) och uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten (41 § punkten 3 förordningen om elektronisk kommunikation). När det gäller internetåtkomst och tillhandahållande av internetåtkomst ansågs uppgifter om typ av kapacitet för överföring och uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilde abonnenten (43 § punkterna 4 och 5 förordningen om elektronisk kommunikation) inte som viktiga utan som bra att ha i vissa fall. Samtliga övriga uppgifter bedömdes som viktiga.

Sammanfattningsvis ansågs denna redovisning stärka slutsatsen att de lagrade uppgifterna är ägnade att fylla en viktig funktion i de brottsbekämpande myndigheternas verksamhet med att skydda allmän säkerhet och förebygga, undersöka, avslöja och lagföra brott. Lagringen av uppgifterna för brottsbekämpande ändamål bedömdes därför som en lämplig åtgärd för att nå det eftersträvade målet.

I proportionalitetsprövningen beaktades de aspekter som EU-domstolen särskilt lyfte fram i sin dom. Domstolens resonemang i denna del gick sammanfattningsvis ut på att det kan ifrågasättas om en lagring av trafikuppgifter som omfattar samtliga personer och samtliga elektroniska kommunikationsslag är en proportionerlig åtgärd, trots att de uppgifter som lagras i de allra flesta fallen inte har någon som helst koppling till brottslig verksamhet av allvarligt

slag eller kan förväntas komma att användas vid utredande och lagföring av brott.

I analysen konstaterades att det är svårt att se någon annan rimlig väg för att på förhand begränsa lagringens omfattning till att omfatta endast uppgifter med koppling till brottslig verksamhet än att låta lagringsskyldigheten uppkomma först sedan någon form av misstanke riktats mot en viss person. En sådan begränsning bedömdes dock inte kunna göras utan att en mängd uppgifter som är av stor vikt för brottsbekämpningen försvinner. Inga historiska trafikuppgifter från tiden före ett brott begåtts och inga av de uppgifter som i dag inhämtas i polisens underrättelseverksamhet för att förebygga, förhindra eller upptäcka allvarlig brottslighet skulle då med säkerhet finnas att tillgå. Datalagring som metod bedömdes kort sagt förutsätta att alla uppgifter lagras, bl.a. eftersom det inte är möjligt att i förväg veta eller misstänka vilka uppgifter som kan vara viktiga.

EU-domstolen ansågs i denna del sätta fingret på själva grundtanken med lagringen av trafikuppgifter enligt datalagringsdirektivet, nämligen att säkerställa att uppgifterna finns tillgängliga för det fall de skulle behövas för att bekämpa allvarliga brott. Domen bedömdes dock inte kunna tolkas så att denna grundtanke, sedd för sig, hade underkänts av domstolen, utan det var den omfattande lagringen kombinerat med i första hand bristen på regler som begränsar tillgången till uppgifterna som gjorde lagringen oproportionerlig. Det konstaterades att de svenska tillgångsreglerna därför var av avgörande betydelse även för bedömningen av frågan om lagringens omfattning kan anses proportionerlig. Även skyddet för den merpart av alla uppgifter som lagras men aldrig begärs utlämnade måste också konstateras vara tillräckligt högt.

4.4.2.2 Särskilt om uppgifter som omfattas av yrkesmässig tystnadsplikt

Domstolen lyfte i sin dom också fram att det inte fanns någon begränsning i direktivet som möjliggjorde att kommunikation med personer som enligt nationell lag omfattas av yrkesmässig tystnadsplikt undantogs från lagringskravet. I analysen konstaterades att svenska regler om undantag från vittnesplikt för exempelvis advokater

och läkare omfattar uppgifter som anförtrotts dem i deras yrkesutövning. Vidare noterades att regeringen nyligen föreslagit att reglerna om avlyssningsförbud vid hemlig avlyssning av elektronisk kommunikation i 27 kap. 22 § rättegångsbalken ska utökas från att avse endast kommunikation med försvarare till att omfatta alla de yrkeskategorier som undantas från vittnesplikt enligt 36 kap. 5 § andra–sjätte styckena rättegångsbalken (prop. 2013/14:237 s. 131 f.). Det konstaterades samtidigt att det aldrig har varit aktuellt med något motsvarande förbud för uppgifter som inhämtas genom hemlig övervakning av elektronisk kommunikation. Med det synsätt som således kommer till uttryck i svensk lagstiftning – att det är uppgiftens innehåll som avgör om den omfattas av yrkesmässig tystnadsplikt – bedömdes det långsökt med en modell där exempelvis vissa telefonnummer på förhand skulle undantas från ett lagringskrav som i övrigt gäller generellt. Det ansågs i stället lämpligast att säkerställa en proportionell avvägning mellan brottsbekämpnings- och integritetsintresset genom en balanserad reglering om brottsbekämpande myndigheters tillgång till lagrade uppgifter. Det framhölls också att EU-rätten tillåter att medlemsstaterna löser frågor på olika sätt och enligt egna traditioner.

Sammanfattningsvis gjordes bedömningen att det ur ett EU-rättsligt perspektiv inte finns något som tyder på en konflikt mellan reglerna om yrkesmässig tystnadsplikt och ett generellt lagringskrav avseende trafikuppgifter.

4.4.3 Tillgången till lagrade uppgifter

4.4.3.1 Direktivet och EU-domstolens dom

I artikel 4 i datalagringsdirektivet föreskrevs att medlemsstaterna ska vidta åtgärder för att säkerställa att uppgifter som lagras i enlighet med direktivet görs tillgängliga endast för behöriga nationella myndigheter i närmare angivna fall och i enlighet med nationell lagstiftning. De förfaranden som skulle följas och de villkor som skulle uppfyllas för att få tillgång skulle fastställas av varje medlemsstat för sig i enlighet med nödvändighets- och proportionalitetskraven samt i enlighet med EU-rätten och folkrätten, särskilt med beaktande av Europakonventionen. Av artikel 1.1 framgick att syftet med lagringen var att säkerställa att uppgifterna finns tillgängliga för ut-

redning, avslöjande och åtal av allvarliga brott såsom de definieras av varje medlemsstat i deras nationella i lagstiftning. Tillgången var därigenom begränsad till brottsbekämpande myndigheter och brottsbekämpande syften (se prop. 2010/11:46 s. 47 f.). Enligt ett uttalande från rådet skulle medlemsstaterna, vid bedömningen av om de nationella brott som möjliggör ett utlämnande är tillräckligt allvarliga, ta ”vederbörlig hänsyn” till de brott som förtecknas i den lista som finns i artikel 2 i rådets rambeslut den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (2002/548/RIF) och till brott där telekommunikation ingår. Listbrotten i rambeslutet är till övervägande del mycket allvarliga brott såsom terrorism, mord och våldtäkt, men även ett antal brott som i och för sig är av något mindre allvarlig karaktär men kan sägas vara typiska för organiserad brottslighet, såsom exempelvis it-brottlighet, förfalskning och hjälp till olovlig inresa finns på listan.

I domen kritiserade EU-domstolen på ett antal punkter det faktum att datalagringsdirektivet inte närmare reglerade hur tillgång gavs till de uppgifter som lagrades enligt direktivet, utan i stor utsträckning lämnade fritt för medlemsstaterna att själva reglera den frågan (punkterna 60–62). Domstolen pekade på att det inte fanns något objektivt kriterium som begränsade tillgången till uppgifter i förhållande till brottets svårhetsgrad. Inte heller reglerade direktivet närmare hur de nationella myndigheterna kan få tillgång till uppgifterna. Vidare innehöll direktivet inga bestämmelser som begränsade antalet personer som kan få tillgång till uppgifterna till vad som kan anses absolut nödvändigt. Domstolen lyfte också fram att de nationella myndigheternas tillgång till lagrade trafikuppgifter inte var beroende av en föregående kontroll, antingen av en domstol eller av ett annat organ vars uppgift är att begränsa tillgången till vad som kan anses strikt nödvändigt.

4.4.3.2 Tillgången till abonnemangsuppgifter

Som framgår ovan (avsnitt 3.5.3.3) har en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller annan myndighet som ska ingripa mot brott (Tullverket, Kustbevakningen och Skatteverket) rätt att få tillgång till abonnemangsuppgifter, om uppgiften gäller brott som myndigheten ska ingripa mot (6 kap. 22 § första stycket 2 LEK).

Regleringen innebär att de brottsbekämpande myndigheterna i princip har rätt att inhämta abonnemangsuppgifter för att beivra alla typer av brott utom sådana brott som åtalas enbart av målsäganden.

I analysen påpekades att en uppgift om vem som innehar eller använder ett visst nummer för kommunikation inte är information som i sig är särskilt integritetskänslig. Sett isolerade i förhållandet till annan information om hur numret har använts kan sådana uppgifter nämligen inte användas för att kartlägga och analysera en individs privatliv. Uppgifterna kan emellertid användas tillsammans med andra uppgifter om trafik som förekommer i de allmänna kommunikationsnäten och därigenom indirekt utnyttjas för att kartlägga integritetskänsliga uppgifter om den enskildes privatliv. Ibland kan uppgifter om vilka personer eller organisationer en individ har haft kontakt med i sig vara mycket integritetskänsliga, t.ex. om uppgifterna kan avslöja att kontakter har förekommit med stödorganisationer för psykiatriska hälsoproblem eller med medicinska institutioner av olika slag. Samtidigt noterades att även om trafikanalys av metadata i vissa fall kan avslöja integritetskänsliga uppgifter, kan uppgifterna inte avslöja själva innehållet i kommunikationen. En enstaka uppgift om vem som är abonnent kan inte heller användas för att kartlägga sociala kontakter. Det påpekades också att uppgiften om vem som innehar ett visst internetabonnemang inte med säkerhet säger något om identiteten på användaren av en ip-adress eftersom en viss adress kan användas av flera personer. Möjligheterna att kartlägga enskildas privatliv med utgångspunkt i enstaka kontaktuppgifter bedömdes därför i många fall bli begränsade.

Det konstaterades också att möjligheten till utlämnande av uppgifter om en telefoni- eller internetanvändares identitet för brottsbekämpande ändamål svarar mot ett viktigt samhällsintresse som kan rättfärdiga ett intrång i privatlivet. Det framhölls att intrånget måste begränsas till vad som är strikt nödvändigt och att ju allvarligare ett misstänkt brott är, desto större integritetsintrång måste den enskilde typiskt sett tåla. Samtidigt påpekades att enskilda kan bli tvungna att tåla intrång även när det gäller brott med förhållandevis låga straffvärden, t.ex. i de fall uppgifterna är nödvändiga för att det överhuvudtaget ska finnas förutsättningar för myndigheterna att utreda misstankar om brott.

När det sedan gäller proportionaliteten bedömdes att medlemsstaterna, trots EU-domstolens generella uttalanden om att myn-

digheternas tillgång ska begränsas till brott som är av tillräckligt allvarlig natur, måste anses ha ett visst utrymme för att reglera vad som ska gälla för att lämna ut olika typer av uppgifter. Det konstaterades att domen inte kan tolkas så att varje form av utlämnande av någon lagrad uppgift som sker för att bekämpa mindre allvarlig brottslighet än sådan brottslighet som ursprungligen motiverat lagringsskyldigheten kommer i konflikt med unionsrätten. En nationell lagstiftning som tillåter att s.k. kataloguppgifter–uppgifter om vem som har en viss adress eller ett visst telefonnummer–kontrolleras och lämnas ut till brottsbekämpande myndigheter för att bekämpa även annan brottslighet än sådan som objektivt sett kan betecknas som allvarlig ansågs inte i sig stå i strid med den unionsrättsliga proportionalitetsprincipen. I den bedömningen beaktades att enbart kataloguppgifter inte är särskilt integritetskänsliga och att en enstaka uppgift om t.ex. en dynamisk ip-adress inte möjliggör någon mer omfattande kartläggning av den enskildes personliga förhållanden.

Slutligen analyserades frågan om kontrollen över utlämnandet av abonnemangsuppgifter. Inledningsvis framhölls att det av EU-domstolens dom inte kan utläsas att rättighetsstadgan och unionsrättens allmänna principer innebär att det är nödvändigt att inrätta en ordning med förhandsprövning av varje slag av åtkomst till uppgifter. Tvärtom ansågs det rimligt att skilda kontrollmekanismer bör kunna inrättas beroende bl.a. på vilket integritetsintrång som uppkommer till följd av utlämnandet och användningen av uppgifterna (se t.ex. Europadomstolens dom i P.G. och J.H. mot Förenade kungariket, nr 44787/98, § 46). Mot bakgrund av att abonnemangsuppgifter, tagna för sig, inte är särskilt integritetskänsliga bedömdes det tillräckligt med en oberoende kontroll och tillsyn i efterhand för att utlämnandet ska vara förenligt med regleringen om skydd för privatlivet och den personliga integriteten i Europakonventionen, rättighetsstadgan och unionsrättens allmänna principer.

Vid bedömningen av kontrollsystemet noterades i analysen att tillsynen över polisens och övriga brottsbekämpande myndigheters tillämpning av lagar och andra författningar i den brottsbekämpande verksamheten delas mellan flera myndigheter och att Datainspektionen och SIN har delvis överlappande tillsynsansvar när det gäller polisens och Säkerhetspolisens behandling av personuppgifter (se avsnitt 3.5.4.2). Slutsatsen var dock att den svenska regleringen torde rymmas inom ramen för vad som är godtagbart. Samtidigt

påpekades att det inte är möjligt att vara helt säker på att den nuvarande utformningen av tillsynsansvaret och de brottsbekämpande myndigheternas rutiner för dokumentation och loggning av inhämtning av abonnemangsuppgifter fullt ut tillgodoser kraven på effektiv kontroll. Vidare framhölls att unionsrätten och europarätten bara anger en miniminivå för skyddet av de grundläggande fri- och rättigheterna, och att utgångspunkten är att den svenska regleringen inte bör balansera på gränser för vad som är tillåtet enligt unionsrätten och Europakonventionen.

4.4.3.3 Tillgången till uppgifter enligt rättegångsbalken

Hemlig övervakning av elektronisk kommunikation kan användas av de brottsbekämpande myndigheterna för att få tillgång till trafikuppgifter och lokaliseringsuppgifter under förundersökning och, i vissa fall, för att förhindra vissa särskilt allvarliga brott (se avsnitt 3.5.3.4).

I analysen konstaterades inledningsvis att det stora flertalet brott som omfattas av tillämpningsområdet för hemlig övervakning av elektronisk kommunikation har ett minimistraff på minst sex månaders fängelse. Det ansågs inte råda någon tvekan om att dessa brott är att betrakta som allvarliga och att samhällsintresset av att förebygga och utreda brotten är starkt.

Det noterades vidare att hemlig övervakning av elektronisk kommunikation därutöver får användas i förundersökning om narkotikabrott och narkotikasmuggling av normalgraden och för att utreda dataintrång och barnpornografibrott av normalgraden trots att dessa brott har lägre minimistraff än fängelse i sex månader. Det framhölls att det vid hantering av betydande mängder narkotika i överlåtelsesyfte inte sällan döms till straff i den övre delen av straffskalan. Samhällsintresset av att förebygga och utreda narkotikabrott ansågs vara betydande, inte minst för att denna brottstyp är vanligt förekommande inom ramen för organiserad brottslighet. Brotten bedömdes i dessa fall som allvarliga i objektiv mening.

När det gäller barnpornografibrott och dataintrång framhölls att straffskalorna för dessa brottstyper stödjer slutsatsen att brotten inte är att betrakta som lika allvarliga som de övriga brottstyper som berättigar till användning av hemlig övervakning av elektronisk

kommunikation. Det kunde dock konstateras att tillgången till trafikuppgifter många gånger kan vara helt avgörande för att det över huvud taget ska vara möjligt att utreda och lagföra dessa brott, något som naturligtvis påverkar proportionalitetsbedömningen. Mot bakgrund av samhällets starka intresse av att skydda barn mot sexuell exploatering ansågs en ordning som innebär att barnpornografibrott inte kan utredas knappast kunna godtas. Vid motsvarande avvägning när det gäller dataintrång beaktades att brottet i vissa fall kan leda till omfattande integritetsintrång för enskilda och även andra omfattande skadeverkningar, bl.a. vid olika former av affärsspionage eller intrång i samhällsviktiga elektroniska uppgiftssamlingar. Samhällsintresset av att utreda brotten bedömdes därför vara betydande.

I analysen noterades vidare att hemlig övervakning av elektronisk kommunikation får användas även för att utreda – samt i vissa fall också för att förhindra – vissa samhällsfarliga brott som inte har ett straffminimum på fängelse i minst sex månader, exempelvis sabotage och spionerі. Dessa brott betraktas som särskilt allvarliga eftersom de riktar sig mot samhällsstrukturen och mot rikets säkerhet. Det ansågs därför finnas ett starkt samhällsintresse av att brotten effektivt kan utredas och förhindras.

I analysen beaktades också att den svenska regleringen inte bara innehåller specifika begränsningar i fråga om vilka brott som kan motivera en övervakningsåtgärd, utan även att de principer som gäller för all användning av straffprocessuella tvångsmedel innebär ytterligare begränsningar i möjligheterna till övervakning. Bland annat får en hemlig övervakningsåtgärd enligt 27 kap. rättegångsbalken användas bara när det är av synnerlig vikt för utredningen och en mindre ingripande åtgärd inte är tillräcklig. Tvångsmedlet måste även i fråga om sin art, styrka, räckvidd och varaktighet stå i rimlig proportion till vad som står att vinna med åtgärden. Vidare är myndigheternas befogenheter att använda ett tvångsmedel bundna till de ändamål för vilket tvångsmedlet har beslutats.

I analysen framhölls också att den svenska regleringen av de brottsbekämpande myndigheternas tillgång till trafik- och lokaliseringsuppgifter under pågående förundersökning bygger på att en allmän domstol i det enskilda fallet ska pröva om förutsättningarna för att lämna ut uppgifterna är uppfyllda innan uppgifterna lämnas ut och att undantag från denna regel gäller bara i vissa brådskande

fall. Vidare påpekades att tillsyn bedrivs även i efterhand av SIN genom inspektioner och genom kontroller på begäran av enskild. Systemet med domstolsprövning och tillsyn ansågs säkerställa att det finns en mycket effektiv kontroll som uppfyller europarättens och unionsrättens krav.

Sammantaget bedömdes i analysen att den lagring av uppgifter som sker för utlämnande av trafik- och lokaliseringsuppgifter i enlighet med bestämmelserna i 27 kap. rättegångsbalken uppfyller de krav som följer av den unionsrättsliga proportionalitetsprincipen.

4.4.3.4 Tillgången till uppgifter enligt inhämtningslagen

Som framgår ovan är de brottsbekämpande myndigheternas tillgång enligt inhämtningslagen i princip begränsad till att avse uppgifter som är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Av SIN:s redovisning av tillsynsverksamheten under år 2013 (dnr 891-2014) framgår att de vanligast förekommande brottsrubriceringarna vid inhämtning enligt lagen har varit grovt narkotikabrott och grov narkotikasmuggling. Av uppgifter från polisen framgår att i övrigt har uppgifter hämtats in om grova rån, mord, grov allmänfarlig ödeläggelse, grov penningförfalskning, människohandel samt några enstaka beslut avseende andra brott såsom grov mordbrand, grov kapning och grovt spridande av gift eller smitta. Uppgifter får i vissa situationer inhämtas även avseende brott som inte har ett straffminimum på två års fängelse. Det handlar om vissa särskilt angivna samhällsfarliga brott, exempelvis sabotage och spioneri som bekämpas av Säkerhetspolisen.

I analysen framhölls inledningsvis att brott vars minimistraff är fängelse i minst två år tveklöst tillhör kategorin allvarliga brott. Vidare bedömdes även de samhällsfarliga brott som omfattas av lagens tillämpningsområde trots att de har lägre minimistraff som allvarliga eftersom de riktar sig mot samhällsstrukturen och mot rikets säkerhet. Det framhölls också att lagen innehåller regler som definierar förutsättningarna för en begäran och vilka uppgifter inhämtningsbeslutet ska innehålla. Lagen innehåller också en proportionalitetsregel.

Ett frågetecken kring de svenska reglerna i ljuset av EU-domstolens dom ansågs däremot vara det förhållandet att uppgifter hämtas in av myndigheterna själva utan föregående prövning av en oberoende instans. Samtidigt framhölls att frågor om rättssäkerhet och integritetsskydd hade varit föremål för ingående överväganden när inhämtningslagen infördes, och det system som då beslutades hade ansetts uppfylla såväl dessa krav som kraven på ett praktiskt fungerande system. Vidare konstaterades att den statistik som hittills har presenterats av SIN och de brottsbekämpande myndigheterna visar att inhämtning sker i ett relativt begränsat antal ärenden och vid arbete med mycket grova brott. En möjlig slutsats av detta ansågs vara att, även om ingen oberoende instans i förväg prövar inhämtandebesluten, så har systemet med en efterföljande tillsyn av SIN en disciplinerande effekt på myndigheternas verksamhet. Dessa aspekter ansågs tyda på att den svenska regleringen vid en helhetsbedömning uppfyller kravet på att tillgången till lagrade uppgifter är begränsad till vad som kan anses strikt nödvändigt. I den bedömningen lades också stor vikt vid att uppgifter enligt inhämtningslagen kan hämtas in bara för mycket allvarlig brottslighet för vilken samhällsintresset av att brotten upptäcks är betydande.

4.4.4 Lagringstiden

EU-domstolen konstaterade i sin dom att lagringskravet i direktivet hade ställts upp utan någon differentiering mellan olika kategorier av data, baserat på hur användbara uppgifterna kan tänkas vara. Inte heller angavs i direktivet, med hänsyn till att medlemsstaterna har tillåtits ett tidspann på sex månader upp till två år, några objektiva kriterier som tillgodoser att lagringstiden begränsas till vad som kan anses strikt nödvändigt (punkterna 63 och 64). Nämnas kan också att Generaladvokaten i sitt yttrande i målet hade kommit till slutsatsen att en lagringstid som överstiger ett år inte kan anses proportionerlig. Som ovan redovisats valdes i Sverige den kortaste lagringstid direktivet tillåter för samtliga uppgiftskategorier, dvs. uppgifterna ska lagras i sex månader räknat från den dag då kommunikationen avslutades (6 kap. 16 d § LEK).

I analysen noterades inledningsvis att, när datalagringsdirektivet förklarats ogiltigt, det inte längre finns några EU-rättsliga krav som

hindrar att en kortare lagringstid än sex månader väljs. Det konstaterades dock att för att de lagrade uppgifterna ska tjäna sitt syfte, nämligen att kunna användas för att upptäcka, utreda och lagföra allvarliga brott, så måste de finnas tillgängliga under en så pass lång tid att de brottsbekämpande myndigheterna har en reell möjlighet att hinna begära ut dem innan de raderas. Av uppgifter som inhämtats från polisen framgick att teledata m.m. som inhämtas i underrättelseverksamhet i de flesta fall är yngre än en månad men att det även finns ärenden där historik upp till sex månader varit av stor vikt i analysarbetet. Det framgick också att den största andel uppgifter som begärs in i utredningsverksamheten är yngre än tre månader. Uppskattningsvis 20–25 procent angavs dock vara äldre än tre månader och cirka 10 procent av den totala mängden äldre än fem månader. Behovet av äldre uppgifter angavs särskilt gälla tidskrävande förundersökningar avseende grova våldsbrott av spaningskaraktär samt bekämpning av grova seriebrott som våldtäkter och mordförsök där det många gånger finns behov av äldre trafikdata för att kunna knyta en person till tidigare anmälda brott.

Mot bakgrund av detta ansågs slutsatsen kunna dras att en kortare lagringstid än sex månader skulle leda till att syftet med lagringen riskerade att inte kunna uppfyllas, särskilt vad gäller de grövsta brotten där det finns ett uttalat behov av äldre uppgifter. Det framhölls att det ur ett proportionalitetsperspektiv inte är acceptabelt med ett lagringskrav som tillgodoser behovet av uppgifter för att utreda mindre allvarlig brottslighet, samtidigt som uppgifter inte finns tillgängliga för att utreda grövre brott. Om en lagring för brottsbekämpande ändamål över huvud taget ska ske, ansågs det att tiden för lagringen måste vara sådan att det blir möjligt för de brottsbekämpande myndigheterna att använda de lagrade uppgifterna.

Sammanfattningsvis bedömdes därför en lagringstid om sex månader uppfylla EU-domstolens krav på att tiden ska begränsas till vad som kan anses strikt nödvändigt.

4.4.5 Säkerheten för lagrade uppgifter

4.4.5.1 Skyddsregler och utplåning av uppgifter

EU-domstolen fann i sin dom att direktivets regler om skydd för lagrade uppgifter var otillräckliga på flera punkter (se punkterna 66 och 67 i domen). Domstolen konstaterade att artikel 7 inte ställde upp säkerhetskrav anpassade till (i) den stora mängd data som ska lagras enligt direktivet, (ii) uppgifternas känsliga natur eller (iii) risken för att uppgifterna kommer i orätta händer, på ett sätt som kan sägas garantera att uppgifterna hålls konfidentiella. Inte heller hade medlemsstaterna förpliktats att själva föreskriva en sådan ordning. Domstolen fann vidare att artikel 7, läst tillsammans med artikel 4.1 i direktiv 2002/58 samt artikel 17.1 i direktiv 95/46, inte ställde krav på att en särskilt hög säkerhetsnivå upprätthålls hos leverantörerna vad gäller tekniska och organisatoriska åtgärder. Detta eftersom leverantörerna tilläts att ta ekonomiska hänsyn vid bestämmandet av lämplig säkerhetsnivå. Dessutom framhöll domstolen att direktivet inte ställde något absolut krav på att uppgifterna utplånas vid slutet av lagringstiden.

I analysen konstaterades inledningsvis att de svenska leverantörerna, genom regleringen i 6 kap. 3 a § LEK som tar sikte enbart på uppgifter lagrade enligt 16 a § samma kapitel, har en skyldighet att vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda uppgifterna, utan att de i den bedömningen tillåts ta några ekonomiska hänsyn. Den kritik EU-domstolen riktade mot direktivet i det hänseendet bedömdes därför inte relevant för den svenska regleringen.

Vidare kunde det konstateras att 37 § förordningen om elektronisk kommunikation har utformats i mycket nära anslutning till artikel 7 i direktivet. Det ansågs mot den bakgrunden, med hänsyn till EU-domstolens uttalanden, kunna ifrågasättas om enbart regleringen i 6 kap. 3 a § LEK och 37 § i förordningen ställer upp ett tillräckligt preciserat skydd för de lagrade uppgifterna. I den delen beaktades dock även de krav som följer av de föreskrifter som har meddelats av PTS. Det framhölls att dessa föreskrifter är detaljerade och de reglerar såväl frågor om behörighet och åtkomst som om fysiskt skydd för den utrustning som används för att lagra uppgifterna. De reglerar även i detalj frågor om loggning, som gör det möjligt att i efterhand se vem som haft tillgång till lagrade upp-

gifter, samt säkerhetskopiering. Sammantaget ansågs detta inte kunna leda till någon annan slutsats än att det skydd som i Sverige regleras genom lag, förordning och myndighetsföreskrifter är betydligt mer omfattande och mer detaljerat än vad som följde av direktivets krav. Det påpekades också att skyddsnivån är betydligt högre och skyddsreglerna mer preciserade än när det gäller de uppgifter leverantörerna har tillstånd att lagra med stöd av direktiv 2002/58. Utifrån de kriterier domstolen lyfte fram bedömdes de svenska regler som ska säkerställa skyddet för de lagrade uppgifterna vara tillräckligt strikta och precisa.

I analysen framhölls också att bestämmelsen i 6 kap. 16 d § LEK ställer krav på leverantörerna att utplåna uppgifterna vid lagringstidens utgång eller, om en begäran om utlämnande inkommit men inte hunnit behandlas, så fort uppgifterna har lämnats ut.

När det däremot gäller det fortsatta bevarandet hos de brottsbekämpande myndigheterna av uppgifter som lämnats ut noterades att det av naturliga skäl inte finns någon bestämd frist föreskriven för hur länge uppgifterna får bevaras. Det påpekades dock att frågan om utplåning av uppgifter från hemlig övervakning inte är oreglerad, utan bestämmelser om detta finns i främst 27 kap. 24 § rättegångsbalken och 9 § inhämtningslagen. Det framhölls också att det av Europadomstolens praxis följer att förstörandet av material från hemliga tvångsmedel innan en rättegång är avslutad i vissa fall kan kränka den misstänktes rätt till en rättvis rättegång (se Europadomstolens domar i målen *Natunen mot Finland*, nr 21022/04, och *Janatuinen mot Finland*, nr 28552/05, vilka båda avsåg material som inhämtats vid hemlig avlyssning). Ett krav på utplåning av uppgifterna vid en viss bestämd tidpunkt, utan att hänsyn tas till var i processen ett ärende befinner sig, bedömdes därför kunna kränka den misstänktes rätt till en rättvis rättegång enligt artikel 47 i rättighetsstadgan och artikel 6 i Europakonventionen. Med hänsyn härtill ansågs det uteslutet att EU-domstolen kunde ha menat att det även borde finnas regler om utplåning av lagrade trafikuppgifter vid lagringstidens slut hos de brottsbekämpande myndigheterna.

Sammanfattningsvis bedömdes att regleringen i 6 kap. 16 d § LEK om utplåning av uppgifter vid lagringstidens slut hos leverantören uppfyller de krav på ett sådant oåterkalleligt förstörande av uppgifterna som EU-domstolen efterlyste.

4.4.5.2 Krav på lagring inom EU

EU-domstolen pekade i sin dom på att datalagringsdirektivet inte krävde att uppgifterna lagras inom unionen. Detta innebar enligt domstolen att den oberoende myndighetskontrollen av att skydds- och säkerhetskraven för de lagrade uppgifter följs – vilken föreskrivs i artikel 8.3 i stadgan – inte fullt ut kunde anses vara garanterad (punkt 68). Enligt domstolen är en sådan kontroll en grundläggande beståndsdel i skyddet för enskilda individer i samband med behandlingen av personuppgifter.

I analysen framhölls att det mot bakgrund av domstolens uttalanden om intresset av effektiv tillsyn finns mycket som talar för att det bör införas ett krav på att lagringen av uppgifter ska ske inom EU eller EES. I den bedömningen beaktades också risken för s.k. ändamålsglidning, dvs. att uppgifter som lagras för ett visst ändamål kommer till användning i annan verksamhet eller för andra ändamål. Det konstaterades att en leverantör som väljer att lagra uppgifter i en server på en annan stats territorium kan tvingas att lämna ut dessa till utländska myndigheter i enlighet med lagstiftningen i lagringslandet. Det ansågs därför inte kunna uteslutas att uppgifter som lagras med stöd av svensk lagstiftning enbart för ändamål som rör bekämpning av vissa närmare avgränsade typer av brott skulle kunna komma till användning i annan verksamhet eller för bekämpning av annan brottslighet. Ett rimligt antagande ansågs vara att riskerna för sådan ändamålsglidning generellt sett torde öka om lagringen sker i ett tredje land jämfört med om den sker inom EU eller EES.

Samtidigt konstaterades i analysen att en reglering som innebär att leverantörerna förbjuds att överföra uppgifter för lagring i ett tredje land skulle komma i konflikt med den generella regleringen på detta område, främst kommissionens beslut om adekvat skyddsnivå (se avsnitt 3.2.5.1). Det bedömdes dock att medlemsstaterna ändå kan rättfärdiga ett överföringsförbud med hänvisning till att den aktuella lagringen till sin art, omfattning och varaktighet innefattar ett så långtgående ingrepp i enskildas personliga integritet att kraven på säkerhet vid lagringen förutsätter att uppgifterna inte förs över till ett tredje land.

4.4.6 Samlad bedömning

Sammanfattningsvis framhölls att slutsatserna i analysen innebär att det kan finnas skäl att närmare överväga några frågor. Det gäller dels lagringsskyldigheten avseende ett par uppgiftskategorier, dels reglerna om tillsyn såvitt avser inhämtning av abonnemangsuppgifter och reglerna om en oberoende kontroll såvitt gäller inhämtning av uppgifter i underrättelseskedet. Vidare ansågs att det kan övervägas om ett uttryckligt förbud mot lagring utanför EU/EES bör införas.

Det betonades att dessa åtgärder skulle verka för att ytterligare stärka rättssäkerheten och integritetsskyddet i den svenska regleringen. Som nämnts ovan var dock den samlade bedömningen i analysen att det svenska regelverket avseende lagring enligt 6 kap. 16 a–f §§ LEK samt övriga bestämmelser om tillgång och behandling av sådana uppgifter, även utan sådana åtgärder och med beaktande av EU-domstolens uttalanden, inte strider mot unionsrätten eller europarätten.

4.5 Reaktioner på domen

4.5.1 Reaktioner i Sverige

4.5.1.1 Inledande reaktioner på domen

I nära anslutning till att EU-domstolens dom offentliggjordes meddelade flera leverantörer av elektroniska kommunikationstjänster och kommunikationsnät i Sverige att de gjorde bedömningen att den svenska lagstiftning som genomför direktivet står i strid med EU-rätten och att de därför avsåg att upphöra med lagringen av uppgifter enligt 6 kap. 16 a § LEK. Några av dem gick också ut med information om att lagrade uppgifter skulle komma att raderas. Ett par leverantörer begärde i anslutning till domen även besked från PTS om vilken bedömning myndigheten gjorde av domen. Många leverantörer vägrade också att tillämpa de föreskrifter om avgifter för utlämnande av uppgifter som PTS med stöd av 46 § förordningen om elektronisk kommunikation har beslutat ska gälla från och med den 1 januari 2014 (PTSFS 2013:5).

PTS informerade på sin hemsida på internet kort tid efter att domen hade meddelats att myndigheten ”i nuläget inte [kommer] att vidta några åtgärder utifrån datalagringsreglerna”.

4.5.1.2 Reaktioner efter analysen

Strax efter att analysen redovisades meddelade PTS leverantörerna att myndigheten utgick från att datalagringsreglerna skulle tillämpas. Trots det var det flera leverantörer som höll fast vid sin inställning att inte lagra uppgifter. PTS har därefter vidtagit tillsynsåtgärder. Bland annat har myndigheten förelagt flera leverantörer att lagra uppgifter för brottsbekämpande ändamål (beslut den 27 juni 2014, Dnr 14-4175, beslut den 1 oktober 2014, Dnr 14-4682 och beslut den 27 oktober 2014, Dnr 14-8147).

Av uppgifter som utredningen har inhämtat från polisen och PTS framgår att de flesta leverantörerna av elektroniska kommunikationstjänster och kommunikationsnät nu lagrar uppgifter enligt regleringen i LEK. Två av leverantörerna har emellertid överklagat PTS förelägganden till förvaltningsrätten. Hittills har förvaltningsrätten meddelat dom i ett av målen (Förvaltningsrättens i Stockholm dom den 13 oktober 2014 i mål nr 14891-14). I domen prövade förvaltningsrätten den svenska regleringens förenlighet med de aktuella fri- och rättigheterna i RF, Europakonventionen och rättighetsstadgan.

Förvaltningsrätten konstaterade inledningsvis i domen att den lagringsskyldighet som gäller enligt svensk rätt helt innefattar den lagringsskyldighet som datalagringsdirektivet föreskrev, och att den på några punkter går längre än direktivet. Förvaltningsrätten fann därför att de aktuella bestämmelserna om lagring i LEK och FEK innebär en inskränkning i rätten till respekt för privatlivet och skyddet för personuppgifter. Dessutom utgör enligt domstolen myndigheternas tillgång till uppgifterna ytterligare intrång i rättigheterna och att det mot bakgrund av den mängd uppgifter som lagras är fråga om ett betydande intrång. I likhet med EU-domstolen fann dock förvaltningsrätten att bestämmelserna om lagring inte kränker det väsentliga innehållet i de aktuella rättigheterna, att de motiveras av ett godtagbart ändamål – nämligen att bekämpa grov brottslighet

och bidra till den allmänna säkerheten – och att regleringen får anses vara ägnad att uppnå detta ändamål.

Domstolen prövade sedan om inskränkningarna kan anses vara proportionerliga utifrån fyra områden: omfattningen av lagringen, tillgången till de lagrade uppgifterna, lagringstiden och säkerheten för de lagrade uppgifterna.

När det gäller *omfattningen av lagringen* konstaterade förvaltningsrätten att den kritik som EU-domstolen riktat mot direktivet i den delen kan göras gällande även mot den svenska lagstiftningen. Förvaltningsrätten framhöll att, vid bedömningen av om lagringsskyldigheten går utöver vad som kan anses nödvändigt och proportionerligt, hänsyn ska tas till om lagringen skulle kunna begränsas utan att syftet med bestämmelserna går förlorat. Mot bakgrund av att det inte är möjligt att på förhand veta vilka personer som kan bli inblandade i allvarliga brott eller på vilka platser brott kan komma att begås, ansåg förvaltningsrätten att en sådan begränsning av lagringsskyldigheten skulle äventyra syftet med lagringen. Detsamma gällde enligt rätten en eventuell avgränsning till vissa kommunikationsslag, eftersom det inte är möjligt att i förväg känna till vilken utrustning som kommer att användas. Lagringsskyldighetens omfattning ansågs därför inte i sig gå utöver vad som är nödvändigt för att uppnå syftet med bestämmelserna. Förvaltningsrätten framhöll också att det måste göras en sammantagen bedömning av reglernas proportionalitet, och att lagringens omfattning måste ses mot bakgrund av hur bestämmelserna om tillgång till uppgifter är utformade, hur länge uppgifterna ska lagras samt säkerheten kring de lagrade uppgifterna.

Vad avser frågan om *tillgången till uppgifter* prövade förvaltningsrätten, på samma sätt som gjordes i analysen, de tre olika regelverk som reglerar tillgången, dvs. bestämmelserna om tillgång till abonnemangsuppgifter enligt LEK, bestämmelserna om hemlig övervakning av elektronisk kommunikation enligt rättegångsbalken och bestämmelserna i inhämtningslagen.

När det gäller regleringen i LEK konstaterade förvaltningsrätten att bestämmelserna i viss mån kan kritiseras eftersom inhämtningen inte förutsätter att uppgifterna gäller misstanke om allvarliga brott, att flera myndigheter kan få tillgång till uppgifterna utan att det sker någon förhandskontroll och att kretsen av myndighetspersoner som kan få tillgång till uppgifterna inte är begränsad. Enligt förvalt-

ningsrätten ska dock den kritik som EU-domstolen riktade mot direktivet i det avseendet ses mot bakgrund av den mängd uppgifter som skulle lagras enligt direktivet och som därmed kunde lämnas ut under otydliga och oprecisa former. Förvaltningsrätten framhöll att abonnemangsuppgifter i sig inte är lika integritetskänsliga som några av de övriga uppgifter som skulle lagras enligt direktivet. Behovet av en begränsning av tillgången till enbart allvarligare brottslighet, en begränsning av kretsen av myndighetspersoner som kan få tillgång till uppgifter samt behovet av förhandskontroll kunde därför inte anses vara lika starkt. Domstolen påpekade också att tillgången till abonnemangsuppgifter är av stor betydelse för utredning av internetrelaterade brott. Förvaltningsrätten fann mot den bakgrunden att inhämtningen enligt LEK uppfyller de krav som kan ställas på lagstiftningen utifrån proportionalitetsprincipen.

Vad därefter gäller tillgången enligt rättegångsbalken konstaterade förvaltningsrätten att de uppgifter som kan inhämtas enligt regleringen är integritetskänsliga eftersom det är möjligt att utifrån uppgifterna dra slutsatser kring en persons vanor och privatliv. Enligt förvaltningsrätten är dock tillgångsbestämmelserna i rättegångsbalken tydliga och precisa samt begränsade till vad som är strängt nödvändigt.

När det slutligen gäller bestämmelserna i inhämtningslagen konstaterade förvaltningsrätten – av samma skäl som när det gäller tillgång enligt rättegångsbalken – att de uppgifter som lagen ger tillgång till är integritetskänsliga. Det ansågs därför vara av särskild vikt att möjligheterna att få tillgång till uppgifterna inte går utöver vad som är strikt nödvändigt. Domstolen framhöll i det sammanhanget att den brottslighet som lagen är avsedd att användas mot är mycket allvarlig och att den med god marginal är att betrakta som sådan allvarlig brottslighet som angavs i direktivet. Behovet av att möjliggöra utredning kring sådan brottslighet utgör enligt domstolens mening godtagbara skäl för mer långtgående inskränkningar i den personliga integriteten än om det hade varit fråga om mindre allvarlig brottslighet. Den kritik som förvaltningsrätten ansåg kunde riktas mot inhämtningslagen rörde främst antalet personer som är behöriga att få tillgång till uppgifterna samt avsaknaden av förhandskontroll. I den delen konstaterade domstolen att antalet personer som är behöriga att få tillgång till uppgifter är begränsad på så sätt att beslutsfattaren ska vara en myndighetschef eller någon som fått

delegation av denne. Vad gäller förhandskontroll framhölls att en sådan i och för sig skulle medföra att risken för obefogad inhämtning skulle minska. Samtidigt konstaterade förvaltningsrätten att det ligger i sakens natur att underrättelseverksamhet kräver snabb tillgång till aktuella uppgifter och att en förhandskontroll skulle kunna riskera att fördröja denna tillgång. Slutligen påpekades även att SIN:s tillsyn över myndigheternas tillämpning av lagen utgör en ytterligare försäkran.

Sammantaget fann förvaltningsrätten att tillgångsbestämmelserna i såväl rättegångsbalken som inhämtningslagen är tydliga och precisa samt begränsade till vad som är strikt nödvändigt. Bestämmelserna bedömdes därför uppfylla de krav som kan ställas på lagstiftningen utifrån RF, Europakonventionen, EU:s rättighetsstadga och 2002 års direktiv om integritet och elektronisk kommunikation.

Förvaltningsrätten fortsatte sin prövning med att undersöka frågan om *lagringstiden*. I den delen framhölls inledningsvis att EU-domstolen inte hade anmärkt på en lagringstid om sex månader, utan vad som hade föranlett EU-domstolens kritik var i stället att direktivet inte ställde upp några kriterier för när en kortare respektive längre lagringstid kan godtas. Förvaltningsrätten konstaterade att enligt svensk rätt gäller samma korta lagringstid för alla typer av lagrade uppgifter och att en kortare lagringstid än sex månader inte kan anses meningsfull. För att kunna utreda brott måste myndigheterna enligt förvaltningsrätten ha en reell möjlighet att hinna inhämta relevanta uppgifter. Domstolen fann därför att bestämmelserna om lagringstiden i LEK är proportionerliga och att de uppfyller de krav som kan ställas på dem.

Därefter behandlade förvaltningsrätten frågan om *säkerheten för de lagrade uppgifterna*. Det noterades att det vid implementeringen av direktivet hade införts en bestämmelse i LEK som innebär att lagringsskyldiga leverantörer ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna. Domstolen framhöll att det framgår av förarbetena att bestämmelsen inte lämnar något utrymme för att bestämma säkerhetsnivån genom en avvägning mellan teknik, kostnader och risken för integritetsintrång (prop. 2010/11:46 s. 75). Det påpekades även att PTS föreskrifter om säkerheten bl.a. innebär att leverantörer ska vidta åtgärder för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring, mot otillåten lagring, behandling av eller tillgång till och

otillåtet avslöjande av uppgifterna. Leverantörerna ska även bedriva ett kontinuerligt och systematiskt säkerhetsarbete med beaktande av de särskilda risker som lagringsskyldigheten medför. Förvaltningsrätten ansåg därför att den svenska regleringen kring säkerheten för uppgifterna är mer omfattande och preciserad än motsvarande regler i datalagringsdirektivet, och att de också medför ett högre krav på skyddsnivå. Den korta lagringstiden ansågs dessutom medföra mindre risker för konkreta integritetsskador. Den kritik som EU-domstolen riktade mot direktivet kunde därför enligt förvaltningsrätten inte göras gällande mot de svenska reglerna. Vidare konstaterade domstolen att regleringen i LEK ställer krav på att uppgifterna ska utplånas efter utgången av lagringstiden.

Förvaltningsrätten noterade att det i svensk rätt saknas bestämmelser som reglerar frågan om var uppgifterna ska lagras. Frågan var därför om den oberoende myndighetskontrollen som föreskrivs i artikel 8.3 i EU:s rättighetsstadga kan garanteras samt om svensk rätt ger tillräckliga garantier för att säkerställa ett effektivt skydd mot riskerna för missbruk och otillåten tillgång eller användning av uppgifterna. I denna del konstaterade domstolen att leverantörerna ska uppfylla de höga krav som ställs på säkerheten oavsett var dessa väljer att lagra uppgifterna. Det framhölls att det ingår i PTS tillsynsansvar att leverantörerna följer LEK och de föreskrifter som har meddelats med stöd av lagen, samt att PTS har omfattande befogenheter för att säkerställa att leverantörerna gör detta. Förvaltningsrätten ansåg att dessa regler möjliggör en tillfredsställande oberoende myndighetskontroll av skyddet för personuppgifter och att de även utgör tillräckliga garantier, vilka säkerställer ett effektivt skydd mot riskerna för missbruk och otillåten tillgång eller användning av uppgifterna. Domstolen framhöll dock att en reglering om var uppgifter får lagras skulle förtydliga och i viss mån höja säkerheten för uppgifterna. Avsaknaden av en sådan reglering bedömdes emellertid inte medföra att säkerheten var så låg att lagringen borde upphöra.

Avslutningsvis gjorde förvaltningsrätten en *samlad bedömning* av den svenska regleringens proportionalitet. Domstolen påpekade att den funnit att tillgångs- och säkerhetsbestämmelserna, trots vissa svagheter, uppfyller de krav som proportionalitetsprincipen ställer. Den fråga som återstod var därför om lagringens omfattning är förenlig med de fri- och rättigheter som ska garanteras enskilda. Förvaltningsrätten beaktade att, även om den svenska regleringen

möjliggör en omfattande lagring, reglerna om tillgång och säkerhet är tydliga och precisa samt begränsade till vad som är strikt nödvändigt. Till detta kom enligt domstolen att lagringen är motiverad av det mycket angelägna behovet av att tillhandahålla de brottsbekämpande myndigheterna effektiva verktyg vid utredning av brott. Med beaktande av detta behov fann förvaltningsrätten att de inskränkningar som de aktuella bestämmelserna innebär i rätten till respekt för privatliv samt skydd för personuppgifter uppfyller proportionalitetskravet och är förenliga med RF, Europakonventionen, EU:s rättighetsstadga samt 2002 års direktiv om integritet och elektronisk kommunikation. Förvaltningsrätten avslog därför överklagandet.

Den aktuella leverantören har överklagat förvaltningsrättens dom till kammarrätten. En annan leverantör har också anmält till EU-kommissionen att Sverige begår fördragsbrott genom att fortsätta att genomdriva en lagstiftning om datalagring som står i strid med artiklarna 7 och 8 i stadgan.

4.5.2 Andra reaktioner

4.5.2.1 Uttalande från artikel 29-gruppen

Den 1 augusti 2014 antog den s.k. artikel 29-gruppen[2] ett uttalande med anledning av EU-domstolens dom om datalagringsdirektivet (14/EN/WP 220). I uttalandet konstaterades att nationell lagstiftning baserad på direktivet inte direkt påverkas av domen. Trots det uppmanade gruppen medlemsstaterna och EU:s institutioner att utvärdera domens konsekvenser för nationell lagstiftning och tillämpning av regler om datalagring. Det påpekades därvid att nationell lagstiftning måste stå i överensstämmelse med artikel 15(1) i direktiv 2006/24/EU, rättighetsstadgan och EU-rättens allmänna principer. Gruppen framhöll särskilt att nationella datalagringsregler bör utformas på ett sådant sätt att masslagring av alla typer av uppgifter undviks, och att lagringen i stället blir föremål för lämpliga differentieringar, begränsningar eller undantag. Enligt gruppen bör nationella myndigheters tillgång till lagrade uppgifter begränsas till det strikt nödvändiga vad gäller kategorier av uppgifter och personer som

[2] Se vidare om artikel 29-gruppen i avsnitt 6.3.1.

berörs. Vidare bör tillgången vara föremål för materiella och processuella villkor.

Slutligen framhölls i uttalandet att den nationella lagstiftningen bör erbjuda ett effektivt skydd mot risken för otillåten tillgång eller annat missbruk av uppgifter. Ett sådant system bör innehålla krav på att datalagringen kontrolleras av en oberoende myndighet som garanterar att EU:s dataskyddslagstiftning följs.

4.5.2.2 Danmark

I Danmark regleras skyldigheten att lagra uppgifter om elektronisk kommunikation i § 786 i retsplejeloven. Enligt den bestämmelsen är leverantörer av telenät och teletjänster skyldiga att registrera och bevara uppgifter om elektronisk kommunikation i ett år för att kunna användas vid utredning och lagföring av brott. Lagringsplikten gäller både tele- och internetkommunikation och omfattar upplysningar om vem som har haft kontakt med vem, däremot inte upplysningar om innehållet i meddelanden. Lagringspliktens omfattning definieras närmare i förordning och omfattar en rad olika uppgiftskategorier i fråga om fast och mobil telefoni, kommunikation med sms, ems och mms samt internettrafik och e-post (Bekendtgørelse nr. 988 af 28 september 2006 om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik [logningsbekendtgørelsen]).

De uppgifter om elektronisk kommunikation som leverantörerna är skyldiga att lagra är till största delen historiska trafikuppgifter. Det innebär enligt dansk rättspraxis att utlämnande av uppgifter kan ske med stöd av retsplejelovens regler om edition. Normalt krävs då att även förutsättningarna för ingrepp i meddelandehemligheten är uppfyllda. I vissa fall är det dock tillräckligt att enbart förutsättningar för edition föreligger. Det gäller i de fall det begärs uppgifter om vilka master en mobiltelefon har varit uppkopplad mot eller uppgifter om vem som varit brukare av en specifik internetadress vid en viss tidpunkt.

Enligt retsplejeloven är det endast polisen som kan få tillstånd till att göra ingrepp i meddelandehemligheten och därigenom få tillgång till uppgifter om historisk teletrafik (§ 780). De närmare förutsättningarna för sådana ingrepp framgår av § 781. För att ingrepp

ska få göras krävs enligt den bestämmelsen att det föreligger viss misstanke (misstankekravet) och ett behov av att göra ingreppet (behovskravet) samt att den brottslighet som utreds är av visst allvar (kriminalitetskravet). Sålunda krävs att det finns särskilda skäl (bestemte grunde) att anta att åtgärden kommer att ge upplysningar om meddelanden eller försändelser som har skickats till eller från en misstänkt, och att ingreppet kan antas vara av avgörande betydelse för utredningen. Det är vidare ett krav att utredningen avser ett brott som kan leda till fängelse i sex år eller mer eller uppsåtliga brott mot straffelovens kapitel 12 (brott mot statens självständighet och säkerhet) eller 13 (brott mot statsförfattningen och de översta statsmyndigheterna, terrorism m.m.). Möjligheten att göra ingrepp i meddelandehemlighet omfattar vidare ett antal särskilt uppräknade brott där behovet av en sådan möjlighet har ansetts vara särskilt stort. Det gäller bl.a. barnpornografibrott, koppleri och brott mot utlänningslagen (udlændingeloven). Gemensamt för de särskilt uppräknade brotten är att de har lägre straffskala än sex års fängelse.

Ett ingrepp i meddelandehemligheten kräver att åtgärden står i proportion till föremålet för ingreppet, sakens betydelse och den kränkning och olägenhet som ingreppet kan antas vålla den som ingreppet rör (§ 782). Vidare får ingrepp göras endast efter beslut av domstol, om inte situationen är sådan att ändamålet med åtgärden går förlorat om domstolens beslut avvaktas. I sådana fall ska åtgärden läggas fram inför domstol senast 24 timmar från verkställigheten av ingreppet (§ 783). Innan rätten beslutar i frågor om ingrepp i meddelandehemligheten ska en advokat utses för den som ingreppet rör. Advokaten ska ha möjlighet att yttra sig (§ 784).

Enligt retsplejelovens § 788 ska den som ingreppet riktas mot som huvudregel underrättas om åtgärden i efterhand. Detta gäller dock inte om underrättelsen skulle vara till skada för en utredning om brott som kan leda till ingrepp i meddelandehemligheten.

När det gäller reglerna om edition framgår av retsplejelovens § 804 att rätten, som ett led i utredningen av en lagöverträdelse som faller under allmänt åtal, kan förelägga en person som inte är misstänkt att visa upp eller ge in ett föremål som han eller hon har rådighet över. Förutsättningarna för ett sådant föreläggande är att det finns anledning att anta att föremålet antingen kan tjäna som bevis, bör beslagtas eller vid lagöverträdelsen har frånhänts någon som kan kräva det tillbaka. I motsats till reglerna om ingrepp i

meddelandehemligheten kräver editionsreglerna inte att lagöverträdelsen ska vara av någon viss svårhetsgrad. Beslut om edition fattas av domstol. Om ändamålet med åtgärden skulle gå förlorat om domstolen beslut avvaktas får dock polisen besluta om åtgärden (retsplejelovens § 806). Om den som beslutet riktas mot i ett sådant fall motsätter sig beslutet ska frågan snarast möjligt och inom 24 timmar läggas fram inför domstolen.

Säkerheten för lagrade uppgifter regleras i dansk rätt av persondataloven. Av lagen framgår att den registeransvariga ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda mot oavsiktlig eller otillåten förstörelse, förlust eller försämring av uppgifter samt mot obehörigt röjande, missbruk eller annan behandling i strid med lagen (§ 41 och 42). I lagens förarbeten förutsätts att dessa åtgärder, med hänsyn till aktuell teknisk nivå och de kostnader som är förknippade med åtgärderna, ska säkerställa en tillräckligt hög säkerhetsnivå i förhållande till de risker som behandlingen innebär och arten av de uppgifter som ska skyddas. Av lagen framgår också att personuppgifter bara får föras över till ett tredje land om landet i fråga säkerställer en tillräcklig säkerhetsnivå (§ 27). Bedömningen av om skyddsnivån är tillräcklig ska göras på grundval av samtliga omständigheter som påverkar överföringen, särskilt uppgifternas art, behandlingens syfte och varaktighet, ursprungslandet och det slutliga destinationslandet samt de rättsregler som tillämpas i det tredje landet. Enligt lagens § 55 utövar Datatillsynsmyndigheten (Datatilsynet) tillsyn över all personuppgiftsbehandling som omfattas av lagen. Myndigheten utövar sina befogenheter helt oberoende (§ 56).

Den 2 juni 2014 publicerade Danmarks justitieministerium en rapport där EU-domstolens dom och de danska datalagringsreglernas förhållande till EU-rätten analyserades grundligt (Saknr. 2014-6140-0620, dokument 1188632). Bakgrunden till rapporten var att det efter att domen meddelades hade rests frågor om huruvida de danska reglerna kan upprätthållas (se rapporten s. 19).

Inledningsvis noterades i rapporten att lagringsplikten enligt de danska reglerna tar sin utgångspunkt i det upphävda direktivet och att den således gäller samma typer av uppgifter och att syftet med lagringen är detsamma som enligt direktivet, dvs. att möjliggöra användning av uppgifterna vid utredning och lagföring av brott. Med utgångspunkt i EU-domstolens dom bedömde Justitieministeriet

därför att även de danska reglerna utgör ett ingrepp i rätten till privatliv och rätten till skydd för personuppgifter enligt artiklarna 7 och 8 i EU-stadgan. Vidare gjorde ministeriet bedömningen att lagringsplikten har ett legitimt ändamål och att majoriteten av reglerna är ägnade att uppnå detta ändamål.

Därefter gjordes en bedömning av om de danska reglerna kan anses tillräckligt avgränsade när det gäller lagringsskyldighetens omfattning, reglerna om tillgång till uppgifterna samt lagringstiden.

När det gäller *lagringspliktens omfattning* konstaterades att de danska reglerna i vissa avseenden går längre än vad direktivet krävde, t.ex. kräver dansk rätt att vissa uppgifter om mobiltelefonsamtal lagras vilket inte krävdes enligt direktivet. Det påpekades också att de danska reglerna, på samma sätt som reglerna i direktivet, är generella och utan någon form av begränsning som tar hänsyn till målet att bekämpa brott.

Såvitt avser *tillgången* till lagrade uppgifter framhöll Justitieministeriet att de materiella villkor som gäller för att ingrepp i meddelandehemligheten ska få göras innebär att viss misstanke ska föreligga (misstankekravet), att det ska finns ett behov av uppgifterna (indikationskravet) och att den brottslighet som utreds ska vara av viss svårhetsgrad (kriminalitetskravet). Det påpekades att kriminalitetskravet som huvudregel kräver att brottet har minst sex års fängelse i straffskalan, men att även en rad andra brott med lägre straffskala omfattas av möjligheten till ingrepp. Det framhölls därtill att ett ingrepp också förutsätter att åtgärden bedöms proportionerlig i det enskilda fallet.

Vidare konstaterades att inhämtning av historiska teleuppgifter kräver att förutsättningar för såväl ingrepp i meddelandehemligheten som edition föreligger. I rapporten påpekades att dansk rätt i dessa situationer innehåller en rad processuella förutsättningar som t.ex. krav på domstolsbeslut, krav på att det utses en advokat för den som ingreppet gäller samt krav på underrättelse till den enskilde i efterhand. Det påpekades också att det även vid inhämtning av andra uppgifter, där endast reglerna om edition gäller, finns processuella krav. Till exempel fattas beslut om edition som huvudregel av rätten på begäran av polisen.

Sammanfattningsvis konstaterades i rapporten att dansk rätt innehåller ett antal garantier avseende lagringen av uppgifter och tillgången till dessa. Särskilt vad gäller tillgången ansågs de danska

reglerna skilja sig väsentligt från det upphävda direktivet som till stor del lämnade regleringen av dessa frågor till medlemsstaterna.

När det sedan gäller *lagringstiden* hänvisades till de överväganden som gjorts när reglerna infördes. Det noterades att den bedömning som då hade gjorts var att en lagringstid om ett år inte går utöver vad som är nödvändigt med hänsyn till intresset av att förebygga, utreda och lagföra brott. Det framhölls också att dansk rätt även på denna punkt skiljer sig från det upphävda direktivet som överlät till medlemsstaterna att själva bestämma en lagringstid mellan sex månader och två år. Justitieministeriet bedömde mot den bakgrunden att Danmark på denna punkt har fastslagit en klar avgränsning i lag som är baserad på hänsyn till möjligheterna att bekämpa brott.

I rapporten noterades också att EU-domstolen riktat anmärkningar mot att datalagringsdirektivet, i fråga om säkerheten för de lagrade uppgifterna, inte innehöll tillräckliga garantier mot risken för missbruk och olovlig tillgång till uppgifterna. I den delen framhölls att dansk rätt kräver att tjänsteleverantörerna fastställer en säkerhetspolicy vilken som minimum ska säkerställa att det endast är en begränsad personkrets som kan få tillgång till uppgifterna för legitima ändamål och att obehörig lagring, bearbetning, tillgång eller utlämnande av uppgifter inte kan ske. Det påpekades också att leverantörerna ska följa persondatalovens bestämmelser om nödvändiga tekniska och organisatoriska säkerhetsåtgärder. Vidare påpekades att dansk rätt innehåller en skyldighet att radera eller anonymisera uppgifterna vid utgången av lagringstiden.

Vad avser EU-domstolens påpekande om att direktivet inte krävde att uppgifterna lagras inom EU framhölls i rapporten att dansk rätt innebär att personuppgifter får föras över till tredje land endast om det tredje landet säkerställer en adekvat skyddsnivå för uppgifterna, om förutsättningarna i § 27 stycke 3 i persondataloven är uppfyllda, om Datatillsynsmyndigheten har gett tillstånd till överföringen eller om överföringen görs i enlighet med ett avtal som bygger på sådana standardklausuler som godkänts av kommissionen.

I rapportens slutsatsavsnitt framhöll Justitieministeriet att de danska reglerna – på samma generella sätt som direktivet – omfattar alla personer, alla elektroniska kommunikationsmedel och alla trafikdata utan någon form differentiering, begränsning eller undantag som tar hänsyn till målet att bekämpa allvarlig brottslighet. Med

hänsyn till att EU-domstolens dom bygger på en samlad bedömning kunde denna omständighet enligt ministeriets uppfattning emellertid inte ensamt anses innebära att de danska reglerna står i strid med rättighetsstadgan. Det framhölls att de danska reglerna är klara och precisa och att de innehåller en rad väsentliga garantier som tar sikte på att effektivt skydda de lagrade uppgifterna mot missbruk och olovlig tillgång. Det påpekades också att dansk rätt, till skillnad från direktivet, innehåller flera materiella och processuella bestämmelser som reglerar tillgången till uppgifterna. Särskilt framhölls att tillgången sker enligt retsplejelovens regler om ingrepp i meddelandehemligheten och/eller edition, vilket medför att flera sådana materiella och processuella bestämmelser blir tillämpliga. Därutöver fastställer dansk rätt en lagringstid om ett år med skyldighet för leverantörerna att därefter radera eller anonymisera uppgifterna. På dessa grunder fann Justitieministeriet vid en samlad bedömning att det inte finns anledning att anta att de danska reglerna om lagring av och tillgång till uppgifter står i strid med rättighetsstadgans bestämmelser om rätt till privatliv och rätt till skydd för personuppgifter.

4.5.2.3 Finland

I Finland har ett lagstiftningsarbete nyligen genomförts vilket har inneburit bl.a. att ett stort antal bestämmelser som reglerar frågor om elektronisk kommunikation har samlats i en ny informationssamhällesbalk. Enligt den proposition som låg till grund för förslaget om balken (RP 221/2013 rd) skulle även det centrala innehållet i den finska datalagringsregleringen föras över i oförändrad form till den nya balken. Propositionen överlämnades emellertid till den finska riksdagen i tiden före EU-domstolens dom och innehåller därför inte några resonemang om finsk rätts förhållande till domen. När lagstiftningsärendet behandlades av den finska riksdagens kommunikationsutskott (KoUB 10/2014 rd) inhämtade utskottet ett utlåtande från grundlagsutskottet vilket däremot innehåller en analys av EU-domstolens dom och dess konsekvenser för den nationella regleringen (GrUU 18/2014 rd s. 4 ff.).

Grundlagsutskottet konstaterade inledningsvis i utlåtandet att det inte följer av domen att en fråga som berörs av ett ogiltigförklarat

direktiv inte kan vara föremål för nationell lagstiftning. Det framhölls dock att den nationella lagstiftningen i den aktuella situationen måste bedömas inte bara utifrån de nationella grundlagsbestämmelserna utan också med hänsyn till den i domen nämnda EU-stadgan om de grundläggande rättigheterna och dess bestämmelser om respekt för privatlivet (artikel 7) och skydd av personuppgifter (artikel 8). Enligt utskottet måste de anmärkningar som EU-domstolen gjorde läggas till grund för den konstitutionella bedömningen av de finska reglerna. Därmed måste också den nationella regleringen uppfylla de förutsättningar som nämns i domen, även om domen inte direkt gäller den nationella genomförandelagstiftningen. Det framhölls samtidigt att domen inte ger något direkt svar på hur den nationella lagstiftningen ska utformas för att uppfylla kraven på proportionalitet när det gäller privatlivet och personuppgifter. Man måste enligt utskottet dock utgå från att åtminstone sådana bestämmelser strider mot proportionalitetskravet som innebär omfattande, ospecificerad och långvarig lagring av uppgifter i kombination med att myndigheter har ospecificerad och obegränsad tillgång till uppgifterna. Den nationella lagstiftningen måste i vart fall ha betydligt mer exakta bestämmelser om begränsningar i fråga om förvaring och användning än vad som fanns i det ogiltigförklarade direktivet.

När det gäller *lagringsskyldighetens utformning* konstaterade utskottet att redan omfattningen av de uppgifter som lagras – samtliga personer, samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter – är problematisk med hänsyn till proportionaliteten. Utskottet ansåg dock att en reglering som avgränsar lagringsskyldigheten i fråga om såväl personkrets som innehåll i meddelanden uppenbarligen skulle vara mycket svårgenomförbar såväl innehållsmässigt som tekniskt. Utskottet menade också att domen inte direkt sätter hinder för en reglering där proportionalitetskraven tillgodoses på andra sätt. Vidare stod det enligt utskottet klart att intresset av att bekämpa allvarlig brottslighet är en grund som talar för bestämmelserna. Regleringen borde därför bedömas även i det perspektivet.

Utskottet konstaterade vidare att innehållet i lagringsskyldigheten inte längre kan anges genom en hänvisning till det ogiltigförklarade direktivet. De uppgifter som ska lagras måste därför specificeras i lagen. Utskottet påpekade därvid att det i lagförslaget måste preciseras vilka uppgifter som är nödvändiga med hänsyn till det bakomliggande syftet med regleringen, dvs. att undersöka, utreda

och åtalspröva allvarliga brott. Detta eftersom det inte ansågs kunna förutsättas att uppgifter som inte är nödvändiga för det syftet ska få lagras.

Såvitt avser *användningen* av de lagrade uppgifterna konstaterade utskottet att den finska lagstiftningen är klart mer exakt än direktivet. Utskottet beaktade i den delen att uppgifterna får användas endast för att undersöka vissa specificerade brott och att endast myndigheter som enligt någon annan lag har rätt att få uppgifterna har tillgång till dem. Den regleringen ansågs uppfylla domens krav på ett objektivt kriterium som gör det möjligt att begränsa antalet personer som är behöriga att få tillgång till och använda de lagrade uppgifterna och endast använda dem i samband med allvarliga brott. Utskottet anförde vidare att det, för att få tillgång till sådana teleövervakningsuppgifter som avses i tvångsmedelslagen och polislagen, krävs domstolstillstånd och att regleringen därför är problemfri även i den delen.

När det gäller *lagringstiden* konstaterade utskottet att den finska regleringen anger att uppgifterna ska lagras i tolv månader från den dag kommunikationen ägde rum, och att denna tid är kortare än den som direktivet tillät. Utskottet ansåg dock att det i ljuset av EU-domstolens dom är betänkligt att lagringstiden inte är specificerad utifrån den möjliga nytta som uppgifterna kan ge när det gäller att bekämpa allvarlig brottslighet. Grundlagsutskottet rekommenderade därför kommunikationsutskottet att bedöma lagringstiden för uppgifterna med hänsyn till lagens syfte och vid behov gradera lagringstiden för olika uppgifter i antingen tolv månader eller kortare tid.

Kommunikationsutskottet hänvisade i sitt betänkande i stora delar till grundlagsutskottets utlåtande. Utskottet framhöll dock för egen del att skyldigheten att lagra uppgifter för myndigheternas behov endast ska gälla företag som anges genom särskilt beslut av inrikesministeriet. Enligt utskottets uppfattning minskar detta förslag sannolikt antalet lagringsskyldiga teleföretag, vilket samtidigt minskar mängden uppgifter som måste lagras. Vidare framhöll utskottet att lagringsplikten endast gäller sådana uppgifter som teleföretagen också annars lagrar för sina egna behov, t.ex. för att säkerställa att fakturor är korrekta, och att lagringsplikten i första hand säkerställer att uppgifterna finns tillgängliga under längre tid än vad som annars skulle ha varit fallet. Utskottet konstaterade därför att

lagförslaget ställer upp väsentligt strängare krav och förbehåll för lagringen av uppgifter än vad det ogiltigförklarade direktivet gjorde.

Kommunikationsutskottet menade vidare att det fortfarande finns ett klart och vägande samhälleligt behov av att för myndigheternas behov lagra uppgifter om kommunikation. Det påpekades att kommunikationsnäten och användningen av olika kommunikationsmedel utgör en väsentlig del av människornas vardag och samhället i stort. Utskottet anförde att uppgifter om kommunikation därför oundvikligen har en central roll för myndigheternas förutsättningar att bedriva brottsutredning. Utskottet såg det som nödvändigt att säkerställa att i synnerhet uppgifter som är oumbärliga i polisverksamhet och brottsutredningar fortsatt måste lagras.

När det gäller lagringsskyldighetens omfattning framhöll utskottet att de uppgifter som ska lagras måste preciseras i lag och att det i detta sammanhang måste bedömas vilka av de uppgifter som är nödvändiga med hänsyn till det bakomliggande syftet med regleringen, dvs. att undersöka, utreda och åtalspröva allvarliga brott. Kommunikationsutskottet menade därvid att vissa uppgifter, utifrån tillgänglig utredning, inte kunde anses nödvändiga för utredning av brott eller åtalsprövning. Detta ansågs gälla telefonitjänster i fasta nät (s.k. trådtelefon), e-posttjänster, tilläggstjänster, EMS-tjänster eller multimedietjänster i mobilnät. Utskottet föreslog därför att skyldigheten att lagra uppgifter för myndigheternas behov i fortsättningen ska gälla endast uppgifter som avser mobilnätets telefonitjänster och SMS-tjänster, internettelefonitjänster och internetaccesstjänster. Vidare föreslog utskottet att de uppgifter från respektive tjänst som ska lagras specificeras i en uttömmande förteckning i förordning eller myndighetsföreskrifter.

Kommunikationsutskottet gjorde också, utifrån viss statistik angående åldern på utlämnade uppgifter under 2013, en bedömning av möjligheterna att gradera lagringstiden för olika uppgifter i antingen tolv månader eller kortare tid. Med ledning av den bedömningen föreslog utskottet att lagringstiden införs stegvis så att uppgifter som avser telefonitjänster och textmeddelandetjänster i mobilnät ska lagras i tolv månader, uppgifter om internetaccesstjänster i nio månader och internettelefonitjänster i sex månader räknat från det att kommunikationen inleddes. Det framhölls i betänkandet att utskottet också hade diskuterat och bedömt möjligheten att införa ännu kortare förvaringstider. Utskottet betonade

dock att teleföretagen redan nu lagrar uppgifter för egna behov så länge att kortare, enhetligare förvaringstider skulle ändra och försämra balansen mellan regleringens fördelar och nackdelar.

Vidare pekade utskottet på att regeringen föreslagit att lagringsskyldiga företag i fortsättningens ska få registrera också förmedlingsuppgifter och andra uppgifter, till exempel uppgifter som uppkommit genom bläddring av webbsidor, om det är nödvändigt för identifiering av en användare av internetaccesstjänster, elektroniska posttjänster eller internettelefonitjänster. Utskottet konstaterade att motiven till detta förslag pekar på praktiska, med brottsutredning förknippade behov som i sig är relevanta. Trots det ansåg utskottet att det inte är möjligt att efter unionsdomstolens avgörande godkänna att nuvarande lagringsskyldighet utvidgas till den typen av internetbaserade uppgifter. Utskottet föreslog därför att den föreslagna bestämmelsen stryks. Behovet av en sådan bestämmelse och möjligheterna att verkställa den kunde enligt utskottet bedömas senare i samband med uppföljningen av konsekvenserna av propositionen.

Slutligen föreslog kommunikationsutskottet att riksdagen godkänner följande uttalande:

> Riksdagen förutsätter att det tillsätts en arbetsgrupp för utvärdering av regleringen av lagring av förmedlingsuppgifter för myndigheternas behov. Arbetsgruppen ska göra en heltäckande utredning av vilka myndighetsbehoven är, om lagringen av uppgifterna och om frågor som hänför sig till integritetsskyddet i samband med lagringen. Utifrån utredningen ska behovet av eventuella ändringar av bestämmelserna bedömas och vid behov utformas ändringsförslag utan onödiga dröjsmål.

Den 15 oktober 2014 godkände riksdagen slutligt förslagen enligt kommunikationsutskottets betänkande.

4.5.2.4 Norge

Norge är inte medlem i EU. Däremot är landet anslutet till avtalet om det europeiska ekonomiska samarbetsområdet (EES-avtalet) vilket syftar till att utvidga EU:s inre marknad till att även omfatta länder i Europeiska frihandelssammanslutningen (Efta). För att EU-rättsakter ska bli bindande för avtalsparterna krävs att lagstiftningen införlivas i avtalet genom att den inkluderas i förteckningen

över protokoll och bilagor till avtalet. För detta ändamål finns en gemensam EES-kommitté som består av företrädare för EU och de tre Efta-länderna Norge, Island och Schweiz. Kommittén har bl.a. i uppgift att granska nya EU-rättsakter om den inre marknaden och besluta i frågor om vilken lagstiftning som ska införlivas i EES-avtalet(se artikel 98 i avtalet), vilket sker genom enhälligt beslut i kommittén (artikel 93.2). Flera tusen akter har på detta sätt införlivats i avtalet. Något beslut om att införliva datalagringsdirektivet har dock inte fattats.

Trots detta lade Norges regering år 2010 fram ett lagförslag till stortinget som syftade till att genomföra datalagringsdirektivet i norsk rätt (prop. 49 L [2010-2011]). Stortinget antog lagförslagen i april 2011 och regleringen skulle därmed ha trätt i kraft under april 2012 (Lovvedtak 46 [2010-2011]). Ikraftträdandet har dock skjutits upp flera gånger, bl.a. i avvaktan på EU-domstolens dom. Sedan domen meddelades har den norska regeringen uttalat att den avser att grundligt gå igenom domen (se t.ex. prop. 1 S [2014-2015] s. 75). Enligt uppgifter i norsk media har statsminister Erna Solberg också uppgett att arbetet med implementeringen har lagts på is tills vidare, men att regeringen har för avsikt att återkomma till stortinget med ett nytt lagförslag vid ett senare tillfälle.[3]

4.5.2.5 Österrike

I Österrike reglerades skyldigheten att lagra uppgifter om elektronisk kommunikation i 102 a § i telekommunikationslagen (Telekommunikationsgesetz 2003, TKG 2003). Enligt den bestämmelsen skulle leverantörer av allmänna kommunikationstjänster lagra uppgifter om användarnas kommunikation i sex månader från det att kommunikationen avslutades.

Den 27 juni 2014 förklarade Österrikes författningsdomstol (Verfassungsgerichtshof) att de österrikiska reglerna om datalagring, samt vissa regler om de brottsbekämpande myndigheternas tillgång till sådana uppgifter, stod i strid med Österrikes dataskyddslag, vilken har konstitutionell status (mål G 47/2012-49 m.fl.). Dom-

[3] Dagbladet, 2014-04-11, Regjeringen legger DLD-arbeidet på is, http://www.dagbladet.no/2014/04/11/nyheter/samfunn/politikk/overvaking/dld/32780686/

stolen konstaterade i domen att reglerna om datalagring och de brottsbekämpande myndigheternas tillgång till datalagrade uppgifter innebär intrång i rätten till skydd för personuppgifter enligt dataskyddslagen. Samtidigt påpekade domstolen att dessa regler syftar till att uppnå mål som nämns i artikel 8 i Europakonventionen och att intresset av att uppnå dessa mål väger tungt. Domstolen framhöll dock att gränserna för möjligheterna att inskränka skyddet för personuppgifter är snävare definierat i dataskyddslagen än i artikel 8 i Europakonventionen. Dataskyddslagen tillåter nämligen att intrång görs bara om det är nödvändigt för att skydda ett tyngre vägande legitimt intresse. Uppgifter som till sin natur är särskilt skyddsvärda får därutöver användas bara för att skydda viktiga allmänna intressen och att det i lag föreskrivs tillräckliga skyddsmekanismer som ska syfta till att skydda individens intresse av konfidentialitet. Enligt författningsdomstolen innebär dessa regler att den proportionalitetsbedömning som ska göras enligt Österrikes dataskyddslag är striktare än den som krävs enligt artikel 8 i Europakonventionen.

Författningsdomstolen prövade därefter om reglerna om tillgång till datalagrade uppgifter kunde anses leva upp till konstitutionens krav. Domstolen konstaterade att, enligt en bestämmelse i straffprocesslagen, utlämnande av uppgifter var tillåtet bl.a. om det kunde främja utredningen av ett uppsåtligt brott som kan leda till fängelse i mer än ett år. Sådana utlämnanden skulle begäras av åklagaren baserat på ett tillstånd av domstol, vilket kunde överklagas av rättsskyddsombudet (Rechtsschutzbeauftragter). Domstolen framhöll i den delen att det i och för sig är möjligt för lagstiftaren att knyta möjligheten att få tillgång till lagrade uppgifter till brottens straffskalor, men detta kräver enligt domstolen att lagstiftningen också innehåller bestämmelser som säkerställer att brottets allvar i det enskilda fallet är sådant att det rättfärdigar ett intrång i de konstitutionella rättigheterna. Enligt domstolen var den aktuella bestämmelsen alltför onyanserad i det avseendet, eftersom möjligheten att få tillgång till uppgifter inte var begränsad till brott som antingen leder till höga straff eller vars lösning med nödvändighet kräver tillgång till datalagrade uppgifter. Domstolen ansåg därför att den inte kunde garanteras att den aktuella bestämmelsen bara används i sådana fall där det är nödvändigt för ändamål som anges i artikel 8 i Europakonventionen. Bestämmelsen bedömdes därför vara oproportionerlig och därmed oförenlig med konstitutionen.

Vidare konstaterade domstolen att säkerhetsmyndigheter under vissa förutsättningar kunde få tillgång till uppgifter om namn och adress för en användare som tilldelats en ip-adress vid en specifik tidpunkt, om uppgiften behövdes för att myndigheten skulle kunna motverka en konkret fara som hotar en individs liv, hälsa eller frihet eller om den behövdes för att avvärja en allvarlig attack eller en kriminell sammanslutning. Domstolen noterade att säkerhetsmyndigheterna kunde få tillgång till dessa uppgifter utan domstolsprövning. Däremot krävdes att rättsskyddsombudet skulle underrättas så fort som möjligt. Vidare konstaterades att bestämmelsen saknade begränsningar relaterade till allvaret i en förestående händelse. Även denna reglering bedömdes därför vara oproportionerlig. Domstolen framhöll att den bedömningen inte förändrades av det faktum att reglerna endast gav säkerhetsmyndigheterna tillgång till uppgifter om namn och adress.

Vad därefter gäller själva lagringsplikten konstaterade författningsdomstolen inledningsvis att lagringen omfattade en stor del av Österrikes befolkning, och att den nästan uteslutande träffade enskilda individer som inte agerat på ett sätt som skulle ha kunnat rättfärdiga att deras uppgifter lagrades. Domstolen slog vidare fast att, även om innehållet i kommunikationen inte sparades, det inte kunde uteslutas att de lagrade uppgifterna skulle kunna användas för att dra slutsatser om enskilda som står i strid med den konstitutionella rätten till skydd för personuppgifter. I det sammanhanget beaktades även att antalet leverantörer av kommunikationstjänster med tillgång till lagrade uppgifter är stort, och att den österrikiska lagstiftningen, även om den innehöll skyddsbestämmelser som gick utöver vad datalagringsdirektivet krävde, inte innehöll något straffrättsligt skydd mot missbruk av uppgifterna. Vidare beaktades att det hade framkommit att varken Dataskyddskommissionen eller Dataskyddsmyndigheten hade gjort några kontroller för att säkerställa att skyddsreglerna efterlevs under den tid som regleringen hade varit i kraft. Domstolen tog också hänsyn till att de individer, vars uppgifter sparades utan att de gett någon anledning till det, inte hade någon möjlighet att utöva sin rätt enligt dataskyddslagen att kräva att uppgifterna raderades. Enligt domstolen var reglerna i det avseendet inte tillräckligt specificerade för att leva upp till dataskyddslagens krav. Domstolen ansåg också att det var oklart om skyldigheten att radera uppgifter efter lagrings-

tidens slut innebar att uppgifterna måste utplånas rent fysiskt, eller om den endast innebar att vidare tillgång till uppgifterna skulle förhindras.

Slutligen framhöll författningsdomstolen särskilt att skyldigheten att lagra uppgifter helt skulle förlora sin mening i och med att domstolen funnit att reglerna om de brottsbekämpande myndigheternas tillgång till de lagrade uppgifterna skulle upphävas. Att lagra uppgifter utan ett specifikt syfte skulle enligt domstolen under alla förhållanden vara oförenligt med konstitutionen. Mot den bakgrunden fastslog domstolen att även reglerna om lagringsskyldigheten var oproportionerliga.

4.5.2.6 Nederländerna[4]

I Nederländerna regleras skyldigheten att lagra uppgifter om elektronisk kommunikation i telekommunikationslagen (Telecommunicatiewet). Enligt lagen ska leverantörer av allmänna telekommunikationsnät och telekommunikationstjänster lagra uppgifter som genereras eller behandlas i verksamheten för att dessa ska kunna användas vid utredning och åtal av allvarliga brott. Lagringsperioden är ett år för uppgifter om fast och mobil telefoni samt för uppgifter om vissa former av internettelefoni. För andra uppgifter om internetanvändning är lagringsperioden sex månader. De uppgiftskategorier som ska lagras överensstämmer med de som skulle lagras enligt datalagringsdirektivet.

De brottsbekämpande myndigheternas tillgång till uppgifter som lagras regleras i straffprocesslagen (Wetboek van Strafvordering). Enligt den lagstiftningen har åklagare (officier van justitie) befogenhet att begära trafikuppgifter, under förutsättning att det föreligger antingen misstanke om ett brott som kan leda till häktning eller en rimlig misstanke om att ett allvarligt lagbrott planeras eller utförs i organiserade former. Vid sidan av åklagare får även utredare begära så kallade användaruppgifter, dvs. uppgifter om namn, adress, plats,

[4] Den 11 mars 2015 ogiltigförklarade en distriktsdomstol i Haag de nederländska datalagringsreglerna (Rechtbank Den Haag, C09/480009/KG ZA 14/1575). I skrivandets stund är det fortfarande möjligt att överklaga domen (se t.ex. http://blogs.wsj.com/digits/2015/03/11/dutch-court-strikes-down-countrys-data-retention-law/). Eftersom domen meddelades först i samband med att detta betänkande lämnades till tryck har vi inte haft möjlighet att göra någon analys av domen i betänkandet.

nummer och typ av tjänst. Befogenheten att begära sådana uppgifter är inte begränsad till utredningar om allvarliga brott, däremot krävs att det föreligger antingen misstanke om brott eller en rimlig misstanke om att brott planeras eller utförs i organiserade former.

Vidare finns vissa särskilda befogenheter när det gäller kontraterrorism. Enligt dessa regler får åklagare begära ut trafikuppgifter i de fall där det finns indikationer på ett terroristbrott. Vid sidan av åklagare får även utredare begära ut användaruppgifter. Under en förberedande utredning som bedrivs med målet att förbereda för en förundersökning om terroristbrott, har åklagare också befogenhet att begära ut datafiler från allmänna och privata institutioner i syfte att söka efter vissa handlingsmönster hos individer som är av betydelse vid bekämpning av terrorism. Denna befogenhet, som kräver godkännande av en domare, gäller generellt och kan således användas även mot leverantörer av elektroniska kommunikationstjänster.

Säkerheten för de uppgifter som lagras enligt de nederländska reglerna regleras av dataskyddslagen (Wet bescherming persoonsgegevens) och telekommunikationslagen. Denna reglering kräver att leverantörerna vidtar lämpliga tekniska åtgärder för att skydda de lagrade uppgifterna från otillåten användning, för att säkerställa att tillgång till uppgifterna bara ges till särskilt utsedda personer och för att se till att uppgifterna omedelbart raderas efter lagringstidens utgång. Personuppgifter som lämnas ut till polisen ska behandlas i enlighet med polisdatalagen (Wet politiegegevens). Kontrollen över att skyddsreglerna följs utövas av Telekommyndigheten (Agentschap Telecom) och av Konsument- och marknadsmyndigheten (Autoriteit Consument en Markt) i samarbete med Dataskyddsmyndigheten (College bescherming persoonsgegevens).

Den 17 november 2014 överlämnade Nederländernas dåvarande säkerhets- och justitieminister Ivo Opstelten en skrivelse till det nederländska parlamentet.[5] I skrivelsen redogjorde ministern för regeringens analys av konsekvenserna av EU-domstolens dom för det nationella regelverket om lagring av uppgifter om elektronisk kommunikation. Inledningsvis framhölls i analysen att EU-domstolens dom inte innebär att den nederländska lagstiftningen på området är ogiltig. Däremot påpekades att reglerna måste stå i överensstämmelse med de grundläggande rättigheterna till skydd för

[5] Referensnummer 586638.

privatliv och personuppgifter enligt den nya tolkning som dessa rättigheter har fått genom domen. Regeringen framhöll dock även att tvingande regler om datalagring är ett oumbärligt verktyg vid utredning och åtal av allvarliga brott.

När det gäller *lagringsskyldighetens omfattning* noterades att datalagringsreglerna syftar till att säkerställa att historiska uppgifter om elektronisk kommunikation finns tillgängliga, om det i efterhand visar sig att sådana uppgifter är relevanta för utredning och åtal för brott. Eftersom det inte är möjligt att på förhand skilja mellan misstänkta och icke misstänkta individer, bedömdes det nödvändigt att lagringsskyldigheten omfattar samtliga personers trafikuppgifter. Enligt regeringens uppfattning borde EU-domstolens kritik av direktivet i den delen, d.v.s. att direktivet träffar alla personer utan begränsningar i förhållande till syftet att bekämpa brott, tolkas i sitt sammanhang. Regeringen fastslog därvid att domen inte kan tolkas så att samtliga omständigheter som domstolen tog upp måste vara uppfyllda i nationell rätt för att kravet på proportionalitet ska kunna anses tillgodosett. I sådana fall skulle det ha varit tillräckligt för domstolen att konstatera att direktivet föreskrev lagring av samtliga personers uppgifter – utan begränsningar i förhållande till syftet att bekämpa brott – för att komma till slutsatsen att direktivet var ogiltigt. Regeringen framhöll att domstolen i stället gjorde en samlad bedömning av samtliga omständigheter som togs upp i domen. Enligt regeringens mening borde domen därför uppfattas på så sätt att domstolen ansett att det faktum, att direktivet inte krävde en koppling mellan den person vars uppgifter lagras och ett allvarligt brott, visserligen kan innebära ett allvarligt ingrepp i rätten till privatliv, men att allvaret i detta ingrepp kan vägas upp genom tillräckliga garantier och skyddsmekanismer när det gäller metoderna för lagring, behandling och tillgång till uppgifterna.

Vad därefter gäller *lagringstiden* framhölls i analysen att syftet med datalagringsregleringen är att vissa uppgifter om elektronisk kommunikation måste finnas tillgängliga för utredning av allvarliga brott. Ett krav på differentiering av lagringstiden för varje enskild uppgiftskategori bedömdes vara oförenligt med detta syfte, eftersom man inte på förhand kan veta för vilken typ av brottslighet som en viss uppgift eventuellt kommer att begäras ut. Regeringen fann därför att reglerna om lagringstiden borde kvarstå oförändrade. EU-domstolens krav på att lagringstiden ska styras av ett

objektivt kriterium som relaterar till syftet att bekämpa brott bedömdes i stället kunna tillgodoses på andra sätt. Regeringen framhöll att en möjlighet till differentiering skulle kunna vara att den tidsperiod, under vilken de brottsbekämpande myndigheterna har möjlighet att få tillgång till uppgifterna görs olika lång beroende på allvaret i det brott som utreds.

När det sedan gäller regleringen av *tillgången till uppgifter* framhöll regeringen att denna fråga redan är strikt reglerad i nederländsk rätt. Det konstaterades att, till skillnad från regleringen i direktivet, möjligheterna att få tillgång till trafikuppgifter är begränsade till fall som gäller allvarliga brott. Regeringen uttalade dock att den, med anledning av EU-domstolens dom, har för avsikt att föreslå några nya skyddsåtgärder i syfte att ytterligare begränsa tillgången. För det första anförde regeringen att det ska införas ett system för differentiering av den tidsperiod under vilken myndigheter kan få tillgång till uppgifter. Detta system kommer enligt regeringen att syfta till att hela lagringsperioden används endast vid de allvarligaste kategorierna av brottslighet som också har de strängaste straffen. I fråga om andra brott, där myndigheterna i och för sig kan begära uppgifter men som inte har lika stränga straff, ska möjligheten att få ut uppgifter gälla under en kortare tidsperiod.

För det andra anförde regeringen att ett system med rättslig prövning kommer att föreslås, i syfte att i högre grad säkerställa att lagrade uppgifter bara används i sådana situationer där det finns tillräcklig anledning till det. Enligt regeringen kommer straffprocesslagen därför att ändras på så sätt att en begäran om trafikuppgifter kommer att kräva förhandsgodkännande av en domare. Däremot ansåg regeringen att det inte finns anledning att ändra reglerna vad gäller möjligheten att begära s.k. användaruppgifter. I den delen beaktades att de uppgiftskategorierna är klart mer begränsade, och att det inte är möjligt att dra några slutsatser som rör privatlivet av uppgifterna. Regeringen ansåg därför att lagringen av dessa uppgifter måste bedömas annorlunda än lagringen av trafikuppgifter.

När det slutligen gäller *säkerheten för de lagrade uppgifterna* konstaterade regeringen att den nederländska lagstiftningen redan innehåller skyddsmekanismer och regler som innebär att de lagringsskyldiga leverantörerna måste vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten för de nätverk och tjänster som de tillhandahåller. Dessa åtgärder ska syfta till att

skydda uppgifterna mot förstöring, förlust, förändring och mot otillåten lagring, behandling, tillgång eller avslöjande. Vidare är leverantörerna skyldiga att se till att endast behöriga personer kan få tillgång till uppgifterna. Det framhölls att reglerna inte ger leverantörerna utrymme för att ta ekonomiska hänsyn vid utformningen av skyddet. Regeringen hänvisade även till en rapport, utgiven av näringsministern år 2013, av vilken det framgick att leverantörerna generellt sett följer säkerhetsreglerna. Mot den angivna bakgrunden ansåg regeringen att nederländsk rätt och dess tillämpning i huvudsak lever upp till EU-domstolens krav på säkerhet för uppgifter som lagras. Regeringen påpekade dock att de nederländska reglerna inte kräver att uppgifterna lagras inom EU, och att detta innebär att det inte fullt ut kan garanteras att Dataskyddsmyndigheten kan övervaka säkerheten och skyddet för uppgifterna. Regeringen uttalade att den därför har för avsikt att ändra regleringen så att leverantörerna blir skyldiga att lagra uppgifterna inom unionen.

5 Vilka uppgiftskategorier ska lagras?

5.1 Inledning

Enligt våra direktiv ska vi föreslå de förändringar som, utifrån analysen av datalagringsdomen och svensk rätt, bedöms lämpliga för att stärka skyddet för den personliga integriteten i förhållande till reglerna om lagring av uppgifter enligt 6 kap. 16 a–f §§ LEK och övriga bestämmelser om tillgång till och behandling av sådana uppgifter. I analysen gjordes bedömningen att det kan ifrågasättas om det finns behov av att lagra vissa av de uppgiftskategorier som lagras enligt dagens regler och att det finns anledning att analysera detta närmare i det fortsatta arbetet. En av de frågor som utredningen har att överväga är därför om lagringsskyldigheten bör begränsas avseende några av dessa uppgiftskategorier.

5.2 Uppgifter som lagras

5.2.1 Lagringsskyldigheten enligt datalagringsdirektivet

Artikel 5 i datalagringsdirektivet var uppdelad utifrån olika ändamål för vilka uppgifterna skulle lagras. I anslutning till respektive ändamål angavs exempel på den typ av trafikuppgifter som skulle lagras för respektive kommunikationssätt. Lagringsskyldigheten enligt datalagringsdirektivet omfattade uppgifter som genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät inom statens territorium, under förutsättning att uppgifterna tillhör någon av de kategorier som specificerades i artikel 5 i direktivet.

Uppgifter som är nödvändiga för att *spåra och identifiera en kommunikationskälla* (punkten 1a) omfattade, beträffande fast och mobil telefoni, det uppringande telefonnumret och abonnentens eller den registrerade användarens namn och adress. När det gäller internetåtkomst, internetbaserad e-post och internettelefoni omfattades uppgift om tilldelad användar-id (som är en unikt id som tilldelas den som abonnerar på eller registrerar sig på en internetåtkomsttjänst eller en internetkommunikationstjänst, artikel 2.2d). Användar-id och telefonnummer som tilldelats kommunikationen i det allmänna telenätet liksom namn på och adress till den abonnent eller registrerade användare som ip-adressen, användar-id eller telefonnumret tilldelades vid tidpunkten för kommunikationen omfattades också av lagringsskyldigheten enligt direktivet.

Uppgifter som är nödvändiga för att *identifiera slutmålet för en kommunikation* (punkten 1b) omfattade, beträffande fast och mobil telefoni, det eller de nummer som slagits samt abonnentens eller den registrerade användarens namn och adress. Slutmålet för internetbaserad e-post och internettelefoni omfattade uppgifter om användar-id eller telefonnummer som tilldelats den avsedda mottagaren av samtalet samt namn på och adress till abonnenten eller den registrerade användaren och den användar-id som tilldelats den avsedda mottagaren av kommunikationen.

När det gäller uppgifter som är nödvändiga för att *identifiera datum, tidpunkt och varaktighet för en kommunikation* (punkten 1c) avsågs beträffande fast och mobil telefoni datum och tid för ett samtals påbörjande och avslutande. För internetåtkomst, internetbaserad e-post och internettelefoni avsågs datum och tid för på-respektive avloggning i tjänsten inom en given tidszon samt beträffande internetåtkomsttjänsten även tilldelad ip-adress och användar-id.

För att *identifiera typ av kommunikation* (punkten 1d) skulle uppgift om telefoni- eller internettjänst lagras.

För att *identifiera användarnas kommunikationsutrustning* (punkten 1e) skulle lagring ske av det uppringande och det uppringda telefonnumret vid fast och mobil telefoni. När det gäller mobiltelefoni skulle lagringen därutöver omfatta den uppringande respektive den uppringda partens IMSI (International Mobile Subscriber Identity) och IMEI (International Mobile Equipment Identity) samt, vid förbetalda anonyma tjänster, datum och tid för den första aktiveringen av tjänsten och den lokaliseringsbeteckning (cell-id) från

vilken tjänsten aktiverades. Lokaliseringsbeteckningen definierades i direktivet som identiteten hos den cell från vilken ett mobiltelefonsamtal påbörjades eller avslutades (artikel 2.2e). Varje basstation i kommunikationsnätet har nämligen en beteckning som är unik för stationen, ett cell-id. När det gäller internetåtkomst, internetbaserad e-post och internet-telefoni gällde lagringen uppringande telefonnummer och DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare.

För att *identifiera lokaliseringen av mobil kommunikationsutrustning* (punkten 1f) krävdes slutligen lagring av lokaliseringsbeteckning (cell-id) för kommunikationens början samt uppgifter som identifierar cellernas geografiska placering genom referens till deras cell-id under den period som kommunikationsuppgifterna lagras.

5.2.2 Lagringsskyldigheten enligt svensk rätt

Lagringsskyldighetens omfattning enligt svensk rätt regleras i 6 kap. 16 a § LEK samt i 39–43 §§ förordningen om elektronisk kommunikation. Dessa bestämmelser omfattar samtliga de uppgiftskategorier som angavs i artikel 5 i datalagringsdirektivet, men de är i viss mån annorlunda strukturerade och definierade. Skälet till detta angavs vid genomförandet främst vara att få till stånd en tydlig och teknikneutral reglering (prop. 2010/11:46 s. 27). Exempelvis användes det vidare begreppet lokaliseringsinformation i stället för direktivets ”lokaliseringsbeteckning (cell-id)” (a. prop. s. 33). Vid genomförande av direktivet beslutades även att lagringsskyldigheten på två punkter skulle gå utöver den lagringsskyldighet som direktivet krävde. Leverantörerna ålades att lagra även uppgifter om misslyckad uppringning och uppgifter om lokalisering av mobilsamtals slut. I motiven anfördes att dessa uppgifter var av stort värde för de brottsbekämpande myndigheterna och att det, även med beaktande av integritets-, kostnads- och konkurrensaspekter, bedömdes att en sådan lagringsskyldighet var proportionerlig i förhållande till ändamålet att beivra brott (a. prop. s. 31 f.). Ett lagringskrav som omfattade även lokaliseringsuppgifter beträffande pågående kommunikation, något som vissa brottsbekämpande myndigheter hade anfört att det

fanns ett behov av, ansågs däremot inte proportionerligt och infördes därför inte (a. prop. s. 35).

5.3 Behovet av lagrade uppgifter

Som redan har framhållits råder det inte någon tvekan om att uppgifter om elektronisk kommunikation är av stort värde för att kunna upptäcka och utreda brott, inte minst vad gäller grov och organiserad brottslighet. För vissa typer av internetrelaterad brottslighet, som exempelvis barnpornografibrott, är trafikuppgifter också av avgörande betydelse för att kunna identifiera en misstänkt gärningsman.

Digitala spår blir en allt viktigare del i polisiärt arbete. Allt oftare utgör t.ex. en ip-adress det första spåret i en utredning av ett anmält brott. Detta medför att uppgift om vem som var abonnent på den aktuella ip-adressen vid en specifik tidpunkt eller under en specifik tidsperiod blir helt avgörande för hur ärendet hanteras vidare. Polisen har vidare påpekat att det ofta är analys av historiska trafikuppgifter, kopplat mot andra underrättelser, som utgör grunden för att ärenden om t.ex. grovt narkotikabrott når framgång. Ofta är det inte möjligt att i ett senare skede använda sig av andra hemliga tvångsmedel som t.ex. hemlig avlyssning av elektronisk kommunikation utan att först ha tillgång till historiska trafikuppgifter som visar vilka abonnemang som en misstänkt person använder sig av. Uppgifter inhämtas enligt polisen främst vid brott som inte är spontana utan som föregås av planering, där trafikuppgifter kan leda fram till vilka personer som deltagit och var dessa har befunnit sig, samt vid brott där det typiskt sett är av betydelse var personer har befunnit sig. En begränsande faktor är det förhållandet att det är tidskrävande att gå igenom materialet vilket gör att man undviker att begära in uppgifter för längre tid än nödvändigt.

Enligt utredningens mening står det klart att lagringen av uppgifter som helhet fyller en viktig funktion i den brottsbekämpande verksamheten (se avsnitt 3.5.2). Vid prövningen av om lagringen också är proportionerlig, dvs. att den inte sträcker sig längre än vad som är strikt nödvändigt för att nå de eftersträvade målen, måste dock behovet av de enskilda kategorierna av uppgifter som lagras

bedömas och vägas mot intresset av skydd för enskildas personliga integritet.

I samband med analysen identifierades några uppgiftskategorier beträffande vilka det ansågs kunna ifrågasättas om lagringen utgör en proportionerlig åtgärd (se Ds 2014:23 s. 52). Såvitt avser telefoni angavs detta gälla uppgifter om s.k. IMSI-nummer (del av 40 § punkten 1 förordningen om elektronisk kommunikation), eftersom denna information går att få fram genom SIM-kortets telefonnummer, lokaliseringsuppgifter om den första aktiveringen av en förbetald anonym tjänst (del av 40 § punkten 3 förordningen om elektronisk kommunikation) och uppgifter som identifierar den utrustning där kommunikation via ip-telefoni slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten (41 § punkten 3 förordningen om elektronisk kommunikation). Såvitt avser internetåtkomst och tillhandahållande av internetåtkomst ansågs lagringsskyldigheten kunna ifrågasättas beträffande uppgifter om den typ av kapacitet för överföring som har använts och uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten (43 § punkterna 4 och 5 förordningen om elektronisk kommunikation).

Utredningen har inhämtat uppgifter från både Polismyndigheten och Säkerhetspolisen vad gäller behovet av dessa kategorier av uppgifter.

När det gäller IMSI-nummer så kan denna uppgift enligt Säkerhetspolisen jämställas med telefonnummer eftersom uppgiften är unik och kan knytas till abonnemanget. IMSI är den identitet som mobiltelefonen använder sig av för att i luftgränssnittet identifiera sig mot basstationer. Det faktiska mobiltelefonnumret, MSISDN, är alltid knutet till en unik IMSI vilket gör att styrningen av samtal till och från mobiltelefonen går rätt.

Myndigheterna har framfört att det finns ett stort behov av att kunna få ut uppgifter om IMSI-nummer och vilket telefonnummer som IMSI-numret är knutet till. I fall där polisen ska inhämta trafikuppgifter från en operatör som i sitt elektroniska kommunikationsnät också hyr ut tjänster till en s.k. virtuell mobiloperatör, MVNO[1], kan det vara så att IMSI-numret, som identitet på abonnemanget, är det sökbegrepp som krävs för att få tillgång till trafikuppgifterna. Likaså

[1] Mobile Virtual Network Operator.

krävs IMSI för att hos en MVNO få tillgång till eventuella abonnentuppgifter, inklusive telefonnummer, som i de flesta fall endast finns hos MVNO och inte hos nätoperatören. I de fall som frågan ställs till en MVNO, så krävs det att MVNO har lagrat telefonnummer och IMSI och att sedan IMSI-numret används för att i efterföljande fråga till nätoperatören få ut trafikuppgifter. Polisen måste alltså först rikta frågan till den virtuelle operatören för att få fram IMSI-numret och därefter till nätoperatören som baserat på IMSI-numret kan ta fram trafikuppgifter. I de fall där polisen använder tekniska hjälpmedel i luftgränssnittet för att identifiera den misstänktes mobiltelefon, så erhålls IMSI-numret som sedan används för att hos operatören knyta det till ett telefonnummer och en eventuell abonnent. Det är viktigt att både telefonnummer och IMSI-nummer sparas av operatören då användaren vid byte till ett nytt SIM-kort kan erhålla ett nytt IMSI-nummer men behålla sitt gamla telefonnummer. Det blir allt vanligare att anonyma abonnemang används i brottslig verksamhet. Då krävs tekniska hjälpmedel för att i luftgränssnittet identifiera den misstänktes mobila kommunikationsutrustning. Det är därför inte tillräckligt med lagringsskyldighet enbart för uppgift om telefonnumret, utan både telefonnummer (MSISDN) och IMSI-nummer krävs för att möta de brottsbekämpande myndigheternas behov.

När det gäller uppgifter om den första aktiveringen av en förbetald anonym mobiltelefonitjänst har Säkerhetspolisen framhållit att det blir att vanligare att personer, som planerar att begå brottsliga handlingar, förser sig med ett stort antal mobiltelefoner med anonyma abonnemang. Mobiltelefonerna aktiveras men används inte för samtal förrän vid tidpunkten för brottet. Anledningen till att kravet på att dessa uppgifter ska lagras infördes i datalagringsdirektivet var terroristattackerna i Madrid. Den tekniska undersökningen visade att mobiltelefoner använts som utlösare till bomberna. Vid den fortsatta utredningen kunde man konstatera att de mobiltelefoner som använts hade varit aktiverade vid en särskild tidpunkt och i samma geografiska område vilket senare ledde till att gärningsmännen kunde lokaliseras och gripas. För att illustrera behovet av att uppgifter om den första aktiveringen av ett abonnemang lagras av operatörerna kan enligt Säkerhetspolisen ett hypotetiskt fall användas som exempel. Inkommer ett hot om en terroristattack mot exempelvis en flygplats, kan aktiverade men inte använda mobiltelefoner finnas

i området. Har abonnemangen dessutom varit aktiva i området under längre tid, kan de misstänkas vara utlösare till bomber. En blockering av kommunikation, med stöd av hemlig övervakning av elektronisk kommunikation, till de aktuella mobiltelefonerna kan förhindra att bomberna utlöses. Användningen av anonyma abonnemang gör att uppgifter om mobiltelefonernas lokalisering blir allt viktigare för att knyta sådana abonnemang till den misstänkte. För att kunna göra detta krävs att datum, spårbar tid och lokaliseringsinformation lagras. Dessa uppgifter är nödvändiga för att kunna identifiera användarens kommunikationsutrustning eller den utrustning som denne tros ha använt. Det har enligt myndigheterna visat sig att uppgifter om vilka mobiltelefoner som befunnit sig i det geografiska område där ett brott begåtts i ibland kan vara det enda spår en utredning kan utgå ifrån.

Myndigheterna har också framfört att gärningsmän som begår planerade grova brott ofta har som praxis att använda anonyma abonnemang. Att få tillgång till de aktuella uppgifterna hjälper polisen att få reda på om det identifierade abonnemanget är en möjlig ”brottslur”, dvs. ett abonnemang som använts endast strax före, under och kanske direkt efter ett brott. Enligt polisen kan uppgifterna om kontantkorten på detta sätt skapa nya ingångar och föra utredningen framåt. Detta kan enligt Säkerhetspolisen exempelvis relateras till terrorattackerna i Paris där en gärningsman hade 13 mobiltelefoner. Behovet av att kunna få uppgifter om var dessa telefoner varit aktiverade, även om de inte använts, kan vara mycket värdefull information i det fortsatta kartläggningsarbetet för att eventuellt konstatera om det fanns medgärningsmän.

Uppgifter som vid ip-telefoni och internetåtkomst identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten är enligt myndigheterna nödvändiga för att identifiera användares kommunikationsutrustning eller den utrustning som de förmodas ha använt. Det är ofta så att en operatör inte har ett ansvar för hela kommunikationskedjan, utan ansvaret avslutas vid en slutpunkt där kommunikationen avskiljs vilket kan vara en anslutningspunkt till ett privat fastighetsnät eller till en annan operatör, exempelvis ett stadsnät. Dessa punkter där kommunikationen avskiljs är viktiga för polisen att kunna få uppgifter om. Det kan innebära att kontakter kan tas med fastighetsägaren för vidare utredning eller att kontakter tas med stadsnätet

för att få tillgång till resterande uppgifter. Myndigheterna har framhållit att det i dessa fall skulle vara svårt – om inte omöjligt – att identifiera ”slututrustningen” om inte uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige finns att tillgå. Enligt myndigheterna är det alltså egentligen inte den ”första utrustningen” som är intressant. Men för att kunna få reda på vilken som är den ”sista utrustningen” behövs uppgiften för att på så sätt kunna leda fram till rätt slutanvändare.

Polisen har också framhållit att huvudregeln bör vara att leverantörerna så långt som möjligt ska lagra och lämna ut de uppgifter som kan identifiera slutanvändaren. Enligt polisen är detta ytterst en fråga om rättssäkerhet för att säkerställa att åtgärderna riktas mot rätt person. Alternativet kan vara att åtgärderna inte kan genomföras.

När det slutligen gäller uppgifter om den typ av kapacitet som har använts för internetåtkomst har myndigheterna framfört att behovet av sådana uppgifter hänger samman med att ansvaret för kommunikationskedjan blir allt mer uppsplittrat. Den som tillhandahåller internetåtkomst har inte alltid uppgifter om var användaren finns rent geografiskt utan endast om att han eller hon har anslutit via en operatör som tillhandhållit en fiberanslutning. Var fiberanslutningen terminerar har endast den som tillhandahåller kapacitet för internetåtkomst, dvs. fiberanslutningen, uppgifter om. Polisen måste därför kontakta den operatör som tillhandahåller fiberanslutningen för att få uppgift om den geografiska plats där användaren finns. Om inte uppgifter om kapacitet för internetåtkomst lagras, kan det innebära att myndigheten inte kan reda ut på vilken geografisk plats användaren befinner sig. Den som tillhandahåller internetåtkomst ska således lagra uppgifter om vilken operatör det är som tillhandahåller kapacitet för internetåtkomst, exempelvis fiber. Genom denna uppgift kan myndigheten få reda på vilken leverantör man ska vända sig till för att få uppgifter om användarens kommunikation. Enligt myndigheterna är det också nödvändigt att kunna göra en kartläggning över en misstänkt persons möjligheter till kommunikation. Om det till exempel kommer fram att den misstänkte har en fiberförbindelse, så kan det innebära att misstankarna stärks och att man kan misstänka att förbindelsen utnyttjas till att kommunicera i brottsliga syften. Möjligheten att få en bild av en misstänkts kommunikationsmöjligheter är alltså viktig och kan också vara underlag för att sätta in tvångsmedel på rätt ställen. Myndigheterna

har vidare betonat att, om myndigheterna inte kan få uppgifter om kapacitet för internetåtkomst, så kan det – i de fall det rör sig om kriminella organisationer som hyr en fiberförbindelse till en lokal varifrån brottslig verksamhet bedrivs – innebära att både platsen för lokalen och den kriminella verksamheten kan döljas. Myndigheterna har samtidigt framhållit att de aktuella uppgifterna visserligen finns hos tjänsteleverantören utan ett krav på lagring. Men om de inte uttryckligen omfattas av lagringskravet, så kan det hända att leverantören vägrar att lämna ut uppgifterna eller lämnar ut dem i ett format som inte enkelt kan läsas.

5.4 Utredningens bedömning

Utredningens bedömning: Det bör inte göras några förändringar i fråga om vilka uppgifter som ska lagras enligt datalagringsreglerna.

Lagring av uppgifter om elektronisk kommunikation är en åtgärd som inkräktar på rättigheter som enskilda är tillförsäkrade enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga. För att en sådan åtgärd ska vara godtagbar krävs att den objektivt sett är ägnad att uppnå syftet med åtgärden och att den är proportionerlig (se även artikel 15 i direktiv 2002/58/EG). En åtgärd kan anses proportionerlig bara om den avgränsas på ett sådant sätt att integritetsintrånget inte blir större än vad som är strikt nödvändigt för att uppnå det eftersträvade målet.

Som nämnts ovan gjordes i analysen bedömningen att det kan ifrågasättas om det finns behov av att lagra vissa av de uppgiftskategorier som lagras enligt dagens regler. Av de uppgifter som polisen nu har lämnat till utredningen framgår dock att samtliga uppgiftskategorier som lagras enligt dagens regler bedöms vara av stor vikt för den brottsbekämpande verksamheten.

I samband med vår kartläggning av inhämtningslagen (se avsnitt 9) har det kommit fram att inhämtningen enligt den lagen i princip uteslutande avser uppgifter om mobiltelefoni. Genom de uppgifter som kommit fram vid kartläggningen – samt de uppgifter som Polismyndigheten och Säkerhetspolisen har lämnat – anser vi att det är klarlagt att det finns ett stort behov av att de uppgifts-

kategorier som lagras beträffande mobiltelefoni även i fortsättningen omfattas av lagringsskyldigheten.

När det gäller behovet av att vid internetåtkomst lagra uppgifter om den typ av kapacitet för överföring som har använts och uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ger det som kommit fram vid vår kartläggning inte någon ledning. Av de uppgifter som Polismyndigheten och Säkerhetspolisen har lämnat framgår dock att det i vissa situationer kan finnas ett stort behov av dessa uppgifter. Enligt vår mening saknas det anledning att ifrågasätta att det förhåller sig på det sättet.

Beträffande några uppgiftskategorier, nämligen uppgifter om typ av kapacitet som används för internetåtkomst samt i vissa fall uppgifter om IMSI-nummer, har det visserligen kommit fram att leverantörerna har tillgång till dessa även utan krav på obligatorisk lagring. För dessa uppgifter skulle det kunna övervägas att upphäva lagringsskyldigheten. Eftersom uppgifterna ändå finns tillgängliga skulle detta emellertid inte leda till någon förstärkning av skyddet för enskildas integritet. Utan ett lagringskrav finns det inte heller några garantier för att dessa uppgifter även i framtiden kommer att sparas av leverantörerna. Enligt utredningens uppfattning utgör dessa omständigheter tillräckliga skäl för att inte föreslå några förändringar beträffande de aktuella uppgifterna.

Sammantaget står det enligt utredningens uppfattning klart att lagringsskyldighetens inte omfattar annat än vad som är strikt nödvändigt för att uppnå syftet med regleringen. Det bör därför inte göras några förändringar i fråga om vilka uppgiftskategorier som ska lagras.

6 Krav på lagring inom EU?

6.1 Inledning

Enligt EU-domstolen är den oberoende myndighetskontrollen en grundläggande beståndsdel i skyddet för enskilda individer i samband med behandlingen av personuppgifter. Domstolen pekade i datalagringsdomen på att en brist i datalagringsdirektivet var att denna kontroll av att skydds- och säkerhetskraven för de lagrade uppgifterna följs – vilket föreskrivs i artikel 8.3 i stadgan – inte fullt ut kunde anses vara garanterat i direktivet (punkt 68). Detta var enligt domstolen en konsekvens av att direktivet inte krävde att uppgifterna skulle lagras inom unionen.

I analysen framhölls att det mot bakgrund av de uttalanden EU-domstolen gjorde i domen om intresset av en effektiv tillsyn finns mycket som talar för att det i svensk rätt bör införas ett krav på att trafikuppgifter som genereras eller behandlas vid användningen av allmänna kommunikationsnät och kommunikationstjänster som omfattas av lagringsskyldigheten ska lagras inom EU eller EES. Detta skulle kunna göras t.ex. genom ett särskilt förbud mot överföring av sådana trafikuppgifter till ett tredje land (dvs. ett land som inte ingår i EU eller är anslutet till EES) för lagring där.

6.2 De svenska reglerna om säkerhet och tillsyn

6.2.1 Säkerhet

När datalagringsdirektivet genomfördes i Sverige konstaterade regeringen att de regler om driftsäkerhet och integritetsskydd som redan fanns i LEK inte var tillräckliga för de uppgifter som skulle lagras enligt direktivet (prop. 2010/11:46 s. 54). Det angavs, mot bakgrund av det nya syfte för vilket uppgifter skulle lagras samt den mängd

uppgifter det rörde sig om, att kravet på säkerhet borde höjas och att säkerhetsnivån borde preciseras. Resultatet blev att det infördes en ny bestämmelse 6 kap. 3 a § LEK av vilken det framgår att den som är lagringsskyldig enligt 6 kap. 16 a § samma lag ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. I förarbetena anges att det därav följer att bestämmelsen, till skillnad från vad som gäller enligt 6 kap. 3 § LEK, inte lämnar något utrymme att bestämma säkerhetsnivån genom en avvägning mellan teknik, kostnader och risken för integritetsintrång (prop. 2010/11:46 s. 75).

I 6 kap. 3 a § andra stycket LEK bemyndigas regeringen eller den myndighet regeringen bestämmer att komplettera lagbestämmelsen med ytterligare föreskrifter om säkerheten. Detta har regeringen gjort i 37 § förordningen om elektronisk kommunikation. Av bestämmelsen framgår att den som är lagringsskyldig ska vidta åtgärder för att säkerställa att de lagrade uppgifterna är av samma kvalitet och föremål för samma säkerhet och skydd som vid den behandling som skett före lagringen. Vidare framgår att åtgärder ska vidtas för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring samt för att förhindra otillåten lagring, behandling av eller tillgång till och otillåtet avslöjande av uppgifterna. Slutligen får uppgifterna göras tillgängliga endast för personal med särskild behörighet. PTS får efter att ha hört Polismyndigheten, Säkerhetspolisen och Datainspektionen meddela närmare föreskrifter om de åtgärder som ska vidtas.

PTS har med stöd av 37 § i förordningen meddelat sådana föreskrifter (PTSFS 2012:4). Dessa går i korthet ut på att den lagringsskyldige ska bedriva ett kontinuerligt och systematiskt säkerhetsarbete med beaktande av de särskilda risker lagringsskyldigheten medför (3 §). Rutiner ska finnas som säkerställer att bara personal med särskild behörighet har tillgång till lagrade uppgifter och de system som hanterar uppgifterna (4 §). Den utrustning som används för att lagra uppgifter ska också placeras i ett särskilt skyddat utrymme för att förhindra förlust av eller otillåten tillgång till uppgifterna (5 §). Vidare ska all behandling av lagrade uppgifter loggas i krypterad form och på ett sådant sätt att det går att följa upp vem som har haft tillgång till uppgifterna och vid vilken tidpunkt (6 §). Lagrade uppgifter ska också säkerhetskopieras (7 §).

Vad slutligen gäller hanteringen av lagrade uppgifter vid lagringstidens slut anges i 6 kap. 16 d § LEK att den lagringsskyldige vid denna tidpunkt genast ska utplåna uppgifterna. Om uppgifterna har begärts utlämnade före utgången av lagringstiden, men inte har hunnit lämnas ut, ska dock leverantören fortsätta lagra uppgifterna till dess att de har lämnats ut. Därefter ska leverantören genast utplåna dem.

6.2.2 Tillsyn

PTS utövar tillsyn över verksamhet som bedrivs med stöd av LEK. Myndighetens tillsyn omfattar efterlevnaden av lagen och de beslut om skyldigheter eller villkor som har meddelats med stöd av lagen (7 kap. 1 § LEK).

För att kunna utöva en effektiv tillsyn har PTS en rad befogenheter till sitt förfogande. Enligt 7 kap. 2 § LEK har PTS rätt att för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av LEK bedrivs. Vidare får PTS förelägga en leverantör att tillhandahålla myndigheten de upplysningar och handlingar som behövs för kontrollen (7 kap. 3 §). Finner PTS skäl att misstänka att den som bedriver verksamhet enligt LEK inte efterlever lagen eller de föreskrifter som har meddelats med stöd av lagen, ska myndigheten underrätta den som bedriver verksamheten om detta förhållande och ge denne möjlighet att yttra sig (7 kap. 4 §). PTS får också meddela de förelägganden och förbud som behövs för att rättelse av en överträdelse ska ske omedelbart eller inom skälig tid. Ett sådant föreläggande eller förbud får förenas med vite (7 kap. 4 §). Om föreläggandet inte följs, får PTS återkalla ett tillstånd, ändra tillståndsvillkor eller ytterst besluta att den som har åsidosatt en skyldighet helt eller delvis ska upphöra med verksamheten. PTS beslut enligt lagen eller enligt en föreskrift som har meddelats med stöd av lagen får överklagas hos allmän förvaltningsdomstol (7 kap. 19 §).

6.3 Överföring av personuppgifter till tredje land

6.3.1 Bedömningen av skyddsnivån enligt dataskyddsdirektivet

Som framgår ovan (avsnitt 3.2.5.1) innebär regleringen i dataskyddsdirektivet att överföring av personuppgifter till ett land utanför EU och EES får ske bara om landet i fråga säkerställer en adekvat skyddsnivå för uppgifterna. Bedömningen av om skyddsnivån är adekvat ska ske på grundval av alla de förhållanden som har samband med en överföring eller en grupp av överföringar av uppgifter. Härvid ska särskilt beaktas uppgifternas art, den eller de avsedda överföringarnas ändamål och varaktighet, ursprungslandet och det slutliga bestämmelselandet, de allmänna respektive särskilda rättsregler som gäller i det tredje landet liksom de regler för yrkesverksamhet som gäller där (artikel 25.2).

För att säkerställa att dataskyddsdirektivet tillämpas på ett enhetligt sätt i medlemsstaterna har den så kallade artikel 29-gruppen bildats. Gruppen har fått sitt namn av artikel 29 i direktivet. I artikel 30 finns bestämmelser om gruppens uppgifter. Gruppen är rådgivande och oberoende och ska se till att direktivet tillämpas enhetligt i medlemsstaterna. Gruppen ska också yttra sig till EU-kommissionen om skyddsnivån i gemenskapen och i tredje land samt ge råd till kommissionen om förslag till ändringar av direktivet. Gruppen har publicerat ett arbetsdokument[1] som innehåller riktlinjer för tillämpningen av artikel 25 och 26 i direktivet. Av arbetsdokumentet följer bl.a. att en bedömning av om ett tredje land erbjuder en adekvat skyddsnivå bör innehålla två grundläggande delar.

För det första bör innehållet i de tillämpliga reglerna i det tredje landet analyseras. För att skyddet ska kunna anses adekvat bör enligt arbetsdokumentet reglerna innehålla åtminstone följande kärna av dataskyddsprinciper:

- *Principen om avgränsning av ändamålet* innebär att personuppgifter ska behandlas för ett specifikt ändamål och får därefter användas eller vidarebefordras endast om detta är förenligt med ändamålet för behandlingen.

[1] Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv, GD XV D/5025/98.

- *Principerna om uppgifternas kvalitet och proportionalitet* innebär att personuppgifter ska vara korrekta och, om nödvändigt, hållas aktuella. Uppgifterna ska vara adekvata, relevanta och inte mer omfattande än vad som krävs för ändamålet med behandlingen.
- Enligt *öppenhetsprincipen* ska enskilda informeras om ändamålet med behandlingen och om vissa andra förhållanden som är förknippade med personuppgiftsbehandlingen.
- *Säkerhetsprincipen* innebär att tekniska och organisatoriska säkerhetsåtgärder ska vidtas av den personuppgiftsansvarige med hänsyn till den risk behandlingen innebär.
- *Rätten till tillgång, rättelse och invändningar* innebär att den registrerade ska ha rätt att få en kopia av uppgifter som behandlas om honom eller henne och rätt att få dessa uppgifter rättade om de är felaktiga. I vissa situationer ska den enskilde också ha rätt att motsätta sig behandlingen.
- Enligt *principen om restriktioner för vidare överföring till andra tredje länder* bör sådan överföring vara tillåten endast om mottagaren också har att tillämpa bestämmelser som erbjuder ett adekvat skydd för uppgifterna.

På vissa särskilda kategorier av personuppgifter bör enligt arbetsdokumentet ytterligare principer tillämpas. Till exempel bör ytterligare säkerhetsåtgärder ha vidtagits om överföringen innefattar sådana personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter som rör hälsa och sexualliv samt uppgifter som rör lagöverträdelser, brottmålsdomar och säkerhetsåtgärder.

Det andra ledet i bedömningen av om ett tredje land säkerställer en adekvat skyddsnivå för personuppgifter är enligt arbetsdokumentet att analysera de mekanismer som finns för att säkerställa att reglerna tillämpas effektivt. Det påpekas i dokumentet att det i Europa finns en bred samsyn om att en nödvändig del av dataskyddet är förekomsten av ett system med extern tillsyn av ett oberoende organ som har till uppgift att övervaka dataskyddsreglernas efterlevnad. Det framhålls samtidigt att sådana mekanismer inte alltid finns i andra delar av världen. För att bedöma om skyddet i ett tredje land är tillräckligt bör analysen enligt dokumentet inrikta sig på att identi-

fiera ändamålen med dataskyddsregleringen i landet och bedöma de judiciella och processuella mekanismer som används. För att kunna anses adekvat bör dataskyddssystemet innehålla mekanismer som har till ändamål att

- upprätthålla en hög nivå av efterlevnad av dataskyddsregleringen,
- erbjuda enskilda stöd och hjälp vid utövandet av deras rättigheter, och
- erbjuda enskilda möjligheter att få rättelse när reglerna inte följs.

Enligt dataskyddsdirektivet ska hänsyn tas inte bara till lagstadgade regler i det tredje landet utan även till t.ex. branschregler och andra självregleringsinstrument. En förutsättning för att sådana regler ska få någon relevans vid bedömningen av om skyddsnivån är adekvat är dock att det kan fastställas att reglerna följs.

6.3.2 Europeiska kommissionens beslut om adekvat skyddsnivå

Enligt artikel 25.6 i dataskyddsdirektivet kan kommissionen besluta att ett tredje land genom sin interna lagstiftning eller på grund av sina internationella åtaganden har en skyddsnivå som är adekvat i den mening som avses i artikeln. Medlemsstaterna ska i sådana fall vidta de åtgärder som är nödvändiga för att följa kommissionens beslut. Kommissionen har fattat ett antal sådana beslut avseende bl.a. Andorra, Argentina, Israel, Nya Zealand, Schweiz och Uruguay. Vidare har kommissionen i förhållande till USA beslutat att de s.k. Safe Harbour Privacy Principles, tillämpade i enlighet med den vägledning som ges i de frågor och svar som utfärdats av Förenta staternas handelsministerium, ska anses utgöra en adekvat skyddsnivå för personuppgifter som överförs från gemenskapen till organisationer som är etablerade i Förenta staterna. Överföring av uppgifter till organisationer som har åtagit sig att följa dessa principer är följaktligen tillåtet. Överföring till Kanada är också tillåten, om mottagaren omfattas av landets lagstiftning om skydd för personuppgifter.

Kommissionens olika beslut om adekvat skyddsnivå är i huvudsak uppbyggda på samma sätt.[2] I beslutsskälen redogörs närmare för det aktuella tredje landets regler när det gäller hanteringen av och skyddet för personuppgifter. Därefter innehåller skälen en bedömning av om det tredje landets regler omfattar alla de grundprinciper som krävs för att skyddsnivån ska anses vara adekvat och om tillämpningen av reglerna garanteras genom administrativa och rättsliga medel samt genom någon form av kontrollorgan, tillsynsmyndighet eller liknande. Besluten innehåller sedan en artikel som anger att, för tillämpningen av artikel 25.2 i dataskyddsdirektivet, det tredje landet ska anses erbjuda en adekvat skyddsnivå för de personuppgifter som överförs från Europeiska unionen. Vidare innehåller besluten bestämmelser om att en medlemsstat under vissa specificerade omständigheter tills vidare får avbryta överföringen av personuppgifter till det tredje landet. Detta gäller om

1. en behörig myndighet i det aktuella tredje landet har funnit att en viss mottagare bryter mot tillämpliga skyddsregler, eller
2. det är i hög grad sannolikt att skyddsreglerna överträds, det finns välgrundad anledning att tro att en behörig myndighet i det aktuella tredje landet inte vidtar eller inte i tid kommer att vidta de åtgärder som behövs för att avgöra ärendet, en fortsatt överföring av uppgifterna skulle innebära en överhängande risk för att de registrerade åsamkas allvarlig skada, och medlemsstaternas behöriga myndigheter har gjort vad som under rådande omständigheter rimligen kan begäras för att anmärka mot den part som är ansvarig för behandlingen och ge denna möjlighet att svara.

Ett sådant tillfälligt avbrott i överföringen ska upphöra så snart det har säkerställts att skyddsreglerna följs och de behöriga myndigheterna i gemenskapen har underrättats om detta. Medlemsstaterna har en skyldighet att utan dröjsmål underrätta kommissionen om åtgärder som innebär att överföringen av personuppgifter till det tredje landet har avbrutits.

Kommissionens beslut har i svensk rätt genomförts genom bestämmelsen i 13 § personuppgiftsförordningen (1998:1191). Enligt

[2] Se t.ex. Kommissionens beslut av den 19 oktober 2010 i enlighet med Europaparlamentet och rådets direktiv 95/46/EG om adekvat skydd för personuppgifter i Andorra (2010/625/EU)

den bestämmelsen får personuppgifter föras över till ett tredje land om och i den utsträckning som Europeiska kommissionen har konstaterat att landet har en adekvat nivå för skyddet av personuppgifter i enlighet med artikel 25.6 i dataskyddsdirektivet. I en bilaga till personuppgiftsförordningen anges de beslut som kommissionen har fattat i det avseendet.

6.3.3 Förhållandet mellan dataskyddsdirektivet och dataskyddskonventionen

De principer om skydd för enskilda personers fri- och rättigheter, särskilt rätten till privatliv, som dataskyddsdirektivet innehåller utgör enligt skälen till direktivet en precisering och en förstärkning av principerna i dataskyddskonventionen (skäl 11).

Av artikel 12.2 i konventionen framgår att konventionsstaterna som huvudregel inte av integritetsskyddsskäl får hindra att personuppgifter förs över till en annan konventionsstat för att användas där. Frågan om förhållandet mellan denna bestämmelse och direktivets förbud mot överföring till länder som inte erbjuder en adekvat skyddsnivå har behandlats i olika sammanhang.

Av det ovan nämnda arbetsdokumentet från artikel 29-gruppen, som gavs ut år 1998, framgår att dataskyddskonventionen i materiellt avseende då bedömdes innehålla fem av de sex grundläggande dataskyddsprinciper som nämns ovan. Den del som ansågs saknas i konventionen var restriktioner för överföring av uppgifter till länder som inte är anslutna till konventionen. När det gäller processuella mekanismer framhölls att konventionen förpliktar staterna att lagfästa dataskyddsprinciperna och att lämpliga sanktioner och rättsmedel ska finnas mot överträdelser av dessa. Detta borde enligt dokumentet vara tillräckligt för att säkerställa en tillräcklig nivå av efterlevnad av reglerna. Det påpekades dock att konventionen inte ålägger staterna att etablera några mekanismer som möjliggör granskning av klagomål, även om konventionsstaterna i praktiken i regel har gjort så.

Slutsatsen i dokumentet var att de flesta överföringar till stater som har ratificerat konventionen kan presumeras vara tillåtna enligt artikel 25.1 i dataskyddsdirektivet, under förutsättning att det aktuella landet har lämpliga mekanismer som säkerställer att reglerna följs och att landet är den slutliga destinationen för överföringen.

Under hösten 2001 antogs ett tilläggsprotokoll till dataskyddskonventionen (ETS 181). Enligt artikel 1 i protokollet ska varje konventionsstat se till att en eller flera myndigheter ansvarar för att kontrollera att de åtgärder respekteras som inom dess nationella lagstiftning ger verkan åt de principer som anges i konventionen och i tilläggsprotokollet.[3] Myndigheten ska därvid bl.a. ha befogenhet att utreda, ingripa och inleda rättsliga förfaranden om de nationella reglerna överträds. Myndigheten ska utöva sina funktioner helt oberoende. Tilläggsprotokollet innehåller vidare bestämmelser som anger att konventionsstaterna ska vidta åtgärder för att säkerställa att överföring av personuppgifter till ett land som inte är konventionspart får ske bara om landet i fråga säkerställer en adekvat skyddsnivå för uppgifterna (artikel 2).

Frågan om förhållandet mellan dataskyddsdirektivet och konventionen behandlades också i samband med att personuppgiftslagen infördes. Datainspektionen vände sig då emot att ett generellt undantag som tillåter överföring för användning enbart i en stat som anslutit sig till dataskyddskonventionen skulle tas in i lagen. Detta eftersom det enligt inspektionens uppfattning inte enbart var en nationell fråga att avgöra i vilken omfattning överföring får ske till stater som inte är medlemmar i Europeiska unionen. Regeringen konstaterade dock att Sverige har skyldigheter inte bara gentemot Europeiska unionen utan också enligt Europarådets konvention, och att det vore oförenligt med konventionen att införa en ordning som innebär att överföringen till en konventionsstat kan hindras av det skälet att staten i någon mening inte skulle anses ha en adekvat skyddsnivå för personuppgifter. Enligt regeringen var det inte heller antagligt att medlemsstaterna inom Europeiska unionen, varav de allra flesta vid antagandet av direktivet hade anslutit sig till konventionen, genom direktivet skulle ha skapat en ordning som vore oförenlig med åtagandena enligt konventionen. De stater som anslutit sig till Europarådets konvention fick enligt regeringens mening anses ha en sådan adekvat skyddsnivå som krävs enligt EG-direktivet (prop. 1997/98:44 s. 95).

[3] I Sverige fullgörs denna uppgift av Datainspektionen.

6.4 Utredningens bedömning

Utredningens bedömning: Det bör inte införas något uttryckligt förbud mot att uppgifter som lagras enligt de svenska datalagringsreglerna förs över till ett tredje land för lagring där.

EU-domstolen konstaterade i datalagringsdomen att datalagringsdirektivet inte krävde att uppgifterna skulle lagras inom unionen vilket enligt domstolen innebar att den i artikel 8.3 i stadgan uttryckligen föreskrivna oberoende myndighetskontrollen av att skydds- och säkerhetskraven följs inte fullt ut kunde anses vara garanterad (p. 68). Enligt domstolen är en sådan kontroll som ska utövas på grundval av unionsrätten en grundläggande beståndsdel i skyddet för enskilda i samband med behandlingen av personuppgifter. Det problem som domstolen satte fingret på var således inte i första hand att direktivet saknade ett krav på lagring inom EU, utan snarare de konsekvenser som domstolen ansåg att detta förde med sig för möjligheterna att utöva oberoende myndighetskontroll.

Ett sätt att garantera effektiviteten av myndighetskontrollen skulle givetvis kunna vara att införa ett krav i nationell rätt på att uppgifter som lagras med stöd av de tvingande datalagringsreglerna ska lagras inom EU eller EES. Ett sådant krav skulle också kunna bidra till att motverka risken för s.k. ändamålsglidning (se Ds 2014:23 s. 96 f.). Enligt utredningens uppfattning kan dock EU-domstolens dom inte tolkas på så sätt att det skulle finnas något principiellt hinder mot en nationell lagstiftning som tillåter att uppgifter lagras utanför unionen, så länge myndighetskontrollen ändå kan anses vara garanterad.

Enligt svensk rätt gäller leverantörens skyldigheter enligt de bestämmelser som anger hur lagringsskyldigheten ska fullgöras, t.ex. de krav som rör säkerheten för de lagrade trafikuppgifterna, även om lagringen förläggs utomlands (prop. 2010/11:46 s. 60). Detta måste särskilt beaktas av leverantörerna, om de överväger att lagra trafikuppgifter utomlands. Det ingår i PTS ansvar att kontrollera att leverantörerna följer regleringen i LEK och de föreskrifter som har meddelats med stöd av lagen. Även detta ansvar gäller oberoende av var leverantörerna väljer att lagra uppgifter. Som framgår ovan har PTS en rad befogenheter till sitt förfogande för att kontrollera att leverantörerna följer skydds- och säkerhetsreglerna. Regeringen

bedömde när datalagringsdirektivet genomfördes att de befogenheter PTS har får anses vara tillräckliga för att myndigheten ska kunna utöva en aktiv och ändamålsenlig tillsynsverksamhet (a. prop. s. 58).

PTS befogenhet att få tillträde till områden, lokaler och andra utrymmen där verksamhet som omfattas av LEK bedrivs kan i praktiken utövas endast i Sverige. Däremot torde möjligheterna att utöva de övriga befogenheter myndigheten har till sitt förfogande, t.ex. att begära upplysningar eller att meddela förelägganden och förbud, inte påverkas av var leverantören väljer att lagra uppgifterna. Mot den bakgrunden bedömer vi att PTS har vissa möjligheter att bedriva en aktiv och ändamålsenlig tillsynsverksamhet även gentemot leverantörer som väljer att lagra uppgifter utanför unionen.

I sammanhanget bör det framhållas att regleringen i dataskyddsdirektivet, dataskyddskonventionen och PUL innebär att personuppgifter inte får föras över till länder som inte erbjuder en adekvat nivå av skydd för uppgifterna. Vid bedömningen av om skyddet kan anses adekvat ska det beaktas om de tillämpliga reglerna i det tredje landet innehåller den kärna av dataskyddsprinciper som gäller inom EU. Dessa principer innebär bl.a. att kvaliteten på det aktuella landets skyddsmekanismer är en viktig omständighet vid bedömningen av skyddsnivån. Regleringen innebär således att uppgifter får föras över bara till sådana tredje länder som har tillräckliga skyddsmekanismer sett i förhållande till den aktuella typen av uppgifter. Kraven på skydd ska också ställas högre ju känsligare uppgifter det är fråga om. Enligt vår bedömning innebär det att det bör krävas att det tredje landet har inrättat någon form av system med fristående myndighetskontroll för att nivån av skydd för datalagrade uppgifter ska anses adekvat. I den mån uppgifter förs över till ett sådant land kommer således skyddet för uppgifterna att kontrolleras även av det tredje landets kontrollmyndighet. Det bör också nämnas att Datainspektionen har i uppgift att utöva tillsyn över att personuppgifter inte förs över till sådana länder som saknar en adekvat skyddsnivå.

Mot den bakgrunden bedömer vi sammantaget att den oberoende myndighetskontrollen är garanterad i svensk rätt även i förhållande till leverantörer som väljer att lagra uppgifter utanför unionen. Avsaknaden av ett krav på lagring inom EU eller EES innebär således inte att regleringen i svensk lag strider mot bestämmelserna om grundläggande rättigheter i EU-stadgan.

Det kan också påpekas att en av de centrala principerna vid bedömningen av om ett land lever upp till kraven på adekvat skyddsnivå är principen om avgränsning av ändamålet. Som framgår ovan innebär principen att personuppgifter får behandlas endast för ett specifikt ändamål och därefter får användas eller vidarebehandlas endast om det är förenligt med detta ändamål. I den mån ett tredje land har infört regler som innebär att lagrade uppgifter i stor utsträckning kan lämnas ut för andra ändamål än det för vilket de samlades in, kan skyddsnivån i landet därför normalt inte anses vara adekvat. Dessa regler innebär således att risken för ändamålsglidning begränsas.

Ett krav i nationell rätt på lagring inom EU eller EES skulle vidare förutsätta att detta är förenligt med EU-regleringen på området och med Sveriges internationella åtaganden i övrigt. Av regleringen i dataskyddsdirektivet framgår att överföring av personuppgifter till tredje land i princip ska vara tillåten, om det tredje landet erbjuder en adekvat nivå av skydd för uppgifterna. Direktivet innehåller inte några bestämmelser som tillåter att medlemsstaterna förbjuder överföring till ett land trots att landet erbjuder en adekvat skyddsnivå. Ett generellt förbud mot överföring av uppgifter som lagras enligt de svenska datalagringsreglerna torde därför förutsätta att det kan konstateras att inget tredje land erbjuder en adekvat nivå av skydd för sådana uppgifter. Exempelvis skulle en möjlighet att motivera ett generellt förbud eventuellt kunna vara att resonera på så sätt att de nu aktuella uppgifterna är så integritetskänsliga att inget tredje land kan anses erbjuda ett adekvat skydd, helt oberoende av vilka skyddsregler som gäller i landet. Ett sådant resonemang är dock knappast hållbart. Regleringen i dataskyddsdirektivet förutsätter att bedömningen av skyddsnivån görs individuellt och med beaktande av samtliga omständigheter hänförliga till en viss överföring eller grupp av överföringar. En ståndpunkt som innebär att vissa uppgifter – oavsett omständigheterna – aldrig kan överföras till tredje land kan inte förenas med det synsättet.

Vidare är medlemsstaterna skyldiga att följa kommissionens beslut som innebär att vissa tredje länder ska anses erbjuda en adekvat skyddsnivå vid tillämpningen av artikel 25 i dataskyddsdirektivet. Som framhölls i analysen skulle ett förbud mot överföring av den typ som nu diskuteras visserligen inte innebära något generellt åsidosättande av kommissionens beslut. Vad det handlar om är i stället att ta ställning till om det finns utrymme för att i nationell

rätt, när det gäller en viss typ av noggrant avgränsad lagring av personuppgifter, inskränka möjligheterna till överföring med hänsyn till att säkerhetskraven måste ställas så högt att en lagring i tredje land inte kan godtas trots att landet generellt anses erbjuda en adekvat skyddsnivå. Som nämnts är den bedömning av skyddsnivån som ska göras enligt dataskyddsdirektivet i grunden individuell, och ett tredje land kan mycket väl anses ha en adekvat nivå av skydd när det gäller en viss typ av uppgifter medan bedömningen kan bli den motsatta när det gäller en annan typ av uppgifter. Samtidigt är kommissionens beslut utformade på ett sätt som inte lämnar något egentligt utrymme för individuella bedömningar när det gäller skyddsnivån i de tredje länder som omfattas av besluten. Besluten innehåller t.ex. inte några bestämmelser som gör det möjligt att undanta någon viss typ av uppgifter eller register. Därför talar det mesta för att kommissionens beslut i fråga om skyddsnivå ska gälla för alla former av överföringar, oberoende av vilka uppgifter det handlar om eller för vilka syften uppgifterna behandlas. Som framgår ovan innehåller besluten dessutom detaljerade bestämmelser om vilka förutsättningar som ska vara för handen för att medlemsstaterna ändå ska få hindra överföring till ett tredje land som omfattas av ett beslut. Dessa bestämmelser ger inte stöd för att generellt förbjuda överföring av någon viss typ av uppgifter. Det förutsätts också i besluten att en åtgärd som innebär att överföring hindras är tillfällig och följer ett särskilt förfarande med bl.a. underrättelse till kommissionen.

Möjligen skulle datalagringsdomen kunna tolkas så att den nu behandlade regleringen inte längre gäller för sådana uppgifter som skulle lagras enligt det upphävda direktivet. En sådan tolkning skulle i så fall kunna baseras på att EU-domstolen skulle ha menat att adekvat skydd enligt dataskyddsdirektivet inte är en tillräckligt hög skyddsnivå för datalagrade uppgifter (se domen p. 67). Enligt vår mening förefaller det emellertid mindre sannolikt att EU-domstolens avsikt har varit att ändra förutsättningarna för tillämpningen av kommissionens beslut om adekvat skyddsnivå. Om denna tolkning vore riktig, borde dessutom kommissionen rimligtvis ha tagit initiativ till att se över sina beslut i syfte att möjliggöra för medlemsstaterna att förbjuda lagring utanför EU. Några sådana initiativ har såvitt vi har erfarit inte tagits. Enligt vår mening framstår det därför som mest förnuftigt att inte på nationell nivå införa ett generellt förbud som står i strid med kommissionens beslut. Ett förbud mot lagring

utanför EU skulle dessutom strida mot Sveriges åtaganden enligt dataskyddskonventionen.

Det kan i sammanhanget påpekas att leverantörernas tystnadsplikt och deras skyldighet att se till att beslut om inhämtning av uppgifter kan verkställas inte påverkas av var uppgifterna lagras. Även om uppgifterna skulle lagras i tredje land har leverantörerna således skyldighet att t.ex. se till att verkställigheten sker på ett sådant sätt att den inte röjs.

7 Inhämtning av abonnemangsuppgifter

7.1 Inledning

En av de brister i datalagringsdirektivet som EU-domstolen pekade på i sin dom var att direktivet inte angav några objektiva kriterier för att avgränsa de nationella myndigheternas tillgång till och användning av de lagrade uppgifterna. Domstolen ansåg därför att direktivet inte säkerställde att uppgifterna bara kunde användas för bekämpning av brott som kan anses vara av tillräckligt allvarligt slag för att motivera det aktuella ingreppet. Inte heller reglerades i direktivet vilka formella och materiella villkor som skulle gälla och vilka krav som skulle ställas på förfarandet för tillgång till uppgifterna. Domstolen noterade också att tillgången till uppgifter inte var underkastad någon förhandskontroll av en domstol eller oberoende myndighet som har till uppgift är att se till att tillgången begränsas till vad som är strikt nödvändigt.

Abonnemangsuppgifter som lagras med stöd av de svenska datalagringsreglerna får lämnas ut till de brottsbekämpande myndigheterna enligt bestämmelsen i 6 kap. 22 § första stycket 2 LEK. Bestämmelsen ställer inte några krav på att den brottslighet som uppgifterna lämnas ut för ska vara av någon viss svårhetsgrad. Vidare får uppgifter hämtas in efter beslut av den brottsbekämpande myndigheten och således utan föregående kontroll av en oberoende instans.

I analysen gjordes bedömningen att en nationell lagstiftning som tillåter att den aktuella typen av uppgifter – uppgifter om vem som har en viss adress eller ett visst telefonnummer – kontrolleras och lämnas ut till brottsbekämpande myndigheter för att bekämpa även annan brottslighet än sådan som objektivt sett kan betecknas som allvarlig inte i sig kan anses stå i strid med den unionsrättsliga proportionalitetsprincipen. Det framhölls också att det av EU-dom-

stolens dom inte kan utläsas att rättighetsstadgan och unionsrättens allmänna principer innebär att det är nödvändigt att inrätta en ordning med förhandsprövning av varje slag av åtkomst till uppgifter. När det gäller inhämtning av abonnemangsuppgifter ansågs det tillräckligt med en oberoende kontroll och tillsyn i efterhand. Det framhölls dock att det inte är möjligt att vara helt säker på att den nuvarande utformningen av tillsynsansvaret och myndigheternas rutiner för dokumentation och loggning av beslut om inhämtning av abonnemangsuppgifter fullt ut tillgodoser kraven på en effektiv kontroll, och att svensk rätt under alla omständigheter inte bör balansera på gränser för vad som är tillåtet enligt unionsrätten och Europakonventionen (Ds 2014:23 s. 69 ff.).

Enligt våra direktiv ska vi, med utgångspunkt i den utförda analysen, föreslå de förändringar som bedöms lämpliga för att stärka skyddet för den personliga integriteten i förhållande till den svenska datalagringsregleringen. Mot bakgrund av vad som anfördes i analysen är en av de frågor som utredningen har att överväga således om det finns behov av åtgärder som förstärker kontrollen över de brottsbekämpande myndigheternas tillämpning av reglerna om inhämtning av abonnemangsuppgifter.

7.2 Vilket integritetsintrång innebär utlämnandet av abonnemangsuppgifter?

Vid bedömningen av vilket kontrollsystem som bör krävas när det gäller de brottsbekämpande myndigheternas tillgång till en viss typ av uppgift har det stor betydelse hur integritetskänslig uppgiften typiskt sett är och hur den används i den brottsbekämpande verksamheten.

Det integritetsintrång som en viss åtgärd som vidtas i brottsbekämpande verksamhet leder till är alltid beroende av omständigheterna i det enskilda fallet. Däremot har det ansetts möjligt att jämföra olika åtgärder utifrån det integritetsintrång som de typiskt sett kan leda till. Det handlar då om att värdera de möjligheter till integritetsintrång som *lagstiftningen* om de olika åtgärderna erbjuder.

När det gäller de hemliga tvångsmedlen brukar hemlig övervakning av elektronisk kommunikation anses medföra ett typiskt sett mindre integritetsintrång än hemlig avlyssning av elektronisk kom-

munikation eftersom det förstnämnda tvångsmedlet inte ger någon information om innehållet i kommunikationen (se t.ex. prop. 2002/03:74 s. 23 f). Hemlig kameraövervakning och hemlig avlyssning av elektronisk kommunikation har – trots att metoderna är olika varandra och därmed svåra att jämföra – ansetts kunna leda till integritetsintrång på typiskt sett likvärdiga nivåer (se t.ex. prop. 1995/96:85 s. 21 f.). Hemlig rumsavlyssning har pekats ut som det hemliga tvångsmedel som typiskt sett medför det största intrånget (se t.ex. prop. 2013/14:237 s. 70).

Med uppgifter om abonnemang avses t.ex. uppgifter om abonnentens nummer, namn, titel och adress. Även s.k. IMSI-nummer har ansetts falla in under kategorin uppgift om abonnemang. Det är självfallet så att de brottsbekämpande myndigheterna liksom andra inhämtar uppgifter om abonnemang genom att utnyttja öppna källor, t.ex. telefonkatalog och internet. För uppgifter som inte på det viset är öppna genom avtalet mellan leverantören och kunden, t.ex. hemliga telefonnummer och ip-adresser, utnyttjas i stället bestämmelserna i lagen om elektronisk kommunikation.

De olika typerna av abonnemangsuppgifter har det gemensamt att de – isolerade från andra uppgifter – inte kan användas för att kartlägga enskilda individer. För att abonnemangsuppgifter ska kunna användas på det sättet krävs att de kombineras med annan information. Till exempel kan abonnemangsuppgifter begäras ut för att få reda på vem som tilldelats en viss dynamisk ip-adress under en viss tidsperiod. Utan någon annan information, t.ex. i fråga om hur ip-adressen har använts under perioden, säger uppgiften ingenting om den aktuella abonnentens kommunikation. Om myndigheterna däremot känner till att en adress har använts för någon viss kommunikation, t.ex. för att skicka ett hotfullt meddelande, kan uppgiften om vem som abonnerade på adressen när kommunikationen ägde rum givetvis ha stor betydelse. På motsvarande sätt kan en uppgift om vilket telefonnummer en viss person använder kombineras med information om hur numret har använts. Uppgifterna kan då användas för att t.ex. kartlägga en misstänkts kontaktnät. En uppgift om att en misstänkt person abonnerar på ett visst telefonnummer kan också vara nödvändig för att ett beslut om t.ex. hemlig avlyssning eller övervakning av elektronisk kommunikation ska kunna meddelas. Utan tillgång till annan information kan uppgiften om

vilket telefonnummer personen använder däremot inte användas för kartläggning.

Utlämnandet av abonnemangsuppgifter innebär ett visst integritetsintrång eftersom det innebär att abonnentens identitet röjs. Nivån av integritetsintrång kan också variera något beroende på vilken uppgift som lämnas ut. Vid användning av internet lämnar användaren ofta fler avtryck efter sig än vid t.ex. användning av telefoni. En uppgift om vem som har använt en viss ip-adress kan därför typiskt sett anses vara något mer känslig än motsvarande uppgift i fråga om ett telefonnummer. När de brottsbekämpande myndigheterna begär ut en uppgift om vem som använt en viss ip-adress vid ett visst tillfälle torde dock syftet ofta vara att kontrollera vem som t.ex. har skrivit ett specifikt meddelande eller liknande, snarare än att i allmänhet kartlägga den aktuella personens aktiviteter på internet.

Enligt vår uppfattning kan det sammantaget inte råda någon tvekan om att abonnemangsuppgifter typiskt sett är klart mindre integritetskänsliga än många andra kategorier av uppgifter, t.ex. trafik- och lokaliseringsuppgifter. Vid den bedömningen beaktar utredningen särskilt att enstaka abonnemangsuppgifter i sig inte gör det möjligt att kartlägga abonnentens kommunikationer, utan snarare är att betrakta som ett slags komplement till andra uppgifter. Vi bedömer därför att uppgifter om vem som innehar eller använder ett visst nummer – i jämförelse med många andra uppgifter – inte är särskilt integritetskänsliga. Abonnemangsuppgifter får också lämnas ut till flera olika myndigheter för andra ändamål än brottsbekämpande verksamhet. Till exempel får uppgifter under vissa förutsättningar lämnas ut till en myndighet som behöver uppgiften för delgivning (6 kap. 22 § första stycket 1 LEK), till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet (första stycket 4) och till Skatteverket om verket finner att uppgiften har betydelse för ett ärende om kontroll av skatt eller avgift eller rätt folkbokföringsort (första stycket 5). Detta förhållande stödjer slutsatsen att abonnemangsuppgifter inte anses vara särskilt integritetskänsliga.

Det kan i sammanhanget också noteras att uppgifter som går utöver vad som kan anses som identitetsuppgifter, t.ex. vilka andra ip-adresser som användaren har kommunicerat med, vilka hemsidor som en viss ip-adress har besökt och liknande, inte omfattas av den aktuella bestämmelsen i LEK.

7.3 Rutiner för dokumentation och loggning

Den öppna polisen har uppgett att Rikspolisstyrelsen tidigare har tagit fram nationella riktlinjer för hanteringen av uppgifter om elektronisk kommunikation.[1] I tiden före den nya polisorganisationen hanterades beslut och dokumentation avseende inhämtning av uppgifter enligt LEK av respektive polismyndighet enligt lokal rutin.

Sedan den 1 januari 2015 gäller enligt myndighetens arbetsordning att möjligheterna till delegation har delats in i tre olika kompetensnivåer utifrån den beslutskompetens som ärendena kräver. Beslut om inhämtning av uppgifter enligt 6 kap. 22 § första stycket 2 LEK har delats in i kompetensnivå 2, vilket innebär *"förmåga att hantera komplicerade och svårbedömda ärenden; Beslutsfattaren ska ha erfarenhet inom beslutsområdet och dessutom ha fördjupade kunskaper på området genom utbildning eller på annat sätt."* Detta är den miniminivå som gäller nationellt. Vid delegation ska även lämplighet vägas in.

Den Nationella operativa avdelningen (NOA) har från och med den 1 januari 2015 ett processansvar och arbetar för att skapa en mer enhetlig hantering. Till exempel är avsikten att göra ett beställningsformulär som blir nationellt och generiskt. Däremot finns inga enhetliga rutiner om hur dessa förfrågningar dokumenteras eller loggas, utan hur det hanteras följer av gängse regler om diarieföring. Polisen har inte en sammanställning av dessa förfrågningar och kan därför inte få fram uppgifter om hur många eller hur dessa beställningar ser ut i dagsläget. Lösningen avseende detta kan i framtiden vara att ett elektroniskt system tas fram där man loggar förfrågningar och att en behörighetsgräns automatiskt byggs in i systemet för att kunna inhämta dessa typer av uppgifter. Polisen har ambitionen att detta ska genomföras i framtiden.

Säkerhetspolisen har framfört till utredningen att det inte finns någon myndighetsgemensam rutin för dokumentation av beslut om inhämtning av abonnemangsuppgifter. Ett exempel på ett system som används är att beslutsfattare på Säkerhetspolisen kontaktar den operatör som är berörd med en fråga kring abonnent på det eller de teledaresser som är av intresse. Om operatören kan lämna abonnentuppgifter till teleadresser, upprättas en notering om detta

[1] dnr POA-102-4352/12

i ärendets logg eller i en särskild promemoria i det digitala ärendehanteringssystemet. Av denna uppgift framgår vem som ställde frågan, vilken operatör som var mottagare, vilken teleadress och vilken abonnent som var aktuell.

7.4 Kontrollsystemet

Det finns i dagsläget inte några regler som specifikt tar sikte på tillsyn över de brottsbekämpande myndigheternas inhämtning av uppgifter om abonnemang enligt LEK. Möjligheten att hämta in sådana uppgifter anses inte vara ett hemligt tvångsmedel (se prop. 2013/14:273 s. 134) och omfattas därför inte av SIN:s tillsyn över användningen av sådana tvångsmedel. Däremot står tillämpningen av reglerna under den mer övergripande tillsyn som utövas av JO och JK.

Normalt är inhämtning av abonnemangsuppgifter ett led i en automatiserad behandling av personuppgifter. Sådan behandling står således under Datainspektionens tillsyn. Bestämmelser om personuppgiftsbehandling finns – vid sidan av i personuppgiftslagen – i t.ex. kustbevakningsdatalagen (2012:145), polisdatalagen, lagen om polisens allmänna spaningsregister, lagen (2005:787) om behandlingen av uppgifter i Tullverkets brottsbekämpande verksamhet och lagen (1999:90) om behandlingen av personuppgifter vid Skatteverkets medverkan i brottsutredningar och anknytande förordningar samt förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet. För Polisens och Säkerhetspolisens personuppgiftsbehandling enligt polisdatalagen har även SIN i uppgift att utöva tillsyn över behandlingen. Datainspektionens och SIN:s tillsyn inriktas i första hand på att kontrollera att myndigheterna följer de föreskrifter som gäller för behandlingen av personuppgifter.

Datainspektionens och SIN:s delvis överlappande tillsynsansvar när det gäller Polisens och Säkerhetspolisens personuppgiftsbehandling är för närvarande under utredning. Frågan hänger delvis samman med omorganisationen av polisen. I Polisorganisationskommitténs betänkande *Tillsyn över polisen* (SOU 2013:42) framhöll kommittén att det kan ifrågasättas om det är lämpligt att två granskningsorgan i vissa delar har identiska tillsynsuppdrag. Bland annat ansågs det vara mindre lämpligt att det råder oklarhet för de objekts-

ansvariga och för allmänheten om vilket tillsynsorgan som ytterst ansvarar för granskningen av så viktiga frågor som polisens behandling av känsliga personuppgifter. Det ansågs också sannolikt att överlappande granskningsuppdrag leder till en mindre effektiv tillsyn som orsakar störningar i den granskade verksamheten som sådan. Vidare ansågs det problematiskt att tillsynsorganen skulle kunna komma till olika slutsatser vid sina respektive granskningar och att det kunde vara svårare för polisen att tillgodogöra sig resultatet av granskningar från två olika tillsynsorgan.

Kommittén konstaterade sammanfattningsvis att det finns flera omständigheter som talar för att de tillsynsuppgifter som SIN har överlappande med Datainspektionen bör hanteras endast inom en av dessa organisationer. Enligt kommitténs mening var det dock för tidigt att utvärdera om tillsynen över polisens personuppgiftsbehandling – som vad avser den öppna polisen så sent som i mars 2012 lades till SIN:s tillsynsområde – bör utföras i annan ordning. Kommittén ansåg att denna fråga inom inte allt för lång tid borde följas upp och närmare utvärderas av regeringen.

Den 6 februari 2014 beslutade regeringen om tilläggsdirektiv till kommittén (dir. 2014:17). I det nya uppdraget ingår bl.a. att analysera hur tillsynen över polisens personuppgiftsbehandling kan organiseras så att överlappning mellan olika tillsynsmyndigheter i så stor utsträckning som möjligt undviks. Uppdraget ska redovisas senast den 30 april 2015.

Vidare beslutade regeringen den 22 december 2014 att ge en särskild utredare i uppdrag att överväga hur ett i högre grad samlat integritetsskydd kan fungera inom en och samma myndighetsstruktur genom att tillsynen över behandling av personuppgifter samlas hos en myndighet (dir 2014:164). I uppdraget ingår bl.a. att lämna förslag på hur tillsynen – helt eller delvis – kan samlas hos en myndighet samt hur myndighetens uppdrag bör vara utformat och vilka befogenheter myndigheten bör ha för att kunna upprätthålla en effektiv tillsynsverksamhet. Uppdraget ska redovisas senast den 31 januari 2016.

7.5 Utredningens förslag

Utredningens förslag: Beslut om inhämtning av abonnemangsuppgifter ska fattas av myndigheten. Myndighetschefen ska dock få delegera uppgiften att fatta sådana beslut till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Delegationsbesluten ska dokumenteras av myndigheten. Därutöver ska beslut om inhämtning av abonnemangsuppgifter alltid kunna fattas av förundersökningsledaren.

Det ska införas en uttrycklig regel om att beslut om inhämtning av abonnemangsuppgifter i brottsbekämpande verksamhet ska dokumenteras. I ett beslut om inhämtning av uppgifter ska skälen för beslutet anges. Det ska också anges vem som har fattat beslutet samt vilken brottslighet och vilka abonnemangsuppgifter beslutet avser.

Det ska förtydligas i lagen om elektronisk kommunikation att uppgifter om abonnemang får, utöver i en förundersökning, hämtas in även i de brottsbekämpande myndigheternas underrättelseverksamhet.

7.5.1 En särskild tillsynsuppgift?

En möjlig åtgärd för att stärka kontrollen över inhämtningen av abonnemangsuppgifter skulle kunna vara att ge ett tillsynsorgan i uppdrag att utöva tillsyn som specifikt tar sikte på de brottsbekämpande myndigheternas tillämpning av regeln i 6 kap. 22 § första stycket 2 LEK. En sådan uppgift skulle kunna utformas så att tillsynen bedrivs antingen på tillsynsorganets eget initiativ eller på begäran av enskild. Eftersom det handlar om inhämtning av information i brottsbekämpande verksamhet skulle det vara naturligt att den uppgiften i sådana fall anförtroddes SIN.

Vi anser dock att det är tveksamt om det är motiverat med en sådan kontroll. Det är viktigt SIN:s effektivitet som kontrollmekanism långsiktigt kan upprätthållas. Det är därför värdefullt att SIN kan koncentrera sina resurser på att granska den mer integritetskänsliga informationsinhämtningen. I annat fall finns det en risk för att kontrollsystemet urvattnas och dess effektivitet försämras.

Av betydelse för bedömningen är också hur effektivt ett tillsynsuppdrag av det aktuella slaget kan förväntas vara. SIN:s tillsyn ska särskilt syfta till att säkerställa att den granskade verksamheten bedrivs i enlighet med lag eller annan författning. När nämnden beslutar att inleda tillsyn på eget initiativ görs detta främst utifrån en bedömning av var risken för en felaktig rättstillämpning hos de granskade myndigheterna är som störst (se t.ex. SIN:s årsredovisning för 2013, dnr 7-2014, s. 10). Nämnden använder sig i huvudsak av en tematisk tillsynsmetodik där gällande författningar och interna föreskrifter och riktlinjer från berörda myndigheter först analyseras. Därefter undersöks rutiner och praktisk tillämpning.

Eftersom abonnemangsuppgifter inte har ansetts vara särskilt integritetskänsliga innehåller reglerna om inhämtning av sådana uppgifter, till skillnad från reglerna om hemliga tvångsmedel, relativt få förutsättningar för inhämtningen. Det finns t.ex. inte något krav på att den brottslighet som inhämtningen avser ska vara av något visst allvar (se prop. 2011/12:55 s. 102 f.). Enligt utredningens mening är det mot den bakgrunden svårt att se att inhämtningen av abonnemangsuppgifter skulle vara förknippade med några direkta risker för felaktig rättstillämpning. Visserligen har det framförts till oss att det förekommer att frågan om vilka uppgifter som kan anses utgöra uppgifter om abonnemang – i förhållande till andra uppgiftskategorier för vilka strängare krav gäller – ger upphov till meningsskiljaktigheter mellan teleoperatörerna och de brottsbekämpande myndigheterna. Denna omständighet skulle kunna tala för att SIN borde få i uppgift att kontrollera myndigheternas tillämpning av reglerna om inhämtning av abonnemangsuppgifter. Samtidigt är SIN:s tillsynsområde inte avgränsat genom angivandet av gällande lagar om hemliga tvångsmedel (se 1 § lagen [2007:980] om tillsyn över viss brottsbekämpande verksamhet). Det beror bl.a. på att tillsynen omfattar även fall då användningen av metoderna sker helt eller delvis otillåtet (prop. 2006/07:133 s. 80). Detta innebär att, om en brottsbekämpande myndighet skulle använda reglerna om inhämtning av abonnemangsuppgifter för att skaffa sig tillgång till exempelvis trafikuppgifter, så omfattas det förfarandet av nämndens tillsyn. I den mån det skulle komma fram indikationer på sådana felaktigheter kan SIN alltså redan enligt dagens regler granska myndigheternas beslut om inhämtning av abonnemangsuppgifter. Härtill kommer att SIN:s tillsyn, för att vara effektiv, inte bör spridas för mycket

och till att avse områden som från integritetsskyddssynpunkt framstår som mindre angelägna.

Sammantaget bedömer vi att behovet av en tillsynsfunktion som specifikt tar sikte på att granska inhämtningen av abonnemangsuppgifter inte framstår som särskilt stort. Vidare har SIN framfört att nämnden ställer sig tveksam till nyttan av sådan tillsyn. De skäl som talar för att införa regler om tillsyn som är specifikt inriktade på de brottsbekämpande myndigheternas tillämpning av reglerna om tillgång till abonnemangsuppgifter är därför inte tillräckligt starka för att de ska uppväga nackdelarna med en sådan reglering. Den mer övergripande tillsyn som utövas av JO och JK samt, såvitt gäller myndigheternas personuppgiftsbehandling, av Datainspektionen och SIN får i detta sammanhang vara tillräcklig. Som framgår nedan föreslår vi dock att det ska införas regler om att beslut om inhämtning av abonnemangsuppgifter ska dokumenteras. Detta kan förväntas bidra till att den tillsyn som finns kan bedrivas mer effektivt.

7.5.2 Underrättelse till enskild?

När hemliga tvångsmedel används i en förundersökning är huvudregeln att den som är eller har varit misstänkt för brott samt vissa innehavare av platser, teleadresser och elektroniska kommunikationsutrustningar ska underrättas om åtgärden i efterhand. Underrättelseskyldigheten omfattar bl.a. uppgifter om vilka tvångsmedel som har använts, vilken plats, adress eller utrustning som övervakats eller avlyssnats samt när detta har skett.

Syftet med underrättelseskyldigheten är bl.a. att den enskilde ska få möjlighet att bedöma vilket integritetsintrång som åtgärden har inneburit och att reagera mot vad han eller hon kan anse har varit en rättsstridig åtgärd. En skyldighet att lämna en sådan underrättelse har även ansetts kunna ha en återhållande verkan på användningen av hemliga tvångsmedel och bidra till att prövningen inför ett beslut sker på ett än mer noggrant sätt (prop. 2006/07:133 s. 30). Ett krav på att enskilda ska underrättas är således en åtgärd som syftar till att förbättra kontrollen över tillämpningen av reglerna.

Som framgått ovan (avsnitt 3.5.4.2) finns det ett flertal undantag från skyldigheten att underrätta enskilda om att hemliga tvångsmedel har använts. Om vissa former av sekretess gäller för uppgifterna

i en underrättelse, ska denna skjutas upp till dess att sekretess inte längre gäller. Om sekretess fortfarande gäller efter ett år, behöver underrättelse över huvud taget inte lämnas. Vissa utredningar om brott som faller inom Säkerhetspolisens ansvarsområde är också helt undantagna från underrättelseskyldighet.

När det gäller inhämtning av uppgifter i underrättelseverksamhet enligt inhämtningslagen finns ingen motsvarighet till rättegångsbalkens krav på underrättelse till enskild. Frågan om ett sådant krav borde införas övervägdes dock i samband med att lagen infördes. Regeringen uttalade då att en skyldighet att underrätta enskilda om inhämtning av uppgifter i underrättelseverksamhet, med hänsyn till verksamhetens framåtblickande perspektiv och övergripande natur, skulle riskera att motverka huvudsyftet med underrättelseverksamheten. En sådan skyldighet skulle därför behöva förses med en rad undantag. Vidare skulle det enligt regeringen i många fall kunna ta lång tid innan en underrättelse kunde lämnas, och den eventuella identifiering och granskning av kommunikationen som måste föregå en underrättelse skulle kunna innebära ett ytterligare integritetsintrång. I många fall torde det enligt regeringen inte heller vara möjligt eller i vart fall förenat med betydande svårighet att identifiera den person som varit föremål för övervakningen. Det beaktades även att användningen av uppgifterna i en förundersökning förutsätter tillstånd av domstol till hemlig övervakning av elektronisk kommunikation. I de fall där uppgifterna innebär en påtaglig integritetspåverkan för en enskild skulle därmed bestämmelserna om underrättelseskyldighet i rättegångsbalken bli tillämpliga (prop. 2011/12:55 s. 107).

I samma lagstiftningsärende övervägdes även frågan om det borde införas en underrättelseskyldighet avseende inhämtandet av abonnemangsuppgifter. Regeringen anförde att inhämtning av sådana uppgifter inte innebär ett så betydande integritetsintrång att det bör medföra ett krav på underrättelse (nämnda prop. s. 108). Vi instämmer i den bedömningen. Visserligen skulle ett krav på underrättelse kunna bidra till ökad kontroll över de brottsbekämpande myndigheternas tillämpning av reglerna. En sådan skyldighet skulle dock, liksom är fallet med de hemliga tvångsmedlen, behöva förses med omfattande undantag med hänsyn till sekretessintressen. Underrättelsefrågan skulle därför i många fall behöva hållas öppen under lång tid vilket innebär att det blir nödvändigt för de brottsbekäm-

pande myndigheterna att bevaka och fortlöpande pröva sekretessfrågor. En sådan ordning skulle vara orimligt resurskrävande för myndigheterna sett i förhållande till de aktuella uppgifternas integritetspåverkan. Det bör därför inte införas något krav på underrättelse till enskild avseende inhämtningen av abonnemangsuppgifter.

7.5.3 Parlamentarisk kontroll?

Regeringen redovisar årligen uppgifter om tillämpningen av reglerna om de hemliga tvångsmedlen till riksdagen. Bakgrunden till denna ordning är att det ansågs ligga en betydelsefull rättssäkerhetsgaranti i att riksdagen ges möjlighet till insyn i hur lagstiftningen tillämpas (se t.ex. bet. 1981/82:JuU54 s. 4).

Frågan om regeringens redovisning bör omfatta även de brottsbekämpande myndigheternas inhämtning av abonnemangsuppgifter i brottsbekämpande verksamhet har tidigare varit föremål för vissa överväganden. Detta har dock inte lett till att det införts någon sådan ordning (se t.ex. bet. 2011/12:JuU8 s. 33 och prop. 2013/14:237 s. 135).

För att en redovisning till riksdagen ska fylla sitt syfte är det inte tillräckligt att bara redovisa en uppgift om antalet inhämtningsbeslut. Om redovisningen ska kunna användas som underlag för en bedömning av om tillämpningen av reglerna lever upp till kraven på proportionalitet, måste den även innehålla andra uppgifter, t.ex. i fråga om vilken nytta tillämpningen leder till i den brottsbekämpande verksamheten. En sådan redovisning skulle alltså kräva att de brottsbekämpande myndigheterna utarbetar rutiner för att följa upp samtliga beslut om inhämtning av abonnemangsuppgifter och göra bedömningar av vilken nytta dessa lett till. Utredningen bedömer att en sådan ordning skulle ta större resurser i anspråk än vad som är motiverat av nyttan med en redovisning.

7.5.4 Beslut om inhämtning av abonnemangsuppgifter bör fattas på en viss nivå

Enligt 6 kap. 22 § första stycket 2 LEK ska uppgift om abonnemang som gäller misstanke om brott lämnas till en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet. Frågan om utlämnande ska prövas av den brottsbekämpande myndigheten. Däremot finns det inte några regler som anger vem inom den aktuella myndigheten som har rätt att fatta beslut om att hämta in sådana uppgifter. Ett sätt att förstärka kontrollen över tillämpningen av reglerna om inhämtning av abonnemangsuppgifter skulle kunna vara att begränsa kretsen av personer som har rätt att fatta sådana beslut. En sådan regel finns t.ex. i inhämtningslagen (4 §) av vilken det framgår att beslut om inhämtning ska fattas av myndighetschefen eller, efter särskild delegation, av annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. I förarbetena anges att delegation bör kunna ske till t.ex. myndighetschefens ställföreträdare, rikskriminalchefen, biträdande rikskriminalchefen, biträdande säkerhetspolischefen, biträdande länspolismästare, länskriminalchefer, chefer för operativ verksamhet och chefer för underrättelseverksamhet (prop. 2011/12:55 s. 123). Den som har fått sådan delegation får inte fatta beslut om inhämtning i verksamhet som han eller hon deltar i (4 § andra stycket).

Det är rimligt att befogenheten att fatta beslut om inhämtning av abonnemangsuppgifter inte ska tillkomma samtliga anställda inom de aktuella myndigheterna. Det finns därför skäl att införa regler som begränsar den personkrets som kan besluta om tillgång till uppgifterna (jfr EU-domstolens dom p. 62).

De kompetenskrav som Polismyndigheten sedan den 1 januari 2015 ställer för att beslutskompetens ska kunna delegeras framstår som rimliga. Detta motsvarar i huvudsak den reglering som i dag gäller enligt inhämtningslagen. Det bör därför föreskrivas att beslut om inhämtning av abonnemangsuppgifter fattas av myndighetschefen med möjlighet för denne att delegera uppgiften till sådana anställda vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Med tanke på att abonnemangsuppgifter generellt sett inte är lika integritetskänsliga som de uppgifter som kan hämtas in enligt inhämtningslagen finns dock inte

anledning att begränsa möjligheterna för den som beslutsbefogenheten delegeras till att fatta beslut i operativ verksamhet som han eller hon deltar i.

Reglerna om inhämtning av abonnemangsuppgifter i brottsbekämpande verksamhet kan, som utvecklas närmare nedan, användas både under en förundersökning och i underrättelseverksamhet. Normalt leds en förundersökning av antingen en åklagare eller en förundersökningsledare vid Polismyndigheten eller Säkerhetspolisen. Förundersökningsledaren har, enligt vad som framgår av 1 a § förundersökningskungörelsen (1947:948), ansvar för förundersökningen i dess helhet. Förundersökningsledaren ska se till att utredningen bedrivs effektivt och att den enskildes rättssäkerhetsintressen tas till vara.

Vid delegering av beslutanderätt och arbetsuppgifter inom Polismyndigheten eller Säkerhetspolisen ska det särskilt beaktas bl.a. om uppgiften innebär att grundlagsskyddade fri- och rättigheter kan komma att inskränkas. I sådana fall får uppgiften överlämnas endast till en särskilt kvalificerad beslutsfattare som har den utbildning, kompetens och erfarenhet som krävs. Polismyndigheten eller Säkerhetspolisen får inte överlämna åt någon annan än en polisman att leda förundersökning eller att avgöra frågor som Polismyndigheten enligt rättegångsbalken ska besluta i (8 § polisförordningen [2014:1104]).

Oavsett om förundersökningen är polis- eller åklagarledd är förundersökningsledarens uppgifter i huvudsak desamma. En åklagare som leder en förundersökning har dock rätt att besluta i betydligt fler frågor än polisiära förundersökningsledare eftersom vissa typer av beslut får fattas endast av åklagare. Även polisiära förundersökningsledare har dock en rad befogenheter, bl.a. att fatta vissa beslut som berör inskränkningar i enskildas fri- och rättigheter. Till exempel har förundersökningsledaren befogenheter att fatta beslut om hämtning till förhör (23 kap. 7 § rättegångsbalken och 6 § förundersökningskungörelsen), beslag (27 kap. 4 § andra stycket rättegångsbalken), husrannsakan (28 kap. 4 § rättegångsbalken) samt kroppsvisitation och kroppsbesiktning (28 kap. 13 § rättegångsbalken).

Vid sidan av polis- och åklagarmyndighet har även Tullverket och Kustbevakningen, inom vissa i lag angivna områden, befogenhet att leda förundersökning. I dessa fall leds förundersökningen av sär-

skilda befattningshavare som förordnas av myndigheten för att fullgöra uppgiften som förundersökningsledare (se t.ex. 19 § lagen [2000:1225] om straff för smuggling och 11 kap. 4 § andra stycket lagen [1980:424] om åtgärder mot förorening från fartyg).

Mot bakgrund av de krav som alltså ställs på den som anförtros uppgiften att leda en förundersökning samt de relativt långtgående befogenheter som förundersökningsledare har i övrigt, är det naturligt att beslut om inhämtning av abonnemangsuppgifter även utan särskild delegation får fattas av förundersökningsledaren.

7.5.5 Krav på dokumentation

Bestämmelser om skyldighet att dokumentera beslut som fattas i den brottsbekämpande verksamheten ökar möjligheterna till kontroll i efterhand. En uttrycklig regel om att beslut om inhämtning av abonnemangsuppgifter ska dokumenteras kan alltså förväntas bidra till att den tillsyn som utövas av JO, JK, Datainspektionen och SIN blir mer effektiv. En sådan regel bör därför införas. Kravet på dokumentation bör omfatta skälen för beslutet. Vidare bör det dokumenteras vem som har fattat beslutet samt vilken brottslighet och vilka abonnemangsuppgifter som beslutet avser.

7.5.6 Verkställighet

Det finns i dagsläget inte några bestämmelser som reglerar vilka uppgifter de brottsbekämpande myndigheterna ska lämna till operatörerna i samband med verkställighet av beslut om inhämtning av uppgifter om elektronisk kommunikation. Det har kommit fram att det som i praktiken lämnas i huvudsak är en uppgift om vilken lagstiftning som ligger till grund för beslutet och sådana uppgifter som är nödvändiga för att beslutet ska kunna verkställas (se även avsnitt 9.3.3.5). I en begäran om abonnemangsuppgifter anges alltså vilka uppgifter myndigheten begär tillgång till och att begäran avser ett beslut enligt 6 kap. 22 § första stycket 2 LEK. Därutöver lämnas uppgift om myndighetens diarienummer etc. Enligt vår uppfattning framstår detta som en lämplig ordning.

7.5.7 Utlämnande för andra ändamål

Enligt 6 kap. 22 § LEK får abonnemangsuppgifter lämnas ut även till en rad olika myndigheter för andra ändamål än brottsbekämpande verksamhet. För vissa av dessa ändamål torde det ligga i den enskildes eget intresse att uppgifterna lämnas ut, t.ex. då en uppgift behövs för att efterforska personer som har försvunnit på fjället (första stycket 3) eller i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall (första stycket 6). I vissa andra fall kan det däremot normalt inte anses ligga i den enskildes intresse att uppgifter lämnas ut. Exempelvis får abonnemangsuppgifter i vissa situationer lämnas ut till en myndighet som behöver den för delgivning (första stycket 1), till Kronofogdemyndigheten om uppgiften behövs i exekutiv verksamhet (första stycket 4) och till Skatteverket, om uppgiften är av väsentlig betydelse i ett ärende om bl.a. kontroll av skatt (första stycket 5). Det skulle, åtminstone när det gäller de sistnämnda situationerna, kunna övervägas om motsvarande krav på dokumentation och beslutsnivå borde ställas även när det gäller andra utlämnanden än sådana som avser brottsbekämpande verksamhet. I dessa fall får dock inte några uppgifter som lagras enligt de tvingande datalagringsreglerna lämnas ut (se 6 kap. 16 c § LEK). Frågan om vilka krav som ska gälla för dessa utlämnanden omfattas därmed inte av våra direktiv.

7.5.8 Utlämnande av abonnemangsuppgifter i underrättelseverksamhet

Säkerhetspolisen har framfört till utredningen att det bör klargöras att bestämmelsen i 6 kap. 22 § första stycket 2 LEK kan tillämpas i de brottsbekämpande myndigheternas underrättelseverksamhet. Bestämmelsen är i dagsläget utformad så att en uppgift om abonnemang får lämnas ut om den rör ”misstanke om brott”.

Som framgår av avsnitt 3.5.3.2 kunde brottsbekämpande myndigheter tidigare hämta in trafikuppgifter med stöd av LEK (6 kap. 22 § första stycket 3 LEK i dess lydelse före den 1 juli 2012). Även den bestämmelsen krävde enligt sin ordalydelse att uppgifterna rörde misstanke om brott. Trots detta var den inte begränsad till en förundersökningssituation utan ansågs kunna användas även i underrättelseverksamheten (se SOU 2009:1 s. 72 f.). I samband med att

bestämmelsen upphävdes uttalade regeringen att den skulle ersättas av bl.a. regleringen i inhämtningslagen (prop. 2011/12:55 s. 1).

Enligt vår mening bör regeln i 6 kap. 22 § första stycket 2 LEK rimligtvis tolkas på samma sätt som den tidigare regeln i första stycket 3. Detta stämmer för övrigt väl överens med den tolkning av bestämmelsen som Polismetodutredningen har gjort (a. SOU s. 187). Enligt uppgift från polisen är det också så bestämmelsen tillämpas i dagsläget.

Mot den angivna bakgrunden står det klart att gällande rätt innebär att de brottsbekämpande myndigheterna har befogenhet att begära tillgång till abonnemangsuppgifter redan på underrättelsestadiet. Detta är en såväl rimlig som logisk ordning, inte minst med tanke på att myndigheterna i detta skede kan få tillgång till mer känsliga uppgifter enligt reglerna i inhämtningslagen.

Av rättssäkerhetsskäl bör lagstiftning som innebär att brottsbekämpande myndigheter kan få tillgång till uppgifter som berör enskildas privatliv vara så tydlig som möjligt. Uttrycket ”misstanke om brott” för tankarna till en redan begången konkret gärning vilket är mindre väl förenligt med de brottsbekämpande myndigheternas underrättelseverksamhet som i huvudsak är inriktad på att avslöja om viss, inte närmare specificerad, brottslighet har ägt rum, pågår eller kan antas komma att begås. Vi instämmer därför i Säkerhetspolisens uppfattning att lagtexten bör justeras för att klargöra att abonnemangsuppgifter får hämtas in i underrättelseverksamhet.

På flera håll i lagstiftningen används uttrycket ”brottslig verksamhet” för att avgränsa åtgärder som får vidtas i sådan verksamhet (se t.ex. 2 § inhämtningslagen och 5 kap. 1 § polisdatalagen). Med uttrycket avses verksamhet av viss konkretion (se prop. 2009/10:85 s. 362 f.). Däremot krävs inte att misstanken avser en konkretiserad gärning på samma sätt som vid förundersökning. Uttrycket brottslig verksamhet har tidigare kritiserats för att vara otydligt men är numera en vedertagen avgränsning för åtgärder som vidtas i underrättelseverksamhet (se prop. 2013/14:237 s. 104). Uttrycket bör användas även i den aktuella bestämmelsen i LEK.

8 Uppgifter som omfattas av yrkesmässig tystnadsplikt

8.1 Inledning

EU-domstolen lyfte i sin dom fram att en brist i datalagringsdirektivet var att det inte innehöll några undantag från lagringskravet vilket innebar att det var tillämpligt även på personer vilkas kommunikation enligt nationell rätt omfattas av tystnadsplikt (p. 58).

I analysen konstaterades att det synsätt som kommer till uttryck i svensk rätt när det gäller undantag från vittnesplikt och regler om avlyssningsförbud vid t.ex. telefonavlyssning innebär att det är en uppgifts innehåll som avgör om den omfattas av yrkesmässig tystnadsplikt. Det framhölls att, även om de uppgifter som kommer fram i en kommunikation i vissa situationer omfattas av tystnadsplikt, så gör inte det faktum att kommunikationen har ägt rum det. Det ansågs därför långsökt med en modell där exempelvis vissa telefonnummer på förhand skulle undantas från ett lagringskrav som i övrigt gäller generellt. Även om det i fråga om viss kommunikation i något fall kunde finnas ett intresse av att begränsa myndigheternas insyn i att kommunikation över huvud taget har förekommit bedömdes det lämpligast att säkerställa en proportionerlig avvägning mellan brottsbekämpningsintresset och integritetsintresset genom en balanserad reglering om tillgången till de lagrade uppgifterna. Det framhölls dock att detta inte hindrar att det sker fortsatta överväganden om möjligheterna att även på andra sätt förstärka skyddet för viss kommunikation.

8.2 Skyddet för yrkesmässig tystnadsplikt

8.2.1 Tystnadsplikt

Vissa person- eller yrkeskategorier är underkastade tystnadsplikt i fråga om uppgifter som de har erfarit i sin yrkesutövning. Exempelvis finns regler om tystnadsplikt för advokater i rättegångsbalken (8 kap. 4 § första stycket). Ett annat exempel är den tystnadsplikt som följer av reglerna om meddelarskydd enligt 3 kap. 3 § TF och 2 kap. 3 § YGL. Enligt dessa bestämmelser har journalister och andra som arbetar inom massmedia som huvudregel tystnadsplikt för uppgifter som röjer identitet hos den som lämnar uppgifter avsedda att offentliggöras i massmedia. Som ett ytterligare led i meddelarskyddet gäller ett principiellt efterforskningsförbud. Myndigheter och andra allmänna organ får som huvudregel inte efterforska vem som har lämnat meddelandet och som har rätt att vara anonym (3 kap. 4 § TF och 2 kap. 4 § YGL). Ytterligare exempel är den tystnadsplikt som gäller inom hälso- och sjukvården enligt 25 kap. offentlighets- och sekretesslagen (2009:400) och 6 kap. patientsäkerhetslagen (2010:659).

8.2.2 Undantag från vittnesplikt

Det är en allmän medborgerlig plikt att inställa sig som vittne vid domstol och där avlägga vittnesmål. Vittnesplikten är av grundläggande betydelse för domstolarnas möjligheter att få ett fullgott underlag för prövningen av mål och ärenden.

I flera fall får tystnadsplikten ge vika för vittnesplikten. I rättegångsbalken uppställs dock vissa begränsningar i vittnesplikten genom det s.k. frågeförbudet (36 kap. 5 § andra–sjätte styckena). Bestämmelsen har tillkommit av hänsyn till enskildas personliga integritet och privatliv. Lagstiftaren har ansett att den enskilde som huvudregel ska kunna anförtro sig till vissa angivna personer inom dessas yrkesutövning utan rädsla för att informationen ska föras vidare eller annars användas mot honom eller henne (se t.ex. prop. 2009/10:119 s. 23).

Frågeförbudet innebär att personer inom vissa yrkeskategorier, t.ex. advokater och hälso- och sjukvårdspersonal inte får höras som vittnen om något som på grund av deras ställning anförtrotts dem

eller de i samband därmed på annat sätt erfarit, med mindre än att det är medgivet i lag eller den till vars förmån tystnadsplikten gäller samtycker (andra stycket). För rättegångsombud, biträden och försvarare gäller att de får höras som vittnen om vad som anförtrotts dem för uppdragets fullgörande endast om parten medger det (tredje stycket).

Vissa begränsade undantag görs från frågeförbudet när det gäller de nu nämnda yrkeskategorierna (fjärde stycket).

Den som är präst inom ett trossamfund eller den som i ett sådant samfund har motsvarande ställning får inte höras som vittne om något som han eller hon har erfarit under bikt eller enskild själavård (femte stycket). Vidare får den som har tystnadsplikt enligt 3 kap. 3 § TF eller 2 kap. 3 § YGL höras som vittne om förhållanden som tystnadsplikten avser endast i den mån det föreskrivs i nämnda paragrafer (sjätte stycket). Slutligen gäller enligt det sjunde stycket att, om någon inte får höras som vittne enligt paragrafen, så får vittnesförhör inte heller äga rum med den som under tystnadsplikt har biträtt med tolkning eller översättning.

Frågeförbudet innebär inte något förbud mot att höra personer inom de aktuella yrkeskategorierna som vittnen. Däremot får frågor om sådant som omfattas av förbudet inte ställas. Förbudet ska beaktas självmant av domstolen, och det kan inte efterges av vittnet.

8.2.3 Avlyssningsförbud

Enligt 27 kap. 22 § rättegångsbalken får hemlig avlyssning av elektronisk kommunikation eller hemlig rumsavlyssning inte avse samtal, meddelanden eller annat tal där någon som yttrar sig på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram. Om det under avlyssningen kommer fram att det är fråga om ett sådant samtal, meddelande eller tal, ska avlyssningen omedelbart avbrytas. Detsamma gäller vid hemlig avlyssning av elektronisk kommunikation enligt lagen om preventiva tvångsmedel (11 §). Bestämmelserna innebär att den som granskar material från hemlig avlyssning genast måste avbryta granskningen så fort det står klart att samtalet omfattas av avlyssningsförbud. Något krav på att den verkställande myndigheten måste granska

materialet i realtid för att kunna avgöra när avlyssningen ska avbrytas ställs däremot inte (prop. 2013/14:237 s. 184).

Avlyssningsförbudet är utformat med utgångspunkt från bedömningen att uppgifter som på grund av hänsyn till enskildas personliga integritet inte får inhämtas genom vittnesförhör i domstol inte heller ska kunna inhämtas genom avlyssning (se prop. 2005/06:178 s. 68, prop. 2009/10:133 s. 24 och prop. 2013/14:237 s. 132).

Som framhölls i analysen har det aldrig varit aktuellt att införa någonting motsvarande ett absolut avlyssningsförbud när det gäller uppgifter som hämtas in genom hemlig övervakning av elektronisk kommunikation, alltså s.k. metadata som visar att kommunikation har ägt rum men inte vad den innehöll (Ds 2014:23 s. 55). Det synsätt som kommer till uttryck i svensk lagstiftning är att det är en uppgifts innehåll som avgör om den omfattas av skydd mot att de brottsbekämpande myndigheterna tar del av uppgiften. Däremot omfattas uppgifter om *att* kommunikation förekommit normalt inte av sådant skydd.

8.2.4 Skyldighet att förstöra upptagningar och upptecknin gar

Som ett komplement till reglerna om avlyssningsförbud gäller att upptagningar och upptecknin gar från hemlig avlyssning av elektronisk kommunikation och hemlig rumsavlyssning omedelbart ska förstöras i de delar som de omfattas av ett sådant förbud (27 kap. 22 § tredje stycket rättegångsbalken och 11 § andra stycket lagen om preventiva tvångsmedel). Eftersom det inte finns någon motsvarighet till avlyssningsförbudet när det gäller inhämtning av teledata finns följaktligen inte heller någon motsvarande regel om att uppgifter som omfattas av ett sådant förbud ska förstöras.

Enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet får signalspaningsmyndigheten (Försvarets radioanstalt) under vissa förutsättningar och för vissa syften hämta in och avlyssna signaler i elektronisk form vid signalspaning (1 §). Eftersom sådan inhämtning sker helt automatiserat innehåller lagen inte någon motsvarighet till rättegångsbalkens bestämmelser om avlyssningsförbud. Däremot innehåller lagen bestämmelser som anger att upptagningar och upptecknin gar omgående ska förstöras, om innehållet

1. berör en viss fysisk person och har bedömts sakna betydelse för syftet med signalspaningen,
2. avser uppgifter för vilka tystnadsplikt gäller enligt 3 kap. 3 § tryckfrihetsförordningen eller 2 kap. 3 § yttrandefrihetsgrundlagen, eller som omfattas av efterforskningsförbudet i 3 kap. 4 § tryckfrihetsförordningen eller 2 kap. 4 § yttrandefrihetsgrundlagen,
3. omfattar uppgifter i meddelanden som avses i 27 kap. 22 § rättegångsbalken, eller
4. avser uppgifter lämnade under bikt eller enskild själavård, såvida det inte finns synnerliga skäl att behandla uppgifterna för syftet med signalspaningen (7 §).

Regeringen anförde följande i lagens förarbeten (prop. 2006/07:63 s. 105):

> En viktig utgångspunkt är vidare att regler om signalspaning inte får strida mot det skydd för meddelarfriheten som gäller enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Även om signalspaningen inte riktas mot personer som är verksamma på massmedieområdet kommer det inte att gå att helt undvika risken för att exempelvis ett meddelande mellan en journalist och en meddelare inhämtas. Anonymitetsskyddet som garanteras genom journalistens tystnadsplikt bryts då igenom. En upptagning eller uppteckning kan också innefatta ett brott mot det s.k. efterforskningsförbudet. Det ideala skulle vara om inhämtning som berörde massmedieområdet förbjöds. Vid automatiserad inhämtning är det dock inte möjligt att upprätthålla ett sådant förbud. Av praktiska och tekniska skäl kan det inte heller krävas att inhämtningen omedelbart skall avbrytas. Problemet kan inte lösas på annat sätt än genom en föreskrift om att upptagningar eller uppteckningar som står i konflikt med tryckfrihetsförordningen och yttrandefrihetsgrundlagen omedelbart skall förstöras.

Regeringen bedömde också att enbart det förhållandet att information inhämtas inte kunde anses innebära ett brott mot anonymitetsskyddet eller efterforskningsförbudet. Det framhölls därvid att tystnadsplikten i sig inte direkt riktar sig mot det allmänna. Vad däremot gällde efterforskningsförbudet konstaterades att detta visserligen uttryckligen riktar sig till myndigheter och andra allmänna organ. För att en överträdelse av förbudet ska anses föreligga torde dock enligt regeringen krävas att syftet med åtgärden från det allmännas sida varit att efterforska författaren, utgivaren eller meddelaren.

Regeringen anförde att, när sådan information i stället råkar inhämtas av en myndighet som en icke avsedd bieffekt av annan verksamhet, det inte kan anses att efterforskningsförbudet överträtts, i synnerhet inte om det åvilar myndigheten en uttrycklig skyldighet att förstöra upptagning eller uppteckning med sådan information och anonymitetsskyddet följaktligen garanteras (a. prop. s. 106).

8.2.5 Proportionalitetsprincipen

Ett grundläggande krav för att tillstånd till hemlig övervakning av elektronisk kommunikation och inhämtning av uppgifter enligt inhämtningslagen ska kunna meddelas är att åtgärden är proportionerlig (27 kap. 1 § tredje stycket rättegångsbalken och 2 § inhämtningslagen). Vid bedömningen av om en åtgärd kan anses proportionerlig har det betydelse vilken typ av kommunikation uppgifterna avser. Bland annat ska det beaktas om åtgärden innebär intrång i ett rättsligt skyddat intresse, t.ex. meddelarskyddet enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Innebär inhämtningen ett kringgående av förbudet för massmedier att röja sina källor eller för det allmänna att efterforska vem som är meddelare, får inhämtning inte ske (prop. 2011/12:55 s. 122). Detta innebär alltså att risken för att uppgifter om skyddad kommunikation kommer att hämtas in då åtgärden verkställs ska beaktas vid tillståndsgivningen. Vidare gäller proportionalitetsprincipen under hela verkställighetsförfarandet och ska således, även sedan tillstånd har meddelats, beaktas av den verkställande myndigheten. Integritetsintrånget under verkställigheten kan bli så stort att åtgärden inte längre är tillåten, trots att rekvisiten för åtgärden fortfarande är uppfyllda (a. prop. s. 122).

Trots att det inte finns något uttryckligt förbud är alltså möjligheten att hämta in uppgifter om elektronisk kommunikation avseende personer som omfattas av yrkesmässig tystnadsplikt begränsad jämfört med kommunikation som avser andra personer. Däremot kan det givetvis hända att en åtgärd som riktar sig mot någon som inte omfattas av yrkesmässig tystnadsplikt får till följd att även uppgifter om dennes kontakter med personer inom skyddade yrkeskategorier samlas in. Vidare kan uppgifter som avser personer inom skyddade yrkeskategorier komma att inhämtas genom s.k. basstationstömningar.

Enligt uppgifter som utredningen har inhämtat från den öppna polisen finns det inom polisen rutiner och föreskrifter avseende inhämtning av uppgifter som omfattas av yrkesmässig tystnadsplikt. Rikskriminalpolisen har tagit fram en tjänsteföreskrift 2012:5 – *Tjänsteföreskrift om förstörande av upptagningar och uppteckningar från hemliga tvångsmedel*, med anledning av om åtgärden innebär intrång i ett rättsligt skydd. Av denna tjänsteföreskrift framgår i punkten 9.1 att, vid granskning av material från hemliga tvångsmedel, sektionschefen för den sektion som ansvarar för ärendet ska ansvara för att materialet granskas utan dröjsmål. Syftet med denna granskning är att säkerställa att den information som tas emot också får tas emot enligt gällande bestämmelser och att de begränsningar som gäller för respektive tvångsmedel iakttas. Polisen har också framhållit att det i praktiken ofta är omöjligt att i förväg veta om en inhämtning kommer att omfatta uppgifter som omfattas av yrkesmässig tystnadsplikt. Detta är i stället något som hanteras när informationen kommer in till polisen. Den rutin som då råder är att ansvarig förundersökningsledare får fatta beslut om hur materialet ska hanteras.

Säkerhetspolisen har uppgett att myndigheten i dagsläget inte har någon särskild rutin för inhämtning av teledata avseende personer som omfattas av yrkesmässig tystnadsplikt. Vid bedömning av om uppgifter ska inhämtas med stöd av inhämtningslagen görs en proportionalitetsbedömning i det enskilda fallet. Beslut om att inhämta uppgifter utgår från behov av att kartlägga brottsaktiva aktörer och dessas nätverk i syfte att förebygga, förhindra eller upptäcka brottslighet. Det åligger var och en som bearbetar den inhämtade informationen att bedöma om informationen har relevans för arbetet. När det gäller uppgifter som inhämtats enligt inhämtningslagen är det fråga om tekniska data såsom teleadresser, positioner, tidpunkter, kontakter etc. Uppgifterna är således av sådan karaktär att det inte går att få information om innehåll i exempelvis meddelanden.

Vad avser avlyssningsförbudet så finns det en rutin inom Säkerhetspolisen som anger att en första granskning (bearbetning) av inhämtat material ska ske utan dröjsmål och att syftet med denna bearbetning är

a) att kontrollera att materialet kan användas i det pågående ärendet,

b) att se till att information som inte är tillåten tas bort, dvs. att de begränsningar som gäller för tvångsmedel iakttas, exempelvis förbudet att avlyssna samtal mellan den misstänkte och dennes försvarare, och

c) att kontrollera att materialet avser just det objekt/person, telefonnummer eller den plats som framgår av tillståndet samt att rätt inhämtningsåtgärd har tillämpats.

8.3 Utredningens förslag

Utredningens förslag: Det ska införas en skyldighet att förstöra uppteckningar från hemlig övervakning av elektronisk kommunikation och inhämtning av uppgifter enligt inhämtningslagen i de delar uppteckningarna innehåller uppgifter som på grund av frågeförbudet enligt rättegångsbalken inte skulle ha kunnat inhämtas genom vittnesförhör i domstol.

8.3.1 Förbud mot att hämta in uppgifter om kommunikation med personer som omfattas av yrkesmässig tystnadsplikt?

Som framhålls ovan intar svensk rätt den ståndpunkten att det normalt är en uppgifts innehåll som avgör om den omfattas av skydd mot avlyssning och undantag från vittnesplikt. Trots det kan det i vissa situationer finnas ett intresse av att begränsa myndigheternas insyn i att kommunikation över huvud taget har förekommit. Det gäller t.ex. uppgifter om kommunikation med sådana personer som berörs av meddelarskyddet. I dessa fall skulle redan en uppgift om att någon har varit i kontakt med en journalist kunna leda till att det anonymitetsskydd som garanteras genom journalistens tystnadsplikt hotas. Utredningen instämmer dock i den bedömning som regeringen tidigare har gjort i fråga om att efterforskningsförbudet i sådana situationer överträds endast i den mån som syftet från det allmännas sida är att efterforska en författare, utgivare eller meddelare. När sådan information i stället råkar inhämtas av en myn-

dighet som en icke avsedd bieffekt av annan verksamhet kan det således inte anses att efterforskningsförbudet överträds.

En uppgift om att en person har kommunicerat med en journalist omfattas av skydd för meddelarfrihet endast i de fall då kommunikationen innebär att ett meddelande etc. lämnas för publicering. Vid inhämtning av s.k. metadata, dvs. uppgifter som endast anger att kommunikation har ägt rum men inte vad den innehöll, känner de brottsbekämpande myndigheterna normalt sett inte till innehållet i kommunikationen. Detta innebär att det oftast inte går att avgöra vilka uppgifter som omfattas av tystnadsplikt. Ett förbud mot att hämta in sådana uppgifter skulle därför vara mycket svårt att tillämpa. Om myndigheten i något fall skulle känna till att de aktuella uppgifterna omfattas av yrkesmässig tystnadsplikt redan innan inhämtning sker, torde dessutom en tillämpning av proportionalitetsprincipen normalt sett leda till att uppgiften inte får hämtas in. Ett uttryckligt förbud mot inhämtning av uppgifter i sådana situationer skulle därför vara av begränsat praktiskt värde. Något sådant förbud bör därför inte införas.

8.3.2 Förstörandeskyldighet

Ett annat tänkbart alternativ som skulle kunna bidra till att stärka skyddet för uppgifter som omfattas av yrkesmässig tystnadsplikt är att införa regler om att sådana uppgifter ska förstöras i efterhand. Även tillämpningen av en sådan regel skulle visserligen normalt förutsätta att den brottsbekämpande myndigheten känner till innehållet i kommunikationen. Det är dock inte otänkbart att det i undantagsfall skulle kunna inträffa att myndigheten får sådan kännedom. Detta gäller t.ex. då hemlig övervakning av elektronisk kommunikation används tillsammans med hemlig avlyssning av elektronisk kommunikation. I den utsträckning kommunikationen i en sådan situation omfattas av avlyssningsförbud har den brottsbekämpande myndigheten en skyldighet att förstöra upptagningarna och uppteckningarna från avlyssningen. Däremot finns det inte någon uttrycklig skyldighet att radera också uppgiften om att kommunikationen har ägt rum. Detta gäller även om myndigheten genom avlyssningen fått kännedom om att t.ex. ett meddelande lämnades till en journalist för publicering. Enligt utredningens uppfattning är detta en brist i

skyddet för den yrkesmässiga tystnadsplikten. Vi kan inte heller se några tungt vägande skäl mot att den brottsbekämpande myndigheten i en sådan situation ska vara skyldig att radera även uppgifter som anger att kommunikationen har ägt rum.

Sammanfattningsvis bör det införas en skyldighet för de brottsbekämpande myndigheterna att förstöra uppteckningar från hemlig övervakning av elektronisk kommunikation och inhämtning av uppgifter enligt inhämtningslagen i de delar uppteckningarna innehåller uppgifter som, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat inhämtas genom vittnesförhör i domstol. Eftersom möjligheten att avgöra om tystnadsplikt gäller för uppgifter om att kommunikation förekommit normalt är beroende av vad kommunikationen innehöll torde det endast sällan bli aktuellt att tillämpa dessa regler. Detta är emellertid inte något starkt skäl för att avstå från att införa reglerna.

9 Inhämtningslagen

9.1 Direktiven

I våra direktiv framhålls att utformningen av regler om hemliga tvångsmedel förutsätter att en avvägning görs mellan å ena sidan nyttan och behovet av tvångsmedlet och å andra sidan omfattningen och arten av det intrång i den personliga integriteten som tvångsmedlet innebär. För att en sådan avvägning ska kunna göras krävs att nyttan och behovet av tvångsmedlet, ändamålet med tvångsmedelsregleringen samt omfattningen och arten av intrånget i den personliga integriteten kan klarläggas med sådan konkretion att det finns ett gott underlag för att bedöma om befogenheten att använda tvångsmedlet är proportionerlig. Det framhålls vidare att ett sådant underlag bör, när det är möjligt, bygga på uppgifter om den hittillsvarande tillämpningen av det tvångsmedel som avses. Mot den bakgrunden har utredningen i uppdrag att kartlägga den hittillsvarande tillämpningen av inhämtningslagen, analysera vilken nytta tvångsmedelsanvändningen enligt lagen har inneburit för den brottsbekämpande verksamheten samt analysera vilken inverkan lagen har haft på enskildas personliga integritet. Utredningen ska också överväga om de rättssäkerhets- och integritetsstärkande åtgärder som vidtogs när lagen infördes har varit tillräckliga eller om det finns behov av andra sådana åtgärder. Vidare ska utredningen analysera vilka behov Säkerhetspolisen har av en möjlighet enligt inhämtningslagen att hämta in uppgifter för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar vissa samhällsfarliga brott med lägre straffminimum än fängelse två år samt lämna förslag på hur detta behov bör tillgodoses och balanseras mot integritetsintresset.

9.2 Utredningens kartläggning

9.2.1 Metod

Enligt våra direktiv ska resultatet av kartläggningen utgöra underlag för att analysera frågor om tvångsmedlets nytta och påverkan på den personliga integriteten, dvs. frågor som är relaterade till tvångsmedelsanvändningens effekter. Sådana frågor är komplicerade och kräver i många fall en helhetsbedömning som ger anledning till mer öppna frågor och svar än vad som kan fångas upp genom specifika förutbestämda frågor i t.ex. en blankett eller ett frågeformulär (se SOU 2012:44 s. 256).

Utredningen har därför valt en kartläggningsmetod som innebär att vi på djupet har granskat ett urval av underrättelseärenden där inhämtningslagen har tillämpats av Polismyndigheten, Säkerhetspolisen eller Tullverket. I samband med undersökningen har utredningen, i vart och ett av de utvalda ärendena, tagit del av de beslut enligt inhämtningslagen som fattats i ärendena samt bakomliggande skriftligt material. Därefter har företrädare för utredningen intervjuat den ansvarige handläggaren om ärendet. Syftet har varit att tränga djupare in i frågorna om nytta, behov och integritetsintrång. De huvudsakliga frågeställningarna har varit följande:

1. Vilka indikationer har funnits om brottslig verksamheten i de fall myndigheterna har valt att hämta in uppgifter enligt inhämtningslagen?
2. Vilka uppgifter har funnits om den aktuella personen och dennes miljö/nätverk?
3. Varför valde myndigheten att använda inhämtningslagen och vilka omständigheter gjorde att tvångsmedlet användes vid den bestämda tidpunkten?
4. Vilka strategier hade personen och dennes miljö för att skydda verksamheten och sin kommunikation?
5. Vilken information räknade myndigheten med att få och vilken information fick myndigheten?
6. Hur gick myndigheten vidare efter att inhämtningslagen använts?
7. Vilken nytta hade myndigheten av inhämtningslagen?

8. Vilket integritetsintrång räknade myndigheten med, och vad blev det faktiska integritetsintrånget?

I det följande redovisas den undersökning vi har gjort. Vi gör det utförligt och med största möjliga öppenhet. Nödvändig hänsyn till de brottsbekämpande myndigheternas berättigade anspråk på sekretess och i vissa fall även till enskildas integritet gör dock att en del uppgifter måste utelämnas.

9.2.2 Säkerhetspolisens användning av inhämtningslagen

9.2.2.1 Inledning

Undersökningen

En genomgång har gjorts av Säkerhetspolisens användning av inhämtningslagen. Sammanlagt har 60 ärenden granskats – omfattande lika många personer. Undersökningen är kvalitativ, även om också vissa siffror kommer att presenteras i det följande.

Urvalet gick till på det sättet att 60 ärenden – med början i april 2014 och bakåt – togs fram av forskaren i strikt ordningsföljd med hjälp av Säkerhetspolisens diarium. Inledningsvis undersöktes dock enbart 50 ärenden. När dessa ärenden mot slutet inte längre tillförde särskilt mycket ytterligare information togs ytterligare 10 ärenden fram för att kontrollera om det fanns anledning att fortsätta med att granska fler ärenden. Efter att ha gått igenom dessa 10 ärenden bedömdes att ytterligare ärenden inte skulle ge något nämnvärt mervärde varför genomgången avslutades vid 60 ärenden.

Dessa ärenden fördelar sig enligt tabell 1 på följande områden.

Tabell 9.1 Områden som omfattas av den undersökta inhämtningen (n=60 ärenden)

Område	Antal ärenden (och personer)
Terrorbrott (med koppling till grupperingar, exempelvis al-Qaida)	28
Terrorbrott (ensamagerande)	6
Spionage och flyktingspionage (grov olovlig underrättelseverksamhet)	4
Politisk extremism (ofta grova våldsbrott)	21
Spridning av massförstörelsevapen	1

I avsnitten 9.2.2.2–9.2.2.6 kommer dessa områden att närmare utvecklas och resultatet mer i detalj att redovisas.

Undersökningen har gått till på det sättet att forskaren tagit del av Säkerhetspolisens beslut enligt inhämtningslagen med bakomliggande promemoria. Besluten är skrivna på en särskild blankett där beslutsfattarens namn framgår liksom handläggarens namn och dennes närmaste chef. Som regel är som blanketten utvisar tre personer involverade i varje beslut, men i undantagsfall kan även chefen vara föredragande. Vid sidan av att besluten anger vad IHL-inhämtningen avser och tidsperioder är det promemorian som innehåller de substantiella fakta som ligger till grund för IHL-beslutet. Det är handläggaren och i några fall närmast ansvarig chef som författar promemorian. Samtliga ärenden föredras och en sittning kan ta mellan tio och trettio minuter beroende på hur mycket fakta som behöver redovisas och diskuteras. Förutom promemorian kan i vissa ärenden en grafisk nätverksanalys underlätta föredragningen som visar hur den aktuella personen hänger samman med andra. Åtskilliga föredragningar går ganska fort eftersom personerna är kända sedan tidigare.

Efter det att beslut och promemorior gåtts igenom har ansvarig handläggare intervjuats om ärendet. Frågorna har gällt de punkter som anges i avsnitt 9.2.1.

Ett antal ärenden har dock varit svåra att följa upp eftersom handläggarna har slutat eller varit tjänstlediga. Det är heller inte på det sättet att handläggarna i hög grad har ”egna” ärenden utan deras arbetsuppgifter kan växla. I några fall har därför den handläggare

som stått bakom ett beslut inte kunna följa hur det utvecklats eftersom någon annan har tagit över ärendet. I några ärenden har intervjuer med närmast ansvarig chef kunnat komplettera underlaget. I 12 ärenden har dock intervjuer inte kunnat hållas. Det betyder att 48 ärenden har undersökts i detalj och 12 översiktligt, enbart med ledning av skriftliga uppgifter i form av beslut och promemorior.

Sammanlagt har 20 personer intervjuats i ärendena. Vissa har följaktligen intervjuats om flera ärenden. En intervju har tagit mellan 15 och 45 minuter per ärende. Intervjuerna har skett i Säkerhetspolisens lokaler Stockholm och i något fall i Malmö. Några intervjuer har gjorts per telefon till andra orter där Säkerhetspolisen har lokaler.

Dessutom har intervjuer med ett övergripande fokus gjorts med chefen för den tekniska mängddatabearbetningen och operative chefen för kontraterror.

På grund av ärendenas känsliga karaktär har intervjuerna inte spelats in utan anteckningar har i stället förts på en särskild blankett, en blankett för varje ärende. Vissa uppgifter från blanketterna har sedan kodats i Excel för att underlätta sammanställningen av sifferuppgifter.

Några övergripande resultat

De undersökta 60 ärendena har i allt väsentligt gällt mobiltelefoner (95 stycken) och bara några få fasta telefoner (4 stycken). Ärenden som gällt mobiltelefoners unika IMEI-kod (3 stycken) och SIM-kortets IMSI-kod (1 styck) är ovanliga. Samtliga ärenden har gällt historiska trafikdata, men det är också vanligt med geografiska data – var telefonen har befunnit sig. I några ärenden har uppgifterna gällt en månad framåt i tiden, räknat från och med beslutet. Inga ärenden har avsett bastömning, vilket kan förklaras av att Säkerhetspolisen i de ärenden som studerats riktat in sig på bestämda personer, inte på händelser vid vissa platser.

Den genomsnittliga tiden för besluten om inhämtning av trafikdata är 4 månader. Många ärenden gäller dock mellan 1 och 3 månader, men genomsnittet dras upp av några längre inhämtningar.

De flesta ärendena gäller män, men även ett antal kvinnor förekommer.

I de ärenden där födelseår framgår är det genomsnittliga födelseåret 1982. I terrorärendena är det genomsnittliga födelseåret 1985, och påfallande många är mycket unga och födda under första hälften av 1990-talet. För andra kategorier än terror är uppgifterna om ålder alltför ofullständiga för att det ska vara meningsfullt att ta fram ett genomsnitt.

En intressant fråga är vilket resultat inhämtningen hade. En indelning har gjorts i följande kategorier, efter användningen av inhämtningslagen.

- Personen är avförd eller lågprioriterad
- Fortsatt uppföljning, men på samma nivå som före IHL
- Fortsatt uppföljning, men på högre nivå än före IHL

För att förstå dessa kategorier bör man känna till att de undersökta IHL-ärendena till stor del gäller personer som Säkerhetspolisen redan känner till. På ett eller annat sätt är de föremål för viss uppföljning. När sedan något inträffar – typiskt sett att information kommer fram med indikationer på brottslig verksamhet – bedömer Säkerhetspolisen att det behövs ytterligare uppgifter för att klargöra läget.

Mot den bakgrunden bör det vara förhållandevis få IHL-operationer som leder till att personer avförs helt och hållet. I stället ligger det närmare till hands att Säkerhetspolisen efter IHL fortsätter uppföljningen på den tidigare lägre nivån alternativt på den fortsatt högre nivån.

I ett antal fall har dock IHL satts in på personer som är nya för Säkerhetspolisen. Den vanliga situationen är dock inte att IHL används som första inhämtningsmetod, utan vid sidan av de uppgifter som gör att IHL blir aktuellt används också andra kanaler, till exempel polisens belastnings-, anmälnings- och spaningsregister, Säkerhetspolisens centralregister, kontakter med källor etc. Med ledning av denna information tas en ”profil” fram. Det går därför att säga att läget även för dessa nya ärenden är en form av normal inhämtning före IHL, låt vara att den skett under kort tid.

I en del av ärendena har förundersökning inletts och telefonavlyssning satts in (efter domstolsbeslut). Ibland har detta skett viss tid efter en IHL-operation. Undersökningen har dock inte haft ambitionen att följa ett IHL-ärende fram till dagens läge. Det vore

också fel eftersom senare beslut inte behöver grunda sig enbart på den studerade IHL-operationen utan också på senare händelser och information. Därför är det läget direkt efter IHL-operationen som redovisas. I beskrivningarna längre fram kommer dock en del exempel att ges på hur ärenden senare har utvecklats. Det bör tilläggas att bedömningen av hur uppföljningen ska fortsätta direkt efter en IHL-operation givetvis också bygger på även andra uppgifter än trafikdata. IHL är i nästan alla ärenden enbart en av underrättelsekorgarna som sällan kan isoleras från andra källor.

Tabell 9.2 Utfallet efter Säkerhetspolisens IHL-ärenden (n=60)

Utfall	Antal ärenden (och personer)
Information saknas	12
Avförd eller lägre prioritet	4
Fortsatt uppföljning, men på samma nivå som före IHL	19
Fortsatt uppföljning, men på högre nivå än före IHL	25

Träffsäkerheten för att sätta in IHL är hög. I 19 av de 48 ärendena där intervjuer har hållits finns visserligen fortsatt behov av uppföljning, men IHL-kontrollen innebär att de uppgifter som tydde på behov av större insatser från Säkerhetspolisens sida har kunnat stämmas av med hjälp av trafikdata. Situationen har inte bedömts som mer allvarlig än att det har räckt med att fortsätta med den uppföljning som redan skedde före IHL. Längre fram kan givetvis läget förändras, i båda riktningar bör tilläggas. I 25 ärenden visade det sig dock att de uppgifter som låg till grund för beslutet att använda IHL bekräftades på det sättet att Säkerhetspolisen bedömde att det fanns skäl att fortsätta uppföljningen, och det på en högre nivå än före det IHL sattes in. Längre fram kommer en rad exempel på hur Säkerhetspolisen fortsatt denna uppföljning, men redan nu kan sägas att det kan handla om att informatörers uppmärksamhet riktas mot personen, att telefonavlyssning sätts in, att fysisk spaning aktiveras eller att Säkerhetspolisen överväger att ta initiativ till att hålla samtal med personen.

I fyra fall kunde dock Säkerhetspolisen avföra personen eller fortsätta att följa upp på en mycket låg nivå.

Disposition

I det följande redovisas resultatet av undersökningen i sju avsnitt enligt följande uppdelning:

- Terrorbrott med koppling till grupperingar i avsnitt 9.2.2.2
- Terrorbrott, men ensamagerande, i avsnitt 9.2.2.3
- Politisk extremism i avsnitt 9.2.2.4
- Spionage och flyktingspionage (olovlig underrättelseverksamhet) i avsnitt 9.2.2.5
- Spridning av massförstörelsevapen i avsnitt 9.2.2.6
- Några generella synpunkter i avsnitt 9.2.2.7
- Summering av nyttan i avsnitt 9.2.2.8

Varje avsnitt om brottsområden följer i princip en disposition som presenterar de grupperingar eller personer som är aktuella, vilka indikationer som Säkerhetspolisen fick om brottslig verksamhet, skälen till att Säkerhetspolisen bedömde behov av ökad information genom att använda IHL, riskerna med den befarade brottsligheten, personens liksom miljöns säkerhetstänkande, omständigheter som gjorde att IHL sattes in vid det aktuella tillfället, vilken information som Säkerhetspolisen räknade med att få in och vad IHL faktiskt gav och resultatet av IHL-operationen, det vill säga vilket ställningstagande Säkerhetspolisen gjorde med ledning av de inhämtade IHL-uppgifterna samt frågan om integritetsintrång. Den för utredningen centrala frågan om nyttan har olika aspekter och behandlas på flera ställen i texten. Därför avslutas redovisningen med en summering av nyttan.

9.2.2.2 Terrorbrott med koppling till grupperingar

Grupperingar

Som nyss nämnts utgör terrorärendena hälften av de undersökta IHL-operationerna (28 av 60 ärenden). Även de sex ärenden som gäller ensamagerande tar sikte på terrorbrott (avsnitt 9.2.2.3) och

dessutom några av de fall som handlar om politisk extremism (avsnitt 9.2.2.4). Det är ett tecken på terrorns ökade insteg i dagens samhälle och därmed också för Säkerhetspolisens arbete.

Merparten av terrorärendena gäller våldsbejakande islamistiska nätverk med personer med koppling till företrädesvis al-Qaida (19 ärenden) eller al-Shabaab (7 ärenden). I Sverige finns ett antal sådana miljöer i vilka radikalisering och rekrytering sker av nya anhängare. ”Vi har flera miljöer i Sverige, och har man kontakter i sådana miljöer är det oroväckande”, som en handläggare förklarade. En person i en sådan miljö hade rest till Syrien för att ansluta sig till stridande förband och IHL sattes in. I dessa miljöer förekommer personer som bekänner sig till ideologin om global jihad, hyllar Usama bin Laden och som vill införa sharialagar i Sverige. Många av dessa personer i IHL-undersökningen är svenska medborgare.

Personer från utlandet med förbindelse med al-Qaida kommer också till Sverige, ibland för att söka asyl. ”Så fort det finns en koppling till al-Qaida hoppar vi till”, förklarar en handläggare och menar att det då alltid sker en uppföljning av denna information från Säkerhetspolisens sida.

IHL är en metod som kräver mindre resurser än fysisk spaning eller mer ingripande och integritetskänsliga tvångsmedel som telefonavlyssning (numera elektronisk avlyssning). Därför betraktas IHL generellt som en inledande stegrad metod jämfört med andra inhämtningsmetoder – exempelvis som komplement till registerslagning och uppgifter från informatörer eller utländska tjänster. IHL sätts då in för att Säkerhetspolisen behöver få uppgifter bekräftade och de nämnda inhämtningskorgarna inte bedöms kunna lämna svar på de frågor som kommit upp. Den inledande aspekten tar sikte på att IHL ofta används för att undersöka om det finns anledning att sätta in mer resurskrävande och integritetskänsliga åtgärder.

Även om al-Qaida och al-Shabaab dominerar sker uppföljning också av delar av PKK. Det gällde exempelvis en person som deltagit i PKK:s träningsläger. Hotet från PKK beskrivs dock som mindre i Sverige än på många andra håll. Aktivister tillhör andra och tredje generationen invandrare och är därför välintegrerade i det svenska samhället.

Som snart kommer att utvecklas handlar de flesta ärenden om Syrien. Även om flertalet terrorärenden följer ett sådant givet mönster, finns några fall som skiljer ut sig genom att ha koppling

till kända enskilda internationella terrordåd. På det sättet förekommer även Sverige på en internationell terrorkarta, låt vara i periferin.

Indikationer på brottslig verksamhet

De flesta ärenden på terrorsidan som ingår i det undersökta materialet och som gäller personer med koppling till grupperingar handlar om Syrien och personer som återvänder hem till Sverige. De typiska indikationerna på terrorbrott är kombinationen stridserfarenhet från Syrien (förmåga) och att personen kan knytas till extremistmiljöer, både i Syrien och i Sverige (i vart fall indikation på avsikt). De källor som Säkerhetspolisen bygger sina bedömningar på är framför allt informatörer, signalspaning av samtal, utländska tjänster och myndigheter. I det följande ges några belysande exempel på ärenden.

En handläggare förklarar att det tidigare var al-Shabaabresor till Somalia. ”Nu är det Syrien som gäller.” Ett typiskt ärende handlar om en svensk medborgare med utländsk härkomst som rest till Syrien och där anslutit sig till en väpnad gruppering och deltagit i strid. Därefter återvänder han till Sverige och umgås med personer som Säkerhetspolisen kopplar till terrorism; ofta befinner de sig i sådana nyss nämnda radikala miljöer. Av några av ärendena framgår att återvändarna skadats i strid och sökt och fått vård i Sverige.

Några udda ärenden gäller dock andra länder med kända oroshärdar som Tjetjenien. Fokus på Syrien och svenska kopplingar dit har naturligtvis att göra med situationen där och att en hel del personer från Sverige reser dit för att genomgå militär utbildning och ansluta sig till väpnade styrkor. Säkerhetspolisen har haft en särskild uppföljning av Syrienresenärer, inte minst för att de på plats förvärvar en förmåga till terrordåd.

Militär utbildning erbjuds även på andra håll än i Syrien. Ett ärende gällde en person som hade vistats flera år i Jemen och Somalia. Misstankar fanns att personen hade genomgått utbildning vid ett av al-Shabaabs träningsläger. I dessa erbjuds grundläggande militärutbildning. I Sverige umgås han med personer med kända kopplingar till internationell terrorism och vistas i al-Shabaabkretsar. Även en nära släkting till honom påstås ha koppling till

internationell terrorism. Han har bland annat umgåtts med en person som rest till Syrien på jihad. Det finns också uppgifter om att han själv uttryckt vilja att resa på jihad till Somalia eller Syrien.

En person i ett ärende hade varit i Syrien en längre tid och förmodligen tillhört en al-Qaidainspirerad gruppering. Han har själv medgett att han deltagit i strid. Han umgås också i sådana kretsar och har internationella kontakter. Ett annat ärende gällde en högt uppsatt al-Qaidaperson med stridserfarenhet som kommit till Sverige.

Ett ovanligt fall gällde om en person hade deltagit i en befarad attentatsplanering som skulle ha ägt rum på ett visst ställe en bestämd dag. Det fanns uppgifter om att ett attentat skulle ske på svensk mark. De misstänkta attentatsmännen påstods ha tidigare stridserfarenhet. Attentatsplanering förekommer också i ett annat ärende, men attentatet skulle riktas mot utlandet. Även förundersökning hade inletts till följd av ett utfört dråd utomlands. I andra ärenden fanns uppgifter om att en person skulle organisera en al-Qaidagrupp i Sverige eller i ett grannland.

En person hade vistats i Syrien under längre tid, och det fanns uppgifter om att han varit på träningsläger och anslutit sig till en terrorgruppering. Det hade varit svårt att lokalisera honom genom spaning. En annan person hade en bakgrund i stridande förband och befarades vara villig att åta sig självmordsuppdrag.

Ibland görs det gällande att Syrienresenärer på plats enbart ägnat sig åt humanitärt arbete. I ett sådant fall fanns dock uppgifter om att personen deltagit i träningsläger. En annan uppgift som tyder på deltagande i väpnad kamp är att personen fått stridsskador som krävt kvalificerad vård i Sverige. Han hade också tät kontakt med en annan person som deltagit i strid i Syrien.

I ett annat fall gjordes gällande att personen enbart hjälpt till i ett flyktingläger i Syrien. Samtidigt fanns uppgifter om att resan ned till Syrien företogs i sällskap med två terrormisstänkta personer, och från Syrien har personen haft telefonkontakt med en misstänkt terrorist. Uppgifter från den egna familjen tyder på att personen inspirerats av al-Qaidaideologer. En återvändare har också berättat att personen deltagit i träningsläger.

En person hade enligt uppgift en roll i att hjälpa anhängare till jihad att resa till konfliktzoner. Förutom al-Qaidakopplingar och kontakter med kända terrorister fanns uppgifter om gömda sprängmedelsförråd i Sverige. I ett annat ärende hade kontakten med en

sådan facilitator skett via Facebook där bästa resvägen från Turkiet till de väpnade styrkorna i Syrien hade efterfrågats.

En person beskrivs ha tidigare befunnit sig i utkanten av ett nätverk med kända kopplingar till internationell terrorism. Information kom dock fram som tydde på att personen ägnade sig åt stödverksamhet, att radikalisera och rekrytera personer som rest till Syrien för att ansluta sig till stridande förband. Uppgifter fanns också om att han själv var på väg dit. Det finns också bland ärendena personer som konverterat till islam och sedan radikaliserats och rekryterats för att strida i Syrien. I ett annat fall skulle personens lägenhet ha använts som samlingsplats för unga män som sympatiserar med våldsbejakande islamistisk extremism. ”Han har haft kontakt med fyra personer som anslutit sig till al-Shabaab i Somalia.” Personen beskrivs som centralfigur i ett nätverk med misstänkta terrorister och har varit involverad i terrorrelaterade aktiviteter i Sverige, Somalia och Syrien. I ytterligare ett ärende pekas en person ut som koordinator för resor till Somalia. Han påstås själv ha varit på träningsläger, deltagit i strid och radikaliserat flera personer som rest till Syrien.

Varför fanns ett behov av ytterligare information?

Som nämnts sätts IHL typiskt sett in som ett led i en uppföljning när Säkerhetspolisen bedömer att det behövs ytterligare information för att kunna värdera en persons förmåga och avsikt att begå terrorbrott. I det följande ges några exempel från ärendena.

”Det var ett svart hål. Underrättelseläget var dåligt. Vi visste inte vad han hade gjort i Somalia”, berättar en intervjuad handläggare och förklarar varför det fanns behov av att intensifiera uppföljningen. IHL ger information om kontakter, och för Säkerhetspolisen är det främst ”kända” personer i eller utanför Sverige som ger en indikation om vad som kan vara å färde. Det är heller inte ovanligt att nya för Säkerhetspolisen intressanta kontakter kommer fram genom IHL. På det sättet byggs kunskapen upp som kan generera nya ärenden. Det handlar då inte enbart om ytterligare pusselbitar utan att pusslet utvidgas. Av intresse är också att få kännedom om intressanta möten. När på dygnet samtal sker, fre-

kvensen och geografisk anknytning kan också vara nog så talande som kontaktnumren.

Personer som deltagit i träningsläger och strid har givetvis med sig en förmåga hem till Sverige. De har ett vapenkunnande, de kan hantera sprängmedel och vet hur man uppträder i strid. Vissa personer påstås till och med ha specialutbildning i att tillverka bomber och att framställa gift. En person i ett ärende lär ha ingått i en särskild bombgrupp.

Ideologiskt måste dessa personer rimligtvis beskrivas som extremister. Att resa till en annan del av världen och genomgå militär utbildning vid ett träningsläger och sedan delta i strid är givetvis att ta ett mycket stort steg. Ingen kan säga att de inte visat beslutsamhet. De har således en ideologisk agenda, med det behöver givetvis inte innebära att de i Sverige går från ord till handling i betydelsen terrorbrott. Det stora frågetecknet för Säkerhetspolisen är följaktligen inte förmågan, utan att bedöma om personerna har avsikt att utföra eller på annat sätt understödja terrorbrott. Av intervjuerna framgår att IHL bedöms vara ett viktigt redskap i denna grannlaga bedömning.

Den tydligaste risk som de intervjuade handläggarna lyfter fram är att personer som deltagit i strid har med sig någon form av uppdrag till Sverige. Med uppdrag menas att personen fått instruktioner att utföra ett attentat eller liknande på hemmaplan eller någon annanstans. Det är tydligt att Säkerhetspolisen är mer orolig för ett specifikt uppdrag, med de krav och förväntningar som det innebär, än att någon låter sig inspireras efter att ha varit i Syrien eller på annat sätt. I ett ärende angavs att det fanns ett behov av att ”utröna eventuell terrorverksamhet med koppling till Syrien”. I ett annat ärende ställdes frågan: ”Kommer han att stödja eller begå terrordåd riktade mot Sverige eller svenska intressen?” Det gällde en person som bedömdes ha avsevärd förmåga till terrorbrott.

Vad dessa uppdrag består i är för det mesta oklart. Gäller uppdraget terror eller något terrorrelaterat? Uppgifterna är för vaga och oprecisa för att exempelvis kunna leda till förundersökning. Inte ens preventiva tvångsmedel är möjliga till följd av de oklara uppgifterna. Därför återstår uppföljning genom underrättelseverksamhet, och det är där IHL kommer in i bilden enligt intervjupersonerna.

I något fall finns också uppgifter om finansiering av terrorism. Finansiering räknas till stödverksamhet som även innefattar rekry-

tering av personer till stridande förband och att ordna resor och andra praktiska arrangemang för att ta sig till stridszonerna.

Säkerhetstänkande

Säkerhetstänkandet i miljön ligger generellt på en hög nivå. Personer som tillhör al-Qaidamiljön har ofta ett högt säkerhetstänkande och agerar på ett sådant sätt att de ska undgå upptäckt. Av IHL-ärendena framgår en rad metoder för att hemlighålla verksamhet och kommunikation. Redan av den information som kommer fram genom en IHL-operation, ibland i kombination med iakttagelser från informatörer och spaning, kan säkerhetsmässiga mot- och försiktighetsåtgärder framgå. Personerna byter ofta telefon eller SIM-kort. Det kan också vara påfallande lite telefontrafik vilket tyder på andra kommunikationssätt. När personer träffas vid bestämda tider och platser utan att först ha ringt varandra tyder det på alternativa kommunikationskanaler som också kan vara hemliga telefoner som används enbart för vissa samtal. Den kunskap som finns från telefonavlyssning visar att personerna är förtegna i samtal, bestämmer träff vid på förväg angivna mötesplatser och uppträder konspiratoriskt genom att försäkra sig om att de inte är skuggade. Andra tecken på säkerhetsmedvetande är att bostaden är larmad, datorns bildskärm är vinklad på ett sådant sätt att ingen utomstående kan se. I ett IHL-ärende betraktade personen en av de aktuella telefonerna som hemlig.

Flera Syrienresenärer har obemärkt lyckats ta sig dit och sedan tillbaka till Sverige. Först senare har Säkerhetspolisen fått kännedom om vistelsen utomlands. I sådana situationer räknar Säkerhetspolisen med att personerna fått hjälp av facilitators som gett dem råd om hur de ska resa och i övrigt förfara.

En central uppgift för våldsbejakande extremism är att radikalisera och rekrytera. Hemliga möten och kontakter sker bland annat i lokaler bakom en front av legal verksamhet. En person beskrivs ha hemliga möten bakom stängd dörr i en moské. I ett annat ärende kom fram att aktiviteterna kopplade till extremism döljs bakom en front av legal föreningsverksamhet. Den legala verksamheten skulle till och med understödjas genom bidrag från det allmänna. ”Det är ett välfungerande maskineri”, berättar en handläggare.

Som nämnts är åtskilliga personer som Säkerhetspolisen följer upp genom IHL kända sedan tidigare och ingår i miljöer och nätverk med terroranknytning. I Säkerhetspolisens promemorior anges al-Qaida miljöer eller al-Shabaab miljöer på vissa bestämda platser i Sverige. För personer i dessa kretsar är terrorverksamhet i hög grad en realitet. Flera känner personer som stupat i strid i Syrien och på andra håll. Det är personer som uppfattas som martyrer och inspirationskällor. Det är vanligt att personer i dessa grupper dessutom bor nära varandra eller att de är inneboende hos andra anhängare. Många åker själva ner till framför allt Syrien och har vänner som redan är på plats. Dessa miljöer kännetecknas av mycket annorlunda värderingar och erfarenheter än vad som gäller för samhället i övrigt och uppfattas vara en grogrund för radikalisering och understöd för att ta sig ut ur Sverige för jihad.

Konflikten i Syrien har dock fått stor spridning och uppfattas som en historisk händelse även utanför dessa kända lokala al-Qaida och al-Shabaab miljöer eller nätverk i Sverige. Följaktligen innebär det en lockelse att få vara delaktig i något stort, ”den stora striden”. Det gäller inte minst personer som aldrig tillhört något känt nätverk utan låtit sig inspirerats genom kamrater och sociala medier. De har följaktligen inte rekryterats på vanligt sätt genom att ha befunnit sig i eller nära de kända miljöerna. Dessa personer i periferin som dras till terrorism kan uppfattas som mer oberäkneliga än de som ingår i en miljö. Det är mycket enklare att följa upp personer som tillhör en tydlig krets, menar flera intervjupersoner. Samma problem kommer upp för de ensamagerande (se nästa avsnitt).

Frånvaron av en miljö gör att det för åtskilliga Syrienresenärer finns begränsade möjligheter att använda andra källor än IHL. Skälet är att informatörer eller information från andra ärenden förutsätter att personerna befinner sig i ett sammanhang och inte som mer eller mindre solitärer. Dessutom är förutsättningarna goda att använda IHL. För många av de unga män som åker till Syrien för att strida är nämligen säkerhetsmedvetandet inte särskilt högt utvecklat. Det har rimligtvis att göra med att de inte fostrats i en miljö där säkerhet är en viktig del av gemenskapen och verksamheten.

Omständigheter som gjorde att IHL sattes in

Den information som gör att Säkerhetspolisen sätter in IHL på terrorområdet kommer från egna källor, det vill säga informatörer, uppgifter från samverkande utländska säkerhets- och underrättelsetjänster och signalspaning, både genom FRA och utländska motsvarigheter. Särskilt utländska tjänster spelar en stor roll för Säkerhetspolisens uppföljning.

Det föreligger därför alltid indikationer på brottslig verksamhet i IHL-ärendena, men problemet är att det inte är Säkerhetspolisens egna källor (utan utländska tjänster) eller att det inte går att dra alltför stora växlar på information från egna informatörer. Dessa personer kan befinna sig i periferin, ha en fragmentarisk insyn och följaktligen inte ha hela bilden klar för sig. Källans placering och möjlighet att ge första- eller andrahandsinformation är därför en central fråga för Säkerhetspolisens handläggare. Det går inte heller att alltid lita på källor. Informatörer kan ha egna agendor. Särskilt om felaktig information kommit tidigare i ett ärende ökar behovet av att kontrollera uppgifter, exempelvis genom IHL. Ett vanligt svar från handläggare är dock att IHL ”bekräftade andra källor”.

En underrättelsehandläggare förklarar med att ”allt handlar om att triangulera, att använda så många källor som möjligt”. Det är mot den bakgrunden IHL ska ses som en av flera källor, och dessutom ett mindre integritetskänsligt tvångsmedel än exempelvis avlyssning. Även om IHL är en av flera källor betonar intervjupersonerna samstämmigt hur viktigt det är med IHL, inte minst genom att det både är effektivt och resurssnålt. ”När vi under en tid i våras inte kunde använda IHL var det en katastrof”, menade en handläggare och syftade på turbulensen kring EU-domen (se avsnitt 4.3).

I ett ärende där personen deltagit i träningsläger utomlands och hade kontakter med våldsbejakande personer var syftet med IHL att kunna identifiera särskilda möten och kontakter i syfte att kunna sätta in fysisk spaning. ”IHL är kostnadseffektivt och ger en tydlig bild av kontakter, frekvens och geografisk dygnsrytm. Det blir en mindre höstack att leta i”, förklarade en handläggare.

En belysande argumentation för att använda IHL och inte i för hög grad förlita sig på andra källor, eller ha tillgång till andra säkra källor, är hämtad från en promemoria i ett ärende: ”Säkerhetspolisen saknar i dagsläget förmåga att med andra medel inhämta

egen information för att klargöra [namn] avsikter och kopplingar till terrorism.”

Vad som också avses är att det inte är möjligt eller realistiskt att använda sig av fysisk spaning. Utan trafikdata kan det vara svårt att fysiskt lokalisera personer. Det kan också vara ett problem att smälta in i miljön utan upptäckt. Ett skäl som ofta kommer upp i samtalen med handläggare är hur resurskrävande det är med fysisk spaning. Ofta måste flera spanare användas samtidigt i ett uppdrag. I vissa situationer åtskilliga spanare, särskilt om operationen pågår under en tid. Det är tydligt att Säkerhetspolisen prioriterar mycket hårt i hur spaningsresurserna får användas. Dessa går knappast att räkna med i en normal uppföljning.

Som nämnts är det vanliga skälet till att IHL sätts in att en person nyligen kommit hem till Sverige efter att ha deltagit i träningsläger och strid i länder där terrorism förekommer. En typisk kortfattad handläggarkommentar är, ”hade kommit hem, vi behöver kolla vilka kontakter de har”. Som nyss nämnts är den stora frågan om de har något fortsatt uppdrag i Sverige.

Ett annat mindre vanligt skäl är att personen utomlands har en ställning inom al-Qaida och följaktligen har en rad sådana kontakter. Att vara initierad innebär också att ha detaljerad kännedom om tidigare terrorattentat. En person som hade sökt asyl i Sverige misstänktes ha kontakt med en medlem i al-Qaida, dessutom med kunskap om bombtillverkning. Den fråga som ställdes var om den asylsökande skulle hjälpa till med någon form av uppdrag. Det gällde därför att lokalisera den asylsökande och undersöka om han hade kontakt med kända attentatspersoner. Ett annat ärende gällde en person med stark koppling till al-Qaida och som vistades i Sverige. ”Varför Sverige?”, frågade handläggaren, och ”vad har han för kontakter?”

I ett fall menade handläggaren att det hade kommit in så mycket information i inkorgarna att han blev prioriterad. Uppgifterna var så allvarliga att Säkerhetspolisen lade ner extra resurser. Samma sak gällde i ett annat ärende där graverande uppgifter kommit från olika håll. En källa var Säkerhetspolisen dessutom osäker på, och det var därför viktigt att kunna bekräfta eller avfärda källuppgiften.

Vad räknade man med att få för information?

IHL betraktas av intervjupersonerna som en inledande form av hemliga tvångsmedel och, i förhållande till löpande inhämtningskorgar som registerslagningar och uppgifter från informatörer, en stegrad form av löpande inhämtning. Det finns graverande uppgifter om brottslig verksamhet, men som nämnts är dessa för vaga för att nå upp till kraven för preventiva tvångsmedel eller att inleda förundersökning och använda de tvångsmedel som då står till buds. Beroende på vilka uppgifter som kommer fram genom en IHL kan Säkerhetspolisen gå vidare. Av flera intervjuer framgår att handläggarna tänker att de inhämtade uppgifterna skulle kunna leda till att ytterligare steg tas, och att det till och med kan sluta med förundersökning.

Vilka kontakter har han och finns det något som tyder på aktivitet? Har han tät kontakt med den region i vilken han varit? Har han med sig ett uppdrag? Kan kontakter tolkas som att personen har ett uppdrag, eller har han lämnat terrorn bakom sig? Det är frågor som Säkerhetspolisen hoppas få svar på genom att analysera trafikdata.

Som nämnts handlar IHL väldigt mycket om kontakter. Säkerhetspolisen ”börjar lite försiktigt med att utröna vilka kontakter de har”, beskriver en handläggare. Finns det kopplingar till kända nummer? Kommer det upp okända nummer som bör följas upp?

Säkerhetspolisen räknar möjligen med att genom kända kontakter få uppgifter om kopplingar till internationell terrorism. Det kan även vara möjligt att se om telefonen används på ett ovanligt men regelbundet sätt, exempelvis att den är i bruk vid vissa tidpunkter, men inte vid andra.

Även personens rörelsemönster kan ge vägledning, exempelvis genom att det tyder på att han eller hon deltar i vissa möten. Ibland kan sådana möten kretsa kring en ”väldigt viktig person”, som var fallet i ett ärende. Resor till andra städer och följaktligen möten där är centrala frågor i flera IHL-operationer.

När det finns allvarliga uppgifter räknar vissa handläggare med att IHL ska ge ”massiv materia” i betydelsen värdefull information. Samtidigt erkänner man att IHL kan vara ett trubbigt verktyg, med många in- och utgående nummer.

Vilken information fick man fram?

”Personen uppträdde normalt, men hade vissa intressanta kontakter”, beskriver en intervjuad handläggare. I ett annat ärende kom det fram nya för Säkerhetspolisen tidigare okända kontakter som visar att personen ingår i ett nätverk. Som nämnts är det ett ganska vanligt resultat i ärendena att ytterligare kontakter avslöjas.

I ett ärende kom ”högintressant” information fram om terrorism. Informationen indikerade en omfattande kontaktverksamhet inom den våldsförespråkande islamistiska miljön. I en operation menade handläggaren visserligen att personen inte hade några fortsatta kontakter i Syrien, men väl ett större kontaktnät än vad Säkerhetspolisen hade räknat med.

En IHL-operation bekräftade andra källor om att personen med bil hade rest till en stad och deltagit i ett viktigt möte där en synnerligen inflytelserik person skulle ha medverkat.

Det var tvetydiga uppgifter som kom fram i ett ärende. Det var inget som ”stod ut”. En källa kunde dock avfärdas. Även i ett annat ärende var det inget som ”stack ut”, även om personen använde sina telefoner flitigt. Säkerhetspolisen menade dock att det var en ”intressant” person och uppföljningen fortsatte därför, men utan att utökas. Senare kom dock uppgifter fram att han varit mer aktiv med terrorrelaterad aktivitet än vad IHL:n hade visat.

I ett ärende som i hög grad byggde på uppgifter från utländska tjänster kom fram att personen inte hade de kontakter som han borde ha haft om informationen hade varit korrekt. Det fanns inte heller några andra besvärande uppgifter, exempelvis att en asylsökande i Sverige företog ”konstiga resor”.

För en person som Säkerhetspolisen fortfarande har uppföljning på kom inte några alarmerande uppgifter fram genom IHL. Personen reste en hel del till Syrien under förespegling av att det var av humanitära skäl. Säkerhetspolisen misstänker dock att det finns en dold agenda. Därför fortsätter uppföljningen.

Resultat

”Personen kunde avföras eftersom han inte bedömdes som ett säkerhetshot”, konstaterar en handläggare i ett ärende. En av Säkerhetspolisens källor kunde ifrågasättas vilket har betydelse för fram-

tiden. I ytterligare ett fall visade det sig att uppgifterna inte stämde och att han kunde avföras. I något fall kunde Säkerhetspolisen sätta in vissa stödjande insatser eftersom personen befann sig i en utsatt position i en radikal miljö.

Efter IHL visade sig att de tidigare uppgifterna var överdrivna och därför gick den fortsatta uppföljningen ned i intensitet: ”Situationen var inte så akut som vi trodde.” Längre fram kom dock uppgifter fram som gjorde att uppföljningen återigen gick upp i ett högre läge.

Den vanliga situationen är dock att Säkerhetspolisen fortsätter att följa upp personen. Redan IHL innebär en ökad uppföljning, och sedan kan man fortsätta med de instrument som står till buds, exempelvis spaning och att rikta informatörers uppmärksamhet mot personen. Även andra tvångsmedel kan sättas in, men först efter domstolsbeslut. Den stora frågan efter en IHL-operation är vad som ska ske härnäst: ”Ska vi avskriva det här, eller gå vidare?” Vilka uppgifter som kommit in i kombination med tillgängliga resurser bestämmer den fortsatta inriktningen.

Ett IHL-ärende betecknades som ”oerhört framgångsrikt”. Säkerhetspolisen fick därmed ett intressant rörelseschema för personen som ledde vidare till intressanta platser för boende och uppslag till ”samlingshubbar”. Dessutom kom det fram telefonnummer till kända våldsförespråkare i nätverket. I ett annat ärende beskrevs en sedan tidigare intressant person bli ännu mer intressant. Säkerhetspolisen prioriterade och satte in fysisk spaning som är mer resurskrävande.

Även om en person efter en IHL-operation fortfarande beskrivs som ”högaktuell”, kan uppföljningen gå ner i intensitet till följd av vistelse utomlands. I det ärendet kom information även in om personer som rest till Syrien, vilka som kunde tänkas resa dit och i vilka kluster rekrytering förekommer.

I några ärenden bedömdes personerna vara fortsatt intressanta och därmed prioriterade, men på grund av resursbrist sker inte den följande uppföljningen på den nivå som handläggarna önskar. Ibland kan det bero på att personen inte var så central som man inledningsvis hade trott. Återigen kan bristande resurser tala sitt tydliga språk.

Ett ärende ledde till frihetsberövande. Det var dock främst annan information än från IHL som användes som underlag. Säkerhets-

polisen hade i stället ”god källtäckning”, som en handläggare uttryckte det. Även i ett annat ärende hade intresset ökat från Säkerhetspolisens sida, men det berodde inte primärt på IHL utan andra uppgifter.

Integritetsintrång

IHL är ett integritetskänsligt tvångsmedel som syftar till att förebygga, förhindra och upptäcka brottslig verksamhet. En avvägning görs därför i varje ärende mellan nyttan av IHL och intrånget i den personliga integriteten. Ibland kommer särskilda frågor om integritet upp i ett ärende. I ett sådant fall visade det sig att abonnemangen tillhörde en vän till den aktuella personen. Det var en viktig fråga som diskuterades internt på Säkerhetspolisen, hur man skulle göra. I övrigt är integritetsfrågorna inte särskilt komplicerade i ärendena mot bakgrund av de intresseavvägningar som görs i ärendena.

Den vanliga situationen är att mobiltelefon och abonnemang tillhör den aktuella personen och det är också den personen som är användare. Följaktligen är det knappast några utomstående som använder den telefon som omfattas av IHL. Integritetsintrånget är därmed begränsat till brukaren av mobiltelefonen och givetvis de som har kontakt med det aktuella telefonnumret.

9.2.2.3 Terrorbrott – ensamagerande

Organisation?

En udda grupp personer kallar Säkerhetspolisen för ensamagerande. Deras inriktning ligger inom terrorbrott. Det som skiljer dem från andra som Säkerhetspolisen följer upp under rubriken terrorbrott är att de ensamagerande så vitt känt inte tillhör någon grupp och inte heller befinner sig i en miljö med likasinnade. De är helt enkelt ensamagerande.

Den omständigheten att de saknar grupptillhörighet, inte finns i någon särskild miljö och ganska ofta inte heller har några kontakter med för Säkerhetspolisen kända personer gör dem svåra att upptäcka. Vissa av dem kan också ha en mycket långsiktig agenda. I tysthet och med stor beslutsamhet förbereder de sina dåd. Efter

genomgången av 60 IHL-ärenden framstår de ensamagerande som den största utmaningen för Säkerhetspolisen i fråga om att upptäcka och möjlighet att fånga upp, låt vara att de rimligtvis är väsentligt färre till antal än exempelvis de talrika Syrienresenärerna. Samtidigt kan det givetvis vara svårt att bedöma deras förmåga och vilja att utföra terrorbrott.

Samtliga ärenden om ensamagerande som undersökts kan, jämfört med de tydliga mönster som finns framför allt inom de nyss beskrivna terrorärendena med koppling till kända miljöer samt spionagefallen i avsnitt 9.2.2.5, beskrivas som ovanliga, udda, överraskande och ibland sensationella. Ett ärende som ändå är särskilt ovanligt i denna heterogena samling, gällde en person med en bakgrund både i militanta islamistiska nätverk och traditionella kriminella grupperingar. Utomlands hade han tidigare deltagit i både träning och strid. Vad som föresvävade Säkerhetspolisen var risken för ett attentat utan koppling till hans tidigare förflutna med islamistisk inriktning.

Ett annat särskilt ovanligt ärende gällde en person med säregna kontakter. De frågor som Säkerhetspolisen ställde var om personen skulle utföra ett attentat och vilka kontakter denne haft för att skaffa förberedelsematerial?

Indikationer på brottslig verksamhet

På samma sätt som för de tidigare terrorärendena finns indikationer på brottslig verksamhet. Det gällde bland annat inköp av material av udda slag som kan tyda på attentatsförberedelser och att ett telefonnummer kunde knytas till en gärningsperson i omedelbar anslutning till ett utfört terrordåd utanför Sverige. I ett ärende kom informationen från en utländsk tjänst. I ett annat fall var det ett tips från en myndighetsperson som hade gjort vissa iakttagelser.

Ett fall gällde en person som hotade med att utföra ett sprängattentat i Sverige. Han hade också kontakter med personer utomlands som var knutna till en terrororganisation. Kontakt hade också tagits med en annan person, en mycket känd terrorist. Även om det initialt saknades indikationer på brottslig verksamhet var kontakten med terroristen tillräckligt uppseendeväckande för att Säkerhetspolisen skulle agera.

Ett ärende gällde en person med tidigare stridserfarenhet och kunnande om sprängmedel. Enligt Säkerhetspolisen hade en avsikt vuxit fram eftersom han hyste agg mot samhället. När han sedan gjorde några uppseendeväckande inköp befarade Säkerhetspolisen att han planerade ett sprängdåd.

I ett annat ärende hade personen uttryckt att måltavlan för terrordåd borde vara moskéer och regeringar. Även om ensamagerande i hög grad håller sig för sig själva, har flera av dem ett behov att på något sätt manifestera sig ”offentligt”. Det kan ske via sociala medier eller konversationer på Flashback.

Risk

Som framgått är det vanligt att, när uppgifter kommer in till Säkerhetspolisen om en potentiell ensamagerande, han eller hon är tidigare okänd. Skillnaden är därför stor mot de personer som Säkerhetspolisen i vanliga fall arbetar mot i terrorsammanhang. Det är som om de ensamagerande kommer från ingenstans.

När personer som i de flesta undersökta ärenden om ensamagerande kommer från ”ingenstans” är det givetvis särskilt svårt för Säkerhetspolisen att bedöma förmåga och avsikt. Det är mycket enklare att komma fram till en slags grundbedömning för personer som tillhör kända miljöer. Samtidigt är personerna udda och kan uppfattas som särlingar, och för Säkerhetspolisen är det en komplicerad uppgift att skilja fantasier och överdrifter från realiteter.

Flera av de ensamagerande finns inte i kriminalregistret. De finns inte heller på ”myndigheternas radar”. Ett träffande omdöme från en intervjuad handläggare är att personen är ”helt blank”.

Ett fall gällde dock en för Säkerhetspolisen känd person eftersom han hade ett förflutet som tilldragit sig myndigheternas uppmärksamhet.

Säkerhetstänkande

Säkerhetstänkandet är högt utvecklat. ”De arbetar under radarn”, som en intervjuad chef uttryckte det. Norrmannen Anders Behring Breivik som utförde terrordådet i Oslo och Utøya 2011 har i ett manifest beskrivit hur man undgår upptäckt från myndigheternas

sida. Manifestet innehåller också en checklista. Av några undersökta ärenden förefaller det också som om ensamagerande har ett intresse för säkerhetsfrågor. Det har förmodligen att göra med deras läggning, målmedvetenhet och uthållighet. Hemlighetsmakeriet är en del av personligheten och livsföringen.

En ensamagerande i ett ärende beskrivs som mycket skicklig att hemlighålla vad han håller på med. Begränsad användning av telefon tyder på andra vägar för kommunikation. Krypterad kommunikation sker på internet. En annan strategi är att vara skriven på en adress men i realiteten bo på en annan, hemlig adress.

För att upptäcka ensamagerande utgår Säkerhetspolisen inte från ideologisk inriktning eller politisk uppfattning utan från personernas beteende. Personerna beskrivs som mycket avvikande. Ofta är de något av enstöringar. Som nyss nämnts har de trots få sociala kontakter ett behov av att föra fram sina uppfattningar. Lyhörda mottagare som rätt kan tolka och värdera dessa signaler kan identifiera en möjlig ensamagerande. I läggningen ligger också i att vara försiktig, långsiktigt och väl planera det som ska åstadkommas. För att referera till Breivik igen förberedde han sig i nio år. En intervjuperson menade därför att det knappast är möjligt att spana på ensamagerande eftersom ”de inte gör någonting”, deras tidshorisont är ofta lång. Den enda möjligheten för Säkerhetspolisen kan därför ofta vara IHL, i vart fall som ett inledande tvångsmedel.

Miljön

En intervjuperson betonar att Säkerhetspolisen liksom andra säkerhetstjänsters inhämtningsmetoder ”bygger på att människor ingår i miljöer och kommunicerar med varandra”. Ett av de stora problemen med att upptäcka ensamagerande är därför att de inte ingår i någon miljö och är mycket försiktiga med att ta känsliga kontakter. I några av ärendena har dock kontakt tagits med ”kända” personer och Säkerhetspolisen hade på det sättet kunnat hitta fram.

Omständigheter som gjorde att IHL sattes in

Som redan nämnts är en stor skillnad mot de tidigare terrorärendena att de ensamagerande verkar ensamma i det fördolda. Normalt finns därför inte en uppföljning som kan öka i intensitet när illavarslande uppgifter kommer in. I stället kännetecknas flera av ärendena om ensamagerande av att Säkerhetspolisen fått mycket allvarlig information. I några fall har uppgifterna tytt på akuta situationer som fört med sig att Säkerhetspolisen agerat direkt. Utan tidigare uppgifter och med visserligen olycksbådande information, men ändå vag, gör att IHL har använts. Som tidigare nämnts hör dessa situationer med omedelbar användning av IHL till undantagen.

I ett fall hade kontakt tagits med en känd terrorist och i ett annat ärende var det inköpen som ”triggade igång IHL:n”. I ett annat fall var det vissa kontakter av oroväckande natur – personer med förmåga att begå terrordåd – i kombination med uttalanden på internet. Är personen ”fågel eller fisk”, var frågan som ställdes och IHL bedömdes som en ”temperaturmätare” för att bedöma risken för attentat.

Vad räknade man med att få för information?

Som framgick av föregående avsnitt om terrorbrott, räknar Säkerhetspolisen med att IHL ska ge en uppfattning om en persons kontaktnät, framför allt med andra intressanta personer. Med hänsyn till att ensamagerande är försiktiga och håller sig för sig själva är det inte främst kontakter med likasinnade som efterfrågas. I stället är det kontakter som tyder på beställning av varor och tjänster som kan ge någon vägledning om vad den ensamagerande håller på med och har för inriktning. Kontakter med leverantörer är således av stort intresse. I ett fall hade Säkerhetspolisen spanat på personen utan att det hade gett någonting. Samtidigt fanns uppgifter som gjorde att IHL sattes in för att få ytterligare information.

Vilken information fick man?

I ett av de granskade fallen vägrade teleoperatören att med hänvisning till EU-domstolens dom lämna ut några trafikuppgifter. Följaktligen genomfördes aldrig IHL-operationen och någon information kom inte fram. Ärendet gällde hot om ett bombdåd i Sverige.

I en IHL-operation kom uppgifter fram om olika kontakter, bland annat om olika inköp. Dessutom kunde vissa misstankar om personens förehavande beläggas. I ett annat ärende stärktes dock inte några misstankar med anledning av IHL. Nyttan med operationen var dock kunskapen om att det inte förelåg någon ”akut attentatsplan”.

I några fall hade kontakter tagits med personer med anknytning till terrorism, en faktor som selekterar fram dem i Säkerhetspolisens inhämtning. Vad som givetvis oroar Säkerhetspolisens handläggare är de personer är tillräckligt försiktiga för att inte ta sådana kontakter.

Resultat

Efter en IHL-operation kom tillräckligt graverande uppgifter fram som gjorde att Säkerhetspolisens intresse ökade och personen är under fortsatt uppföljning. Som tidigare nämnts kan dock tidsförloppet till planerad handling vara mycket långt. Varken avlyssning eller förundersökning var dock aktuellt vid tidpunkten direkt efter IHL.

I ett annat ärende var personen sedan tidigare under uppföljning och efter IHL-operationen gick Säkerhetspolisen ned till uppföljning på normalnivå. Skälet var att inga graverande uppgifter hade kommit fram i IHL:n.

I ett IHL-ärende fortsatte uppföljningen, men på en lägre nivå. Enligt Säkerhetspolisen finns en avsikt att begå terrorbrott, men förmågan saknas. På sikt bedöms personen dock kunna avskrivas till följd av den bristande förmågan.

Integritetsintrång

För integritetsdiskussionen, se avsnitt 9.2.2.2. På liknande sätt som för terrorärendena är integritetsfrågorna tämligen okomplicerade eftersom det handlar om mobiltelefoner som är knutna till en viss person på ett helt annat sätt än en fast telefon.

9.2.2.4 Politisk extremism

Grupperingar

De grupperingar som Säkerhetspolisen följer upp inom ramen för politisk extremism är knutna till den autonoma rörelsen (vänsterextremism) och vit makt-miljön (högerextremism). De autonoma grupperingarna är företrädesvis Revolutionära Fronten (RF) och Antifascistisk front (Afa). På vit maktsidan dominerar Svenska Motståndsrörelsen (SMR) och personer knutna till Svenskarnas Parti (SvP). På den autonoma sidan förekommer också så kallade aktionsnamn, där personer agerar under ett visst namn utan att det egentligen är en bestämd organisation. I stället kan personer från olika organisationer agera under aktionsnamnet.

Dessa miljöer beskrivs som ”stora och spretiga”, och därför är det svårt för Säkerhetspolisen att peka ut gärningspersoner. Extremistmiljöernas säkerhetstänkande försvårar ytterligare att identifiera personer, det är ”inga syjuntor, för att tala öppet”, som en intervjuad handläggare uttryckte det.

Den autonoma miljön är för individens frihet och mycket långtgående personliga rättigheter. De är motståndare till stora amerikanska företag. Vit makt-miljön är färgad av den ariska tanken och driver en extremt nationalistisk linje. Inom vit makt-rörelsen finns en falang som vill orsaka stora kostnader för det allmänna. Skadegörelse ses därför som början till en revolution. Skadegörelse ingår också som en metod i den autonoma miljön.

I utkanterna av både den autonoma miljön och vit maktrörelsen befinner sig också personer som betraktas som särskilt extrema. De kan vara beredda att gå längre än dem som ägnar sig politisk brottslighet på någon slags normalnivå. Exempelvis i ett ärende karaktäriseras en sådan person av en intervjuad handläggare som ”alltför radikal” för vanliga organisationer på yttersta högerkanten. Det handlar om en grandios personlighet med en vilja att ”göra sig känd i världen”. Hos Säkerhetspolisen uppstår stor oro när en sådan person verkar förbereda något radikalt.

Indikationer på brottslig verksamhet

Det är vanligt att den politiska extremismen har varandra som ömsesidiga måltavlor, vilket resulterar i olika våldsbrott. Särskild den autonoma miljön använder sig av ”hembesök”, där vit maktanhängare utsätts för fysiska angrepp och deras bostäder för skadegörelse. Dessa ofta nära förestående våldsbrott och skadegörelsebrott hanteras ofta av Säkerhetspolisen med preventiva tvångsmedel, ofta telefonavlyssning (SOU 2012:44). IHL förutsätter dock att det är fråga om mycket allvarliga brott och inte den ”vanliga” kriminalitet som ofta förekommer inom de båda miljöerna. I de ärenden som ingår i undersökningen har brottsligheten trappats upp till befarad mordbrand, förberedelse till mord och andra grova våldsbrott av terrorkaraktär. På det sättet liknar IHL-operationerna med koppling till politisk extremism ärendena om terror, både grupperingar och ensamagerande.

Ett ärende på den autonoma sidan hade en bakgrund i systematisk otillåten påverkan mot myndighetslokaler, myndighetspersoner och förtroendevalda. Det gällde främst skadegörelse och trakasserier. Brotten hade dock urartat i mordbrand.

Inom vit makt-miljön förekommer en hel del vapen och följaktligen sker vapenträning som förberedelse till aktioner, och i förlängningen revolutionen. Det finns också ett kunnande att tillverka enklare bomber som molotovcocktails. Ett ärende handlade om ett planerat mord mot en politisk motståndare inom den motsatta politiska miljön. Det skulle vara en reaktion på upptrappad våldspiral mellan miljöerna. ”Känslan finns att måttet nu är rågat”, som en handläggare förklarade mobiliseringen i miljöerna.

Angrepp, motangrepp och hämnd är således vanliga inslag i konflikten mellan de båda extremistlägren. Språkbruket är uppskruvat och det talas om hämnd och våld, men en annan sak är vad som faktiskt sker. Även om organisationerna är strikta beskrivs individerna som oberäkneliga och svårstyrda. Denna oberäknelighet kan dock i undantagsfall gå åt andra hållet, och leda till mycket allvarliga brott.

I ett annat ärende karaktäriserades en person som ”något av en pratmakare”. Enligt den intervjuade handläggaren kanske det ”räcker för honom att ha några beundrare på Facebook och träffa lite kända människor”.

I ett ärende som gällde vit makt-miljön fanns kontakter in den kriminella mc-miljön. Mc-miljön figurerar också i periferin i ett annat ärende som gällde vapen där personen beskrivs vara fascinerad av ”krig, vapen, militaria, nazism och mc-gäng”.

Den autonoma miljön föredrar gatustridsvapen och enklare bomber. I ett ärende fanns dock misstankar om tyngre beväpning och sprängmedel samt en koppling till att ett nätverk av cellstruktur som skulle vara under uppbyggnad. Det ärendet skiljer sig dock från den allmänna beskrivningen som ges av den autonoma miljöns resurser.

Enligt Säkerhetspolisen har den autonoma miljön en god kartläggningsförmåga gentemot politiska motståndare (särskilt Sverigedemokraterna, Svenska Motståndsrörelsen och Svenskarnas parti) och har byggt upp ett varumärke baserat på fruktan. Det attraherar i sin tur våldsbenägna personer. Även personer på den autonoma sidan bedöms vara oberäkneliga. I ett fall karaktäriserades en person som överdrivet ”impulsiv”.

Den goda kartläggningsförmågan inom den autonoma miljön tar sig också uttryck i ett stort datakunnande med dataintrång som metod. Stora delar av den autonoma miljön korrelerar med hackermiljön; allt ska vara fritt, det ska inte finnas några lagar eller andra regleringar. Dataintrång används även som ett angreppsmedel där aktivister påstås ha tagit sig in i några viktiga myndigheters datasystem. Drivkraften hos dessa hackers är inte enbart politisk utan också att imponera på sina likasinnade med teknisk briljans.

Risk

I ett ärende hade Säkerhetspolisen visserligen tillgång till vissa källor, men det fanns indikationer på att personer ur olika grupperingar på den autonoma sidan skulle delta i kommande brottslighet. Där fanns dock en informationsbrist som Säkerhetspolisen ville kompensera med mängddata, det vill säga IHL. Det gällde att ”hitta rätt personer i denna röriga krets”, som en handläggare uttryckte det. ”Vilka knytpunkter finns? Vilka är de centrala personerna?”

I ett fall i extremistmiljön fanns uppgifter om att vapenträning hade ägt rum på en bestämd plats. Syftet skulle vara att förbereda ett mord.

Ett ärende gällde en person som Säkerhetspolisen tidigare hade intresserat sig för och som bland annat ägnade sig åt långtgående hacking. Mot bakgrund av hans kapacitet sattes IHL in när det kom in oroande information som kunde tyda på allvarlig brottslighet. Det var dessa uppgifter som Säkerhetspolisen ville få bekräftade.

I ett ärende hade Säkerhetspolisen ”dåliga ingångsvärden”. Dock var det bara en ”single source” och det behövdes ytterligare information. Samtidigt var uppgiften från källan mycket oroväckande och i förlängningen kunde det handla om människoliv.

I ett fall som gällde flera personer och därmed ärenden befarade Säkerhetspolisen att brottsligheten skulle avse mordbrand mot myndighetslokaler och allvarliga våldsbrott. Det fanns en historik som pekade i den riktningen. I flera andra ärenden figurerar också vapen och bomber, vilket återigen illustrerar terrorinslaget i IHL-ärendena om politisk extremism.

I ett ärende som gränsar till ensamagerande ställde intervjupersonen frågan om det förekom ett ”lonely wolf syndrom”. Svaret blev nej, men enligt den intervjuade handläggaren var personen så ”kufisk att det ändå finns en risk för att det är en Breivik”.

Säkerhetstänkande

Framför allt inom den autonoma miljön är säkerhetstänkandet högt utvecklat. Det är en ”generation uppvuxen med datorer” och därför är IT-kunnandet högt, som en handläggare påpekade. Det finns till och med en säkerhetshandbok som stöd. Särskilda aktivisttelefoner med kontantkort används för kommunikation. Kommunikation sker ofta via olika sms-listor.

Genom fysisk spaning och telefonavlyssning framgår att personer i den autonoma miljön undviker klartext i telefonsamtal. Koder används, och ett meddelande om att exempelvis samlas för att måla banderoller kan i stället betyda att en aktion av annat slag ska genomföras. Vid sådana aktioner lämnas mobiltelefoner kvar i bostaden för att undgå spårning.

Även inom vit makt-miljön finns ett säkerhetstänkande, men det är generellt sett något mindre utvecklat än på den autonoma sidan. Särskilt Svenska Motståndsrörelsen med sin militaristiska inriktning anges dock lägga stor vikt vid säkerhet. Erfarenheten är

att telefonavlyssning inte brukar ge särskilt mycket information. Krypterade chattar eller Skype används för kommunikation. Enbart ett fåtal mycket betrodda personer känner till platser där eventuella vapen förvaras. För utomstående som Säkerhetspolisen är det svårt att få insyn i vad som äger rum inom organisationerna. Medlemmarna drillas hårt i säkerhet och säkerhetsfrågor diskuteras på möten.

Omständigheter som gjorde att IHL sattes in

Säkerhetspolisen har en uppföljning av både den autonoma och vit makt-miljön. Ofta är det något som händer som gör att IHL sätts in. Det finns indikationer på brottslig verksamhet. Däremot saknas mera konkreta uppgifter om vilket brott som ska begås, mot vem och när. Uppgifterna är för vaga för att kunna inleda förundersökning eller använda preventiva tvångsmedel, menar de intervjuade handläggarna. IHL används därför i underrättelseverksamheten för att komma framåt i kartläggningen.

Ibland är också underrättelseläget begränsat. Det är för lite uppgifter i ”korgarna” samtidigt som det finns indikationer på brott.

På en ort började det hända saker och en rad allvarliga aktioner från de autonoma genomfördes. ”Det var som en hälsning, nu kör vi”, och därför behövdes ytterligare information om vad som var å färde.

I ett ärende ville Säkerhetspolisen göra sin kartläggning steg för steg, vilket är ett vanligt sätt att resonera på hos intervjupersonerna. Valet faller då ofta på IHL. Det kom dock fram sådana uppgifter genom IHL:en att stress uppstod och Säkerhetspolisen fick i stället tillstånd att avlyssna telefoner.

Ett IHL-ärende gällde en akut situation med en påstådd situation där sprängmedel skulle förvärvas. Ett annat ärende var också akut eftersom det fanns starka indikationer på vapenanskaffning i syfte att genomföra ett lönnmord.

Vad räknade man med att få för information?

Säkerhetspolisen räknar med att få klarlagt om den aktuella personen har kända kontakter som kan bekräfta eller avfärda andra uppgifter om att allvarlig brottslighet är på gång. Det handlar om

”mobilgenerationen” och därför förekommer sms flitigt. Det anses viktigt att använda IHL för att med hjälp av olika kontakter som tas få indikationer på personers förmåga, och ibland också vilja att agera. Kunskap om personernas kontaktnät anses också mycket värdefullt. Genom IHL går det att få bekräftat tidigare kända uppgifter och kartlägga för att få ny information.

I ett ärende ville Säkerhetspolisen undersöka om det fanns kontakter mellan några personer i vit makt- och mc-miljön. Faran ligger i att mc-miljön bedöms ha lättare att få tag på vapen och sprängmedel som riskerar att levereras till vit makt-miljön. Även geografisk positionering kan ge indikationer på att de aktuella personerna är på väg mot en viss ort där det skulle finnas en kontaktperson.

I ett annat ärende ville Säkerhetspolisen undersöka i vilka kretsar personen rörde sig, även om han reste till en viss stad. Det kunde ge en fingervisning om de befarade attentatsplanerna.

Vilken information fick man fram?

I en operation som gällde flera personer och ärenden kom det fram uppgifter som tydde på förestående brottslighet.

I en annan operation fanns uppgifter om att några centrala personer hade befunnit sig på en viss ort, vilket bekräftade annan information. Även kontaktnätet kunde identifieras och det kom fram oroväckande information om att den yngre generationens aktivister hade kontakt med den äldre bestående av relativt etablerade personer. Däremot saknades uppgift om att de aktuella personerna hade vistats i ett visst område vilket innebar att de befarade attentatsplanerna inte skulle förverkligas.

I ett ärende som gällde den autonoma miljön visade det sig att personen hade mycket kontakt med en rad kända aktivister. En av dem var föremål för förundersökning och några andra kopplades till en mordbrand. ”Det osar katt”, som en handläggare uttryckte det.

Säkerhetspolisen fortsatte uppföljningen, men gick ned i ”normalläge” eftersom situationen inte bedömdes som akut. Den öppna polisen hade varit aktiv mot de autonoma vilket hade fått en avkylande effekt på vit makt-miljöns hämndplaner. Inom vit maktmiljön hade tidigare funnits en besvikelse över att den öppna polisen

inte hade gjort mer för att komma till rätta med de autonomas återkommande våldsutövning.

I ett ärende kom fram att personen mest hade kontakt med ”mc-busar och gamla kompisar”, vilket visade att attentatsplanerna inte var nära förestående; han var ”inte riktigt på G”.

Resultat

”Tvångsåtgärder handlar om nivåer på uppföljning”, som en handläggare uttryckte det. De personer som är föremål för IHL är ändå aktuella för Säkerhetspolisens intresse och uppföljning. Men när temperaturen stiger kan IHL sättas in. Om det inte bekräftar att något är på gång, kan uppföljningen gå tillbaka till ett normalläge. Är dock uppgifterna tillräckligt konkreta och alarmerande, finns andra tvångsmedel att ta till eller fortsätta med, som telefonavlyssning. I ett fall kunde Säkerhetspolisen tack vare IHL gå vidare med telefonavlyssning och förundersökning inleddes.

I ett fall visade IHL att en autonom gruppering var aktiv och därför får den högre prioriteten inom Säkerhetspolisen. I vart fall var det tänkt så, men det är alltid ”en resursfråga”, påpekade en intervjuad handläggare.

I ett ärende fortsatte Säkerhetspolisen att kartlägga och i slutändan inleddes förundersökning, men för andra brott som gällde otillåten påverkan mot politiker och myndighetspersoner. IHL:n bekräftade kopplingar av allvarligt slag till kända extremistkretsar och Säkerhetspolisen kunde dessutom ringa in ytterligare personer som tidigare hade varit okända.

”Vi höll bevakningen, men stegrade den inte”, berättade en intervjuad handläggare om ett ärende som inte visade sig lika akut som befarat. Han beskriver att fördelen med IHL är följande. ”Man ökar sin kunskap och får snabbt en normalbild. Innan terrormisstanken och i närheten av ett datum, är det några förändringar? Har han många kontakter med förmågehöjande, exempelvis grovt kriminella med tillgång till vapen? Även andra tecken på förberedelse kan iakttas, exempelvis kontakt med resebyråer. Kommunikation behövs för det mesta i dagens samhälle.”

Integritetsintrång

För integritetsdiskussionen, se avsnitt 9.2.2.2. Det faktiska integritetsintrånget är som det befarade eftersom det handlar om mobiltelefoner som är personliga. I ett ärende var dock ett nummer felaktigt så uppgifterna lades i ”tuggen”.

9.2.2.5 Spionage och flyktingspionage

Traditionellt spionage

Främmande makt är intresserad av svensk högteknologi och vetenskapliga framgångar, men också av vilka säkerhetsbrister som finns inom känslig svensk industri- och affärsverksamhet. På många håll i världen skiljer man inte tydligt mellan stat och kapital, vilket får till följd att utländska säkerhets- och underrättelsetjänster kan ha en även kommersiell inriktning. Intresset hos främmande makt gäller givetvis också politiska frågor som avtal mellan länder och positioneringar i olika internationella frågor.

Inget ärende förefaller ha en tydlig riktning mot det svenska militära försvaret, ett annars klassiskt område för spionage. Förklaringen kan både vara att undersökningen trots allt omfattar ett begränsat antal ärenden och att det svenska försvaret uppfattas av främmande makt som mindre intressant.

Verksamheten i Sverige bedrivs av underrättelseofficerare som ofta har olika täckbefattningar på ambassader och andra representationer. De försöker i sin tur värva informationsbärare. Underrättelseofficerare är tränade i spioneriets ädla konst och har i allmänhet stora resurser till sitt förfogande. De är uthålliga och kan ägna mycket möda åt målsökning och värvning. Underrättelseverksamheten kan också vara av betydligt mindre kvalificerad art. Exempelvis kan utländska studenter och praktikanter vid svenska universitet och företag ha fått med sig ett uppdrag till Sverige att förse sitt hemland med hemlig information.

Flyktingspionage

Diktaturer är intresserade av att kartlägga flyktingar som finns i Sverige och framför allt via dem få ytterligare kunskap för att slå ned den inhemska oppositionen. Vissa flyktingmiljöer i Sverige beskrivs som i hög grad infiltrerade av flyktingspioner. Utan att de själva vet om det kan det till och med i en och samma miljö finnas flera spioner. På det sättet kan uppdragsgivaren hålla dem under uppsikt. En intervjuad handläggare berättade om ett sådant aktuellt fall, där alltså Säkerhetspolisen hade bättre överblick än var och en av flyktingspionerna.

Flyktingspionagets syfte är alltså att kartlägga och i förlängningen tysta oppositionen mot regimen i hemlandet. Spionerna rapporterar om bland annat vilka som går på politiska möten, hämtar uppgifter från medlemsregister i oppositionella föreningar, lämnar uppgift om nya medlemmar och personer som förväntas komma till Sverige. Uppgifter om kontakter med oppositionella i hemlandet är givetvis av särskilt stort intresse.

Flyktingspionage är följaktligen en del av den interna säkerhetstjänsten, men bedrivs i annat land, i detta fall Sverige. I de studerade IHL-ärendena rubriceras fallen som grov olovlig underrättelseverksamhet eftersom brottsligheten inte riktas mot svenska intressen (rikets säkerhet).

Förr kunde flyktingspionaget vara mer offensivt på så sätt att flyktingar kunde angripas i asyllandet. Enligt flera intervjupersoner hör det dock till det förflutna. Däremot leder det givetvis till otrygghet att flyktingmiljön är infiltrerad och att förflugna ord kan få allvarliga konsekvenser för personer som fortfarande finns kvar i ursprungslandet. Även släktingar i hemlandet som inte har något annat med oppositionen att göra än släktskap med en flykting riskerar att råka illa ut.

De personer i de studerade ärendena som bedriver flyktingspionage är inte några tränade agenter utan har rekryterats av den utländska säkerhets- och underrättelsetjänsten för att infiltrera flyktingmiljön i Sverige. Rekryteringen kan exempelvis ha skett i samband med att den blivande agenten fängslats på grund av sitt oppositionella arbete. En intervjuad handläggare berättar att de ofta är ”sorgliga gestalter, som fängslats och torterats. Få har en ’flödig’ livsstil.” Flyktingspionen rapporterar sedan till sin handledare som

ofta finns i hemlandet. Dessa kontakter sker ofta med telefon och därför är IHL av intresse. För utlandssamtal spelar också signalspaning stor roll. Möten kan också ske i länder som är positiva till den aktuella diktaturen eller där säkerhetstjänsten är svag.

Indikationer på brottslig verksamhet

Ett fall gällde en utländsk person som samlade på sig stora mängder av känslig information från ett företag. Det fanns även tydliga tecken på att personen försökte hemlighålla denna insamling av uppgifter. Det var företagets säkerhetsavdelning som hörde av sig till Säkerhetspolisen. Även i ett annat ärende tog ett företag kontakt med Säkerhetspolisen eftersom man hade fattat misstankar om spionerі. Ärendet gällde en utländsk underrättelseofficer som Säkerhetspolisen kände till och som försökte värva en uppgiftslämnare.

Ett annat ärende tog sikte på en person i Sverige som hade en befattning knuten till främmande makt som enligt Säkerhetspolisen brukade reserveras för säkerhets- och underrättelsetjänsten. Dessutom samarbetade han med en annan person som Säkerhetspolisen redan visste arbetade under täckmantel.

I ett ärende var omständigheterna egendomliga i samband med att en flykting anlände till Sverige. Till det kom att han i förhållande till Migrationsverket intog olika positioner som inte gick ihop med en flyktingsituation. Sammantaget tydde detta på att han agerade på någons uppdrag, menade den intervjuade handläggaren.

I ett annat ärende om flyktingspionage hade personen varit i kontakt med ett telefonnummer som Säkerhetspolisen visste gick till en diktaturstats säkerhets- och underrättelsetjänst. Dessutom hade personen nyligen vistats i hemlandet utan problem och kunnat lämna landet. I ett annat ärende var personen öppet oppositionell mot regimen i hemlandet via Facebook, men hade samtidigt kontakt med samma regims underrättelse- och säkerhetstjänst.

Risk

Riskerna som de undersökta spionageärendena förmedlar är att främmande makt ska komma över information som är till skada för rikets säkerhet. Det handlar både om industriell och politisk information.

Risken med flyktingspionage är att människor i ursprungslandet fängslas, torteras och till och med dödas. Säkerhetspolisen känner till att flyktingspionage i Sverige lett till tortyr och avrättningar i ett annat land. I ett fall bedömer den intervjuade handläggaren att personen haft ett ”omfattande kontaktnät och sannolikt rapporterat omfattande om personer i miljön och på det sättet kunnat identifiera ett stort antal aktivister”. Personen hade ett dussintal kontakter varje dag, och risken för allvarliga skador var därför stor.

Säkerhetstänkande

Säkerhetstänkandet är mycket högt utvecklat hos utländska underrättelseofficerare. De har genomgått särskild utbildning för att kunna hemlighålla verksamheten. De lägger ned stor möda på att kommunicera med sina agenter utan att utomstående ska komma dem på spåren. I ett ärende förekom en ”operativ telefon” som en underrättelseofficer använde enbart för dolda kontakter. För Säkerhetspolisen innebär det samtidigt att trafikdata från en identifierad operativ telefon kan ge mycket värdefull information om känsliga kontakter, exempelvis om värvade agenter i Sverige.

Även bland flyktingspioner finns ett säkerhetstänkande. De använder påhittade mailkonton och konton till Skype och Facebook. Det är vanligt med en ”fullur” som enbart används för kommunikation med underrättelseofficeren i hemlandet. Enligt en intervjuad handläggare är möjligheterna att i dag hemlighålla kommunikation så stora att sådana åtgärder inte längre behöver vara tecken på en utvecklad förslagenhet.

Omständigheter som gjorde att IHL sattes in

I ett fall hade säkerhetsavdelningen vid ett svenskt företag kontaktat Säkerhetspolisen om sina misstankar. Det var olika graverande uppgifter om informationsinhämtning och konspirativt beteende som gjorde att säkerhetsavdelningen slog larm. Någon formell polisanmälan ville dock företaget inte göra utan lämnade i stället över informationen som underrättelsematerial.

Uppgifter kom in om att en underrättelseofficer hade kontakt med en ”intressant” företagare. Underrättelseofficeren höll också på med att försöka värva ytterligare en person. Samtidigt var kunskapen om underrättelseofficeren bristfällig och det var därför som IHL sattes in. I de fall Säkerhetspolisen inleder förundersökning kan telefonavlyssning inledas.

I ett annat ärende fanns starka misstankar om att en person innehade en ”känd underrättelseplattform” och IHL var därför en bra metod för att konstatera om det var ”bu eller bä”, som den intervjuade handläggaren uttryckte det.

I ett fall tydde mycket på flyktingspionage, men Säkerhetspolisen ville undersöka om han hade påbörjat sin brottsliga gärning och ”sonderade om det kommer att ge något att gå in och lyssna”, det vill säga inleda förundersökning och ansöka om telefonavlyssning. Personen hade varit ganska kort tid i Sverige och Säkerhetspolisen hade gjort den bakomliggande kartläggning som var möjlig att göra. IHL användes ”för att komma vidare”. I ett annat ärende bedömdes IHL som en lämplig början på ett ärende som sedan kunde utvecklas till att exempelvis använda preventiva tvångsmedel. En fördel med IHL är att man kan se i vilka kretsar personen rör sig. Kontakt med kända oppositionella i flyktingmiljön samtidigt som samtal sker med underrättelseofficerare är en tydlig indikation på infiltration och en grund för Säkerhetspolisen att gå vidare.

I ett ärende om flyktingspionage hade Säkerhetspolisen information om att det fanns en kontakt med hemlandets säkerhets- och underrättelsetjänst. Handläggaren förklarar: ”När man har den typen av ingångsinfo är den inte komplett. När man använder IHL får man alla kontakter.” På det sättet går det att få fram om det skett fler kontakter och hur omfattande dessa är. Även kontakter med oppositionella kretsar är också viktiga eftersom det ger en indikation på spioneriets omfattning.

I ett fall hade personen kontaktat det egna hemlandets ambassad i Sverige, vilket är anmärkningsvärt för en oppositionell och flykting.

Vad räknade man med att få för information?

I ett ärende som gällde en utländsk underrättelseofficer hoppades den intervjuade handläggaren på att få uppgifter om intressanta kontakter.

En central fråga är vilka som ligger bakom ett beteende som tyder på spionage eller olovlig underrättelseverksamhet. Vid flyktingspionage är det visserligen uppenbart, och vid andra former kan det också vara en främmande makts säkerhets- och underrättelsetjänst. Men i vissa fall kan det vara ett företag eller till och med att personen på eget initiativ samlar information för att kunna använda den i framtiden, kanske för att sälja. IHL syftar då till att få fram uppgifter om personens kontakter för att på det sättet få klarhet om uppdragsgivaren. Det kan också handla om personens rörelsemönster.

I ett ärende om flyktingspionage ville Säkerhetspolisen undersöka om personen hade börjat ta kontakt med oppositionella. I så fall skulle det vara ett tecken på att spioneriuppdraget hade påbörjats.

Vilken information fick man?

I ett ärende om en utländsk underrättelseofficer kom uppgifter fram om en pågående värvning.

I ett fall om flyktingspionage visade det sig att personen hade många kontantkortskontakter. Säkerhetspolisen försökte spåra numren, men kom ingen vart. Det kunde också vara förklaringen till att kontantkort användes, som kännetecknas av att de är svåra att spåra.

I ett annat ärende fick Säkerhetspolisen ”kvitto på” att personen varit på centrala ställen för hans underrättelseinriktning. Det stärkte misstankarna, även om det inte kom fram några nummer.

I ett ärende om flyktingspionage i vardande, konstaterade Säkerhetspolisen att personen enbart försökte etablera sig i Sverige och inväntade order från uppdragsgivaren. Ett använt telefon-

nummer verkade dock gå till handledaren i hemlandets säkerhets- och underrättelsetjänst.

Resultat

Efter en IHL-operation bedömde Säkerhetspolisen att personen inte var viktig nog att fortsätta att lägga inhämtningsresurser på. Däremot fortsatte Säkerhetspolisen att ha en viss uppföljning och man överväger att ha ett samtal med personen för att klara ut olika frågetecken. Ett sådant samtal kan också ha en förebyggande effekt och stoppa fortsatt flyktingspionage. I ett annat ärende om flyktingspionage fortsatte uppföljningen och vissa telefonnummer som misstänktes gå till en diktaturs säkerhets- och underrättelsetjänst skulle undersökas vidare.

I ett annat fall där misstankarna visserligen bekräftades lade man ärendet på is. Men även om det är vilande, kommer uppgifter att adderas till varandra, och mycket tyder därför på ökad aktivitet från Säkerhetspolisens sida, men först längre fram.

Även om inte mycket kom fram i en IHL-operation, var ursprungsinformationen så stark att brukaren av telefonen betraktades som flyktingspion. Därför fortsätter Säkerhetspolisen med uppföljningen, bland annat gick man vidare med preventiv telefonavlyssning.

I ett ärende med en underrättelseofficer tog Säkerhetspolisen kontakt med den person som var under värvning och förklarade i vilken risksituation han befann sig. På det sättet förebyggdes att en person kunde komma att värvas som agent för främmande makt. Resultatet blev att hans kontakter med underrättelseofficeren avbröts.

I en operation mot en person där Säkerhetspolisen bedriver fler ärenden övervägdes om det var lämpligt att ha ett samtal. Erfarenheten är att samtal är effektiva: ”Vad skönt att ni kommit, nu slipper jag fortsätta”, blev vid ett tillfälle svaret hos en avslöjad flyktingspion enligt en intervjuad handläggare.

Ytterligare ett resultat med ett ärende om en underrättelseofficer var att Säkerhetspolisen lärde sig en del om den utländska säkerhets- och underrättelsetjänstens arbetsmetoder och underrättelseinriktning.

Integritetsintrång

Som för IHL-ärenden överlag är det mobiltelefoner som är i fokus och dessa används också av den person för vilket beslutet om inhämtning gäller. I ett fall förekom också fast telefon och då ökade integritetsintrånget eftersom ytterligare en person i hushållet använde telefonen. I det fallet blev dock det faktiska integritetsintrånget inte så stort eftersom Säkerhetspolisen var intresserad enbart av samtal till ett bestämt land, och därmed tog sikte på enbart en person i hushållet.

9.2.2.6 Massförstörelsevapen

Ett mycket ovanligt ärende gällde spridning av massförstörelsevapen (50). Efter murens fall och östblockets upplösning fanns en stor oro för att massförstörelsevapen skulle få en okontrollerad spridning. I dag är denna fråga inte lika aktuell. Bakgrunden till ärendet var att en utländsk medborgare hade en befattning som bland annat gav honom tillgång till mycket känsliga uppgifter. Säkerhetspolisen befarade att hans hemlands säkerhets- och underrättelsetjänst hade varit i kontakt med honom för att komma över vital information. Mannen befann sig därför i en utsatt position och Säkerhetspolisen hade tidigare kunskap om att den utländska säkerhets- och underrättelsetjänsten arbetade aktivt med värvningar.

Fysisk spaning hade emellertid inte gett något. En massa information hade samlats in och uppgifter hade hämtats in från den aktuella verksamheten. IHL var därför det sista man satte in för att få någon pusselbit som tydde på kontakt med främmande makt. Rubriceringen av ärendet var spionerі.

Inga uppgifter kom dock fram som tydde på kontakt med främmande makt. Ärendet avslutades med att Säkerhetspolisen hade ett hotreducerande samtal med mannen.

9.2.2.7 Några generella iakttagelser

Aktuellt i tiden

Säkerhetspolisens IHL-ärenden speglar i hög grad aktuella strömningar i samhället. Den globala rörelsen att ansluta sig till jihad i Syrien dominerar ärendena med terroranknytning. Några ärenden har kopplingar till viktiga politiska händelser som president Obamas Sverigebesök. Den pågående konflikten mellan autonoma grupperingar och vit makt-miljön, där de senare är på defensiven, avspeglas i flera ärenden där hämndaktioner befaras. Sverige som mottagare av stora grupper flyktingar uttrycks i IHL-operationer om flyktingspionage. Sveriges högteknologiska industri är av intresse för främmande makt. Terroristen Anders Behring Breivik har uppenbarligen inspirerat ensamagerande i Sverige, men utan att något undersökt ärende ens planeringsmässigt har kommit i närheten av dådet på Utøya.

Tidsaspekter och kontakter

Åtskilliga ärenden gäller som nämnts Syrienresenärer. Inhämtningen av trafikdata brukar då koncentreras till tiden runt resan, både till och från Syrien. Skälet är att det är i samband med resorna som viktiga kontakter brukar tas med viktiga personer.

Även om ett ärende gäller en längre tid, exempelvis tre eller sex månader, är det vanligt att analysen som i det nyss nämnda resandefallet inskränker sig till tidpunkten före och efter specifika händelser. Skälet är att minska mängden data som ska analyseras. Det betyder att integritetsintrånget generellt sett är lägre än vad den beslutade tidsperioden för IHL-inhämtningen reflekterar.

IHL handlar om kontakter, kontakter och kontakter. Vilka är dessa och vart leder de? Likaså kan geografisk positionering vara viktig för det fall det finns risk för ett attentat mot en viss person eller plats. Det kan också gälla möten. Men även ”radiotystnad” kan vara en indikation på att viktiga möten ägt rum. Inför förestående attentat kan också vissa viktiga samtal förekomma, exempelvis till närstående personer.

Integritetsintrånget

Integritetsintrånget avser brukaren av telefonen och de personer som har kontakt med den telefonen. Eftersom IHL avser enbart trafikdata och geografisk positionering är integritetsintrånget mindre än vid telefonavlyssning.

De undersökta ärendena avser nästan undantagslöst mobiltelefoner. Jämfört med om IHL hade avsett fasta telefoner är integritetsintrånget mindre eftersom mobiltelefoner är personliga på ett annat sätt än en fast telefon i ett hushåll eller i en lokal med flera användare. Följaktligen är det i regel trafikdata från den aktuella personens samtal som hämtas in och ingen annans.

I ett ärende visade det sig att en mobiltelefon brukades av en annan person, för övrigt en person som förekommer i ett eget ärende. Trafikdata från den telefonen gallrades ur analysen. Tidigare har också getts ett exempel på att trafikdata från en annan person hade förstörts.

En problematik av integritetskaraktär är dock att man inte kan veta vad de kartlagda samtalen handlar om. Under Säkerhetspolisens lupp hamnar därför rimligtvis ett stort antal samtal som inte alls har att göra med brott. Fördelen med exempelvis telefonavlyssning – som formellt sett anses väsentligt mer integritetskänsligt än trafikdata – är att det går att bedöma innehållet i samtalen. Därför går det att påstå att IHL till mindre del är integritetskänsligt gentemot abonnenten, men kan vara känsligare för utomstående som råkat ha en telefonkontakt med den aktuella personen.

En intervjuad handläggare förklarar: ”Det är mycket spekulation i telefonlistor. Det kan vara skumma personer, men också oskyldiga samtal. Det kan bli för mycket hypoteser – det är integritetskänsligt.”

En annan intervjuperson nyanserar bilden av frågan om integritet hos kontakterna. Han menar att för många ärenden är inte alltid det enskilda samtalet avgörande utan snarare att skapa en profil för kontaktnätet. För vissa ärenden kan dock det enskilda samtalet vara utslagsgivande för analysen. Det gäller särskilt spionage, där en säkerhetsmetod är att inte ta kontakter som riskerar att fångas upp.

Integritetsaspekten är en fråga som de intervjuade handläggarna funderar över. Det är uppenbarligen en levande fråga, något som diskuteras. Många tycker dock att fysisk spaning egentligen är mer

integritetskänsligt än mängddata. Det kanske speglar dagens informationssamhälle där kommunikation blivit en så integrerad del av tillvaron att kartläggning ”in real life” uppfattas som mer känsligt.

Beslut om IHL ska rapporteras till Säkerhets- och integritetsskyddsnämnden. Denna rutin sker centralt.

Utländska tjänster

I ärendena som gäller terror (dock inte ensamagerande) och flyktingspionage spelar utländska säkerhets- och underrättelsetjänster en stor roll. Det gäller även utländsk signalspaning. Det är naturligtvis svårt för att inte säga omöjligt för en svensk myndighet som Säkerhetspolisen att i detalj kunna följa personers förehavanden och telekommunikation i exempelvis Syrien. Därför är Säkerhetspolisen i IHL-ärendena beroende av uppgifter om dels personer och deras historik, dels kontakter med kända nummer, vare sig det är till utpekade personer med koppling till terrorism eller till diktaturers säkerhets- och underrättelsetjänster.

Även för politisk extremism har utländska säkerhets- och underrättelsetjänster viss betydelse. Skälet är att gärningspersoner med en politisk agenda i viss mån verkar över nationsgränserna, särskilt gäller det ett grannland som Danmark.

Signalspaning

FRA:s signalspaning spelar en stor roll för att identifiera kontakter från Sverige till länder med terroraktiviteter och även till specifika nummer som kan härledas till personer med koppling till terrorism. Detsamma gäller flyktingspioners samtal till sina handledare vid utländska säkerhets- och underrättelsetjänster.

Andra källor

Säkerhetspolisen har egna informatörer som lämnar information. Tips kommer också utifrån och i åtminstone ett ärende var det en uppmärksam försäljare som uppmärksammade Säkerhetspolisen på

en person som bedömdes vara ensamagerande. Migrationsverket är också en kanal för terrorärendena.

Internet är också en informationskälla och flera undersökta ärenden har kopplingar till Facebook och Flashback, exempelvis genom att personer poserat med vapen eller ställt egendomliga frågor som tyder på någon slags attentatsplanering. För flyktingspioner är sociala medier också ett sätt att bygga upp en bild av sig själva som oppositionella regimkritiker.

Viktigt med egen inhämtning för att dölja källor

En metod som Säkerhetspolisen har för att förebygga brott är att hålla samtal med personer där det finns indikationer på att de bedriver flyktingspionage eller som anslutit sig till våldsbejakande extremism och är på väg till en krigszon för att ansluta sig till stridande förband. Samtal kan också hållas med politiska extremister.

Erfarenheten är att uppgifter från IHL fungerar bra i dessa samtal eftersom uppgifterna ger tydliga besked om vilka kontakter personen har och följaktligen också vilken information Säkerhetspolisen besitter. Även geografisk information kan vara övertygande uppgifter. Däremot är det givetvis inte möjligt att referera till källor i personens egen miljö eller till uppgifter från utländska tjänster eller från signalspaning. Mot den bakgrunden fungerar IHL som Säkerhetspolisens på egen hand framtagen objektiv och samtidigt mindre känslig information.

Hög kvalitet på underlaget

Genomgående är underlaget till IHL-besluten av hög kvalitet. För de omständigheter som åberopas som stöd för att sätta in IHL refereras alltid till bakomliggande källor som är registrerade i centralregistret (diarienummer). Promemoriorna får därför nästan en vetenskaplig prägel. ”Skälet till att man är så noggrann är för framtiden”, förklarar en handläggare, och fortsätter: ”Det gäller spårbarheten, om personen blir aktuell igen. Det ökar också rättssäkerheten.” Även om en person avförs som ointressant för tillfället, är sannolikheten stor att han eller hon återkommer i något nytt ärende eller sammanhang. Då är det bra att det finns en PM.”

Referenserna till centralregistret gör att spårbarheten blir hög. Ansvariga chefer kan kontrollera källorna och själva göra en bedömning, vilket dock är mycket ovanligt enligt en intervjuad chef, ”vi litar på våra handläggare”. Det finns också kontrollstationer på vägen. Det främsta skälet är i stället att det går att senare förstärka värdet av vissa källor eller att tvärtom omvärdera dem. Återigen är det många personer i de undersökta IHL-ärendena som följs upp ytterligare eller på annat sätt kommer tillbaka.

Eftersom handläggarna inte alltid följer sina ärenden utan byter arbetsuppgifter i kombination med att gamla promemorior kommer att grävas fram av andra handläggare och ansvariga, blir promemoriorna viktiga för den enskilde handläggaren. Den bedömning som tidigare gjorts i en promemoria lever på det sättet vidare och påverkar givetvis uppfattningen om en handläggares analysförmåga. Handläggarna lägger helt enkelt ner ett stort arbete med att formulera sig i promemoriorna. Det är ytterligare en förklaring till den höga kvaliteten.

Ett skäl är också att handläggningen stramats upp, enligt flera intervjuade handläggare. En intervjuperson berättar att när han började vid Säkerhetspolisen för tio år sedan så var kvaliteten på en del underlag diskutabla. Bland annat saknades referenser till centralregistret för olika fakta och påståenden. Då fanns en risk för att ”sanningar etablerades”, med svagt stöd i det bakomliggande materialet. Inte minst transparansen genom referenser har ökat kvaliteten, menar han.

Promemoriorna påminner om varandra i struktur och det är tydligt att det finns goda förlagor som handläggarna lutar sig mot när de författar egna alster. En intervjuperson förklarar att promemoriorna medvetet hålls korta och koncisa.

Paradoxalt nog beror den höga kvaliteten på promemoriorna också på att Säkerhetspolisen självt fattar beslut om inhämtning. Det bekräftas också av intervjuerna. Informationen i promemoriorna hålls inom en snäv krets och därför vågar handläggarna vara öppna och referera till källor. Eftersom det handlar om underrättelsestadiet är de källor som ligger till grund för besluten mycket känsliga: Utbyte av information med utländska säkerhets- och underrättelsetjänster bygger på förtroende och att inga uppgifter lämnar huset. Personer kan utsättas för livsfara vid blotta antydan om att det i vissa miljöer finns en av Säkerhetspolisens informa-

törer. Svensk och utländsk signalspaning är kringgärdat av särskilt hög sekretess.

Frågan är hur promemoriorna skulle se ut om de vore avsedda för andra än Säkerhetspolisens personal – exempelvis i samband med någon form av externt beslutsförfarande. Sannolikt skulle spårbarheten i uppgifterna bli sämre och uppgifterna bli mer allmänt hållna till följd av uppgifternas känsliga natur.

IHL viktigt för att få resurser till ”egna” ärenden

För handläggarna innebär IHL att de får en trovärdig källa. Det hjälper dem att strukturera tankegångar och hypoteser. Samtidigt är det ett stöd när de lyfter ett ärende uppåt, när prioriteringar diskuteras. Intrycket är att åtskilliga handläggare för en hård kamp för att deras ärenden eller i vissa fall områden ska prioriteras. ”Som handläggare får man mer kött på benen och blir mer trovärdig.” Det kan vara ett utslag av att det finns en konkurrens om resurserna. Samtidigt ger de intervjuade handläggarna prov på ett stort engagemang och därför är det inte förvånande att de vill mer än vad de kan få.

Ett ärende som kan diskuteras

Det finns ett ärende som möjligen kan diskuteras enligt den bedömning som kan göras efter genomgången. Det gällde spionage där handläggaren på eget initiativ berättade att Säkerhetspolisen hade haft en väl extensiv tolkning av rekvisitet rikets säkerhet. Det hade konstaterats när åklagare senare hade konsulterats. Det bör dock tilläggas att ärendet gällde mycket känslig information som i förlängningen riskerade att innebära ett mycket allvarligt säkerhetshot. Problemet var dock att resonemanget byggde på en alltför lång händelsekedja för att den i juridisk mening skulle falla under rekvisitet rikets säkerhet.

Förmåga och avsikt

Som framgått är den svåra ekvationen att rätt värdera de båda avgörande komponenterna förmåga och avsikt. Personer kan ha förmåga, men ingen avsikt att exempelvis begå terrorbrott, vilket verkar vara ett rimligt antagande för den stora majoriteten hemvändande Syrienresenärer. På andra sidan kan det finnas extrema personer där knappast avsikten saknas, men väl en realistisk förmåga att sätta planer eller fantasier i verket.

En uppfattning som kom fram i någon intervju var att för användning av IHL borde en större betoning kunna göras av förmågan. Ett exempel kunde vara vit makt-miljön där man många gånger nöjer sig med vapenanskaffning, vapenträning och liknande förberedelser. De har inte målet att göra något i närtid utan de förbereder en revolution. Avsikten skulle därför vara diskutabel. ”Men minsta försök kommer att ställa till det”, resonerar en handläggare mot bakgrund av den kapacitet vit makt-miljön besitter. Ett sätt att se på det är att förekomsten av automatvapen och sprängmedel i extremistkretsar indikerar en avsikt och därför sammantaget utgör ett tillräckligt stort hot för att sätta in IHL. I bakgrunden ligger erfarenheten att de inblandade personerna är oberäkneliga. Därför utgör enbart tillgången på automatvapen och sprängmedel en uttalad risk.

En annan intervjuperson betonar att en hög förmåga kan vara en indikation på att det också finns en avsikt. Förmåga och avsikt är därför inte av varandra oberoende faktorer. Ett exempel är Syrienresenärer som ingår i ett sammanhang där terrorattentat utanför konfliktområdet är en realitet. Redan av det skälet kan en viss avsikt anses föreligga. Säkerhetspolisen använder sig av modeller för att kunna värdera de båda komponenterna förmåga och avsikt.

9.2.2.8 Nyttan

Integrerat uppföljningsverktyg

Som framgått är de personer som varit föremål för IHL i regel redan kända och följs upp av Säkerhetspolisen. Enbart ett mindre antal är ”nya” i betydelsen att uppföljningen varit förhållandevis kort innan IHL sattes in. Säkerhetspolisen har en rad korgar för inhämtning: utländska samverkande tjänster, svensk och utländsk

signalspaning, egna informatörer, information från samverkande myndigheter, det egna centralarkivet och andra registeruppgifter (till exempel belastningsuppgifter) samt öppna källor på bland annat internet. I de undersökta ärendena sätts IHL typiskt in när Säkerhetspolisen fått in uppgifter som tyder på brottslig aktivitet. Om så visar sig vara fallet, kan nivån på inhämtning eller andra åtgärder höjas ytterligare. I annat fall kan en återgång ske till den uppföljningsnivå som gällde före IHL. På det sättet kan IHL beskrivas som en integrerad del av Säkerhetspolisens löpande uppföljning.

Ett tydligt tecken på hur IHL ingår som en integrerad del av den löpande uppföljningen är den höga träffsäkerheten. I 40 procent av ärendena kunde uppföljningen gå ner till samma nivå som före användning av IHL och i 52 procent fortsatte uppföljningen också, men på en högre nivå än före IHL.

Dessutom underlättas fysiskt spaning av IHL genom att ett mönster framträder om var personen brukar befinna sig vid vissa tidpunkter. Vissa personer skulle det vara svårt att spana på utan tillgång till mängddata.

Vilja och förmåga

Säkerhetspolisens dilemma är att förebygga att allvarliga brott inträffar. Särskilt aktuellt i dessa tider är terrorrelaterade brott som kan leda till både omfattande skador på person och egendom, men också samhälleliga skador vars konsekvenser är svåra att överblicka. Problemet är att bedöma en persons eller grupp personers vilja och avsikt att begå brott, faktorer som måste sammanfalla, dessutom med viss styrka. IHL är ett viktigt hjälpmedel för att göra den bedömningen genom att mängddata beskriver kontakter, kontaktmönster och rörelsemönster. Genom Säkerhetspolisens uppföljning finns en kunskap om kontakters förmåga och avsikt. Kontaktmönster utvisar en persons beteende. Rörelsemönster i kombination med andra uppgifter om viktiga möten eller liknande berättar också om vad som kan vara på gång. På det sättet har IHL en funktion för att bedöma förmåga och avsikt.

Resurseffektiv inhämtning

Det är åtskilliga personer som Säkerhetspolisen följer upp, och resurserna är långt ifrån tillräckliga att ha dessa personer under observation genom fysisk spaning eller telefonavlyssning. Även om en stor andel av dessa personer inte kommer att begå exempelvis terrorbrott, gäller det för Säkerhetspolisen att förhindra de mycket få fall som ändå kan aktualiseras. IHL framstår därför som en resurssnål möjlighet att få en djupare uppföljning för den trots allt stora grupp för vilken indikationer på brott ändå förekommer. Utan IHL skulle Säkerhetspolisen tvingas reducera uppföljningen till ett väsentligt lägre antal personer för vilka det finns spanings- och avlyssningsresurser. Risken är påtaglig att vissa personer kommer att falla igenom och att allvarliga brott inte kan förebyggas. Slutsatsen är därför att utan den enkla fördjupade uppföljning som IHL innebär, sannolikheten ökar för att Säkerhetspolisen ska göra felprioriteringar med de följder som det kan innebära.

Pusslet utvidgas

Nyttan med IHL tar inte sikte på enbart den person som följs upp utan kan också generera ytterligare personer, eller kopplingar mellan personer, som Säkerhetspolisen inte känner till eller där tidigare information varit för svag för annan inhämtning än anteckning i centralregistret. Mot bakgrund av att åtskilliga av de aktuella miljöerna är dynamiska, ibland till och med turbulenta, som den nu pågående vågen av Syrienresenärer, ska inte denna bonusaspekt underskattas. Det är en väl etablerad erfarenhet att ärenden föder nya ärenden eftersom det i bakgrunden finns en rad nätverk som genom olika personer knyts samman.

Ensamagerande och personer utanför kända miljöer

De undersökta ärendena och intervjuerna kommunicerar att Säkerhetspolisen har en förhållandevis god inblick i de miljöer där de för IHL aktuella brotten planeras och utförs, vare sig det gäller terrorism, politisk extremism, spionage eller flyktingspionage. De riktigt vita fläckarna på kartan synes framför allt avse personer som dras till

terrorism utan att tillhöra kända lokala miljöer. Det gäller dels vissa Syrienresenärer som låter sig rekryteras på annat sätt än via tongivande personer i lokala miljöer, dels ensamagerande som till skillnad mot Syrienresenärerna inte går in i en gemenskap utan håller sig för sig själva. Bristen på sammanhang och miljö gör det svårt för att inte säga omöjligt för Säkerhetspolisen att få någon insyn genom informatörer. Av samma skäl kan fysisk spaning ge mycket lite information. IHL bedöms därför som en särskilt viktig inhämtningsmetod för de kontakter som ändå tas.

Effektivt underlag för förebyggande åtgärder

IHL är ett underrättelseverktyg, dessutom för en myndighet där en stor del av verksamheten går ut på att genom uppföljning förebygga brott. IHL har därför en större roll i den brottsförebyggande uppföljningen än att samla bevis för straffrättsliga åtgärder. En viktig förebyggande metod är att hålla samtal. Mängddata från IHL med dess precisa karaktär anses utgöra ett övertygande underlag för samtal. Av sekretess- och säkerhetsskäl har Säkerhetspolisen svårt att använda andra underlag vid samtal, som uppgifter från utländska tjänster eller egna informatörer.

9.2.3 Polismyndighetens och Tullverkets användning av inhämtningslagen

9.2.3.1 Undersökningen

Såvitt avser den öppna polisen och tullen har vi granskat ärenden där det första beslutet enligt inhämtningslagen fattades någon gång under perioden 31 mars 2013–1 april 2014, dvs. under ett år, dock inte sådana ärenden där underrättelsearbete fortfarande pågår. För Tullverkets del har samtliga avslutade ärenden under perioden granskats. När det gäller den öppna polisen har utredningen granskat de ärenden som handlagts av Rikskriminalpolisen (numera den Nationella Operativa Avdelningen) samt av de dåvarande Polismyndigheterna i Skåne, Västra Götaland och i Gävleborgs län.

Utredningen har gått igenom sammanlagt 59 ärenden vilka innefattar totalt 158 inhämtningsbeslut. Sammanlagt har 51 intervjuer

hållits. Vissa handläggare har intervjuats om mer än ett ärende. Intervjuerna har tagit mellan 10 och 30 minuter per ärende. Ett fåtal ärenden har dock varit svåra att följa upp eftersom handläggarna slutat eller varit tjänstlediga. Vidare har handläggaren i något fall haft så svaga minnesbilder av ärendet att det inte har bedömts meningsfullt att genomföra en intervju. Vissa ärenden har således endast undersökts översiktligt med hjälp av det skriftliga materialet. Det har i dessa fall varit svårt att följa hur ärendet har hanterats vidare efter att inhämtningslagen tillämpats. Detta innebär att det är svårt att dra några slutsatser om resultatet av tvångsmedelsanvändningen.

Vid undersökningen har det framgått tydligt att det inte finns några avgörande skillnader mellan hur Polismyndigheten respektive Tullverket arbetar med inhämtningslagen. Utredningen har därför valt att presentera resultatet av undersökningen samlat för dessa två myndigheter.

9.2.3.2 Några övergripande resultat

För den öppna polisens och Tullverkets del har i stort sett samtliga granskade ärenden avsett grovt narkotikabrott och/eller grov narkotikasmuggling. Endast en handfull (fem) ärenden har avsett annan brottslig verksamhet. I dessa fall har det varit fråga om bl.a. grov penningförfalskning, människorov och grovt rån.

I likhet med resultatet för Säkerhetspolisens har besluten i ärendena i allt väsentligt avsett inhämtning av uppgifter utifrån mobiltelefoners telefonnummer (153 beslut). Endast ett beslut har avsett en fast telefon. Beslut som gäller mobiltelefoners IMEI-nummer (tre beslut) och SIM-kortets IMSI-nummer (ett beslut) är ovanliga.

En stor majoritet av besluten har avsett historiska uppgifter om meddelanden enligt 1 § 1 inhämtningslagen (141 beslut). Det är också relativt vanligt (51 beslut) att besluten avser uppgifter om i vilket geografiskt område en telefon finns eller har funnits (1 § 3 inhämtningslagen). Beslut om s.k. basstationstömning (1 § 2) är mycket ovanliga (ett beslut).[1]

[1] Ett beslut kan avse flera punkter i paragrafen.

Den genomsnittliga tiden för beslut om inhämtning av uppgifter är kort, 128 beslut (81 %) avser en tidsperiod som är en månad eller kortare.

Det är inte ovanligt att ärendena hos den öppna polisen och Tullverket avser mer än en person. Totalt antal personer som omfattas av inhämtningsbesluten är 127.[2] I genomsnitt omfattar de granskade ärendena således 2,15 personer. Av de beslut där personens identitet framgår avser 92 beslut män (93 %) och sju beslut kvinnor (7 %).

Uppgifter om personernas födelseår förekommer i ärendena. Dessa uppgifter är dock så ofullständiga att det inte har bedömts meningsfullt att räkna ut ett genomsnitt.

Omfattningen av den öppna polisens tillämpning av inhämtningslagen varierar en del mellan olika delar av landet. Exempelvis har Polismyndigheten i Västra Götaland fattat endast en handfull beslut under den tidsperiod som utredningen har undersökt, medan Rikskriminalpolisen och Polismyndigheten i Skåne har fattat betydligt fler. Vad anledningen till dessa skillnader är har inte gått att fastställa utan kan vi bara spekulera om. En möjlig förklaring som framförts är att polisen i Västra Götaland inte har några särskilda resurser avsatta för analys av telefontrafik i underrättelseverksamheten. De resurser som finns delas mellan denna verksamhet och förundersökningsverksamheten. Det innebär att underrättelseverksamheten ofta får stå tillbaka för de analyser som behöver göras i förundersökningar. En annan förklaring är att det helt enkelt handlar om att polisen i Västra Götaland historiskt sett inte har haft för vana att arbeta med uppgifter om elektronisk kommunikation i underrättelseverksamheten utan först på förundersökningsstadiet. Ytterligare en teori som nämnts under våra samtal med handläggarna är att organisatoriska skäl skulle kunna vara en bidragande orsak till att så få beslut fattas. Förklaringen skulle i sådana fall kunna hänga ihop med att det inte finns någon som är riktigt bekväm med att fatta den aktuella typen av beslut.

[2] Skälet till att antalet beslut (158) är högre än antalet personer (127) är att i vissa ärenden har fler beslut fattats avseende samma person.

9.2.3.3 Indikationer på brottslig verksamhet

Den information som finns i ärendena innan myndigheterna fattar beslut om att hämta in uppgifter enligt inhämtningslagen utgörs oftast av uppgifter från källor, överskottsinformation från förundersökningar eller uppgifter från utländska myndigheter. Ofta är informationen om den misstänkta brottsliga verksamheten förhållandevis konkret. En typisk bakgrundsbeskrivning i ett ärende kan vara t.ex. att uppgifter finns om att en angiven person ägnar sig åt hantering av stora mängder narkotika av något visst slag, att narkotikan kommer från ett angivet land och att personen samarbetar med någon eller några angivna personer. En annan typ av uppgift som är vanligt förekommande är att den person som är aktuell är inblandad i smuggling av narkotika från något visst land och att personen av den anledningen gör resor till landet i fråga. I flera av de undersökta ärendena finns även uppgifter om de misstänkta personernas tillvägagångssätt i olika avseenden, exempelvis att narkotika smugglas in till Sverige genom att den släpps över räcket till Öresundsbron för att hämtas upp av kumpaner vid brofästet. Ett annat exempel på en sådan uppgift är att de misstänkta använder någon viss strategi för att dölja en smugglingsoperation, t.ex. att narkotika göms tillsammans med ett livsmedel som luktar starkt i syfte att förvilla narkotikahundar. Flera handläggare har berättat att myndigheterna hämtar in samtalslistor bara i sådana fall där det finns starka indikationer på att detta verkligen kan ge något. Det har inte kommit fram någonting under vår kartläggning som ger anledning att ifrågasätta det. Några handläggare har också gett uttryck för att det ofta inte räcker med information från en enda källa för att myndigheten ska göra bedömningen att ärendet är värt att satsa resurser på.

Det varierar något hur mycket information som finns sedan tidigare angående den eller de personer som ärendena gäller. En vanlig situation är att ett ärende avser en person som är känd av myndigheten sedan tidigare, t.ex. för att personen tidigare är dömd för liknande brottslighet eller på grund av att han eller hon har varit aktuell i samband med en tidigare förundersökning. Ofta finns det också uppgifter om att den person som är aktuell tillhör en viss gruppering som sysslar med grov organiserad brottslighet.

Det förekommer dock även att det inte finns någon tidigare kännedom om personen eller personerna. Ett exempel på en sådan situation är ett ärende där två postförsändelser innehållande narkotika hade tagits i beslag av utländsk tull. Försändelserna var adresserade till två personer på två olika adresser i Sverige. Båda dessa personer var tidigare okända för myndigheten. Uppgifter hämtades in med stöd av inhämtningslagen i syfte att undersöka om det gick att finna några samband mellan dessa personer.

I flera ärenden förekommer det också att utländska myndigheter lämnar information om att utländska kurirer är på väg till Sverige med narkotika. I dessa fall förekommer det att det saknas uppgift om personernas namn, men att informationen innehåller uppgifter om telefonnummer till personerna.

En annan vanlig situation är att uppgifter som hämtas in enligt inhämtningslagen avseende en viss person visar att denne har kontakter med någon annan person som bedöms vara intressant, och att myndigheterna därför undersöker även den senare. I dessa fall leder det ibland till att inhämtningslagen används även mot den senare personen. I ett ärende framgick det t.ex. av en samtalslista att en misstänkt person (X) hade flera kontakter med en annan person (Y). Denne Y var tidigare dömd för liknande brottslighet, och X hade förhörts i samband med det ärendet. Det förhållandet att X och Y nu hade kontakt med varandra bedömdes vara en stark indikation på att Y kunde vara inblandad i den brottsliga verksamhet som X misstänktes för. En samtalslista togs därför in även beträffande Y.

Det förekommer också att den information som ligger till grund för ett beslut enligt inhämtningslagen delvis kommer från fysisk spaning. I ett ärende hade Tullverket kontrollerat en fraktsändning som visade sig innehålla föremål som kan användas för framställning av narkotika. När fraktsändningen hämtades spanade myndigheten på den person som hämtade den. Spaningspersonalen kunde dock inte följa transporten ända fram till leveransadressen. Uppgifter hämtades då in enligt inhämtningslagen bl.a. i syfte att försöka fastställa den exakta adressen.

I ett annat ärende hade polisens spaningspersonal observerat att den person som myndigheten intresserade sig för hade träffat en annan person som var tidigare dömd för grovt narkotikabrott. Uppgifter hämtades in med stöd av inhämtningslagen, bl.a. för att

försöka kartlägga i vilken omfattning dessa personer hade kontakt med varandra.

9.2.3.4 Behov av information

I samtliga ärenden som utredningen har undersökt har myndigheterna haft ett behov av att kartlägga de personer som ingår i ärendet. Behovet av information har främst gällt personernas kontakter med andra kända kriminella, kontakter med personer som det finns underrättelseinformation om (t.ex. kontakter med utpekade medgärningsmän, kurirer och dylikt) samt personernas positioner och rörelsemönster. Ett mycket vanligt svar på frågan om varför myndigheten valde att använda inhämtningslagen är att uppgifterna används för att kontrollera olika uppgifter från källor, bl.a. för att på så sätt kunna bedöma hur tillförlitliga källuppgifterna är. Ett exempel på en sådan situation kan vara att källor lämnar uppgifter om att två utpekade personer samarbetar i en narkotikaaffär. Myndigheten kan då använda sig av inhämtningslagen för att ta reda på om det förekommer mycket kontakter mellan dessa personer, eller så kan positionsuppgifter användas för att fastställa att personerna har varit på samma plats vid samma tillfälle.

Ett annat exempel på informationsbehov är att myndigheten får uppgifter om att en person har ett narkotikalager, en narkotikaodling eller något liknande på en viss plats. I dessa fall är det av intresse att kontrollera om personen ofta uppehåller sig vid eller i närheten av den platsen. Till exempel fanns i ett ärende källuppgifter om att en person bedrev brottslig verksamhet i en lokal som var belägen någonstans inom ett hamnområde. Uppgifter hämtades in enligt inhämtningslagen för att kontrollera om uppgiften stämde och för att i så fall försöka ta reda på var inom det angivna området lokalen fanns.

Uppgifter om personernas kontakter och rörelsemönster läggs ofta till grund för den fortsatta hanteringen av ärendet. Till exempel kan uppgifter om telefonkontakter vara viktiga för s.k. inre spaning (dvs. sökningar på internet, slagningar i register etc.). En handläggare uttryckte saken så att ”Informationen från inhämtningslagen är som en strut som riktar in det fortsatta underrättelsearbetet”. Det är tydligt att myndigheterna prioriterar hårt hur

resurserna används, och att det i många fall är resurserna som sätter gränserna för vilka ärenden som myndigheterna arbetar vidare med. Uppgifter från inhämtningslagen blir då viktiga, dels för att bygga upp ett ärende med tillräcklig information för att det ska anses vara befogat att satsa resurser på att arbeta vidare med ärendet, dels för att en kartläggning av kontakter och framför allt rörelsemönster givetvis innebär att t.ex. spaningsresurser kan användas mer effektivt.

Det är också vanligt att myndigheterna använder uppgifter från samtalslistor för att identifiera okända personer. Till exempel hade polisen i ett ärende fått uppgifter om att en okänd person organiserade smuggling av kokain från ett visst land via Sverige till ett annat land. Polisen hämtade då in uppgifter enligt inhämtningslagen, vilka bidrog till att den okände personen kunde identifieras.

I ett annat ärende hade polisen mycket information från källor som tydde på att två personer stod i begrepp att göra en resa till ett angivet land för att organisera en smugglingsoperation från landet i fråga. Informationen innehöll ett namn på den ena personen, medan den andra personen endast var angiven med ett smeknamn/alias. Polisen hade dock misstankar om vem denne person var. Genom telefonlistor kunde polisen bekräfta att den namngivna personen hade telefonkontakt med den person som man misstänkte fanns bakom smeknamnet, och man kunde dessutom se att de träffades. På så sätt kunde polisen dra slutsatsen att de hade haft rätt i sina misstankar om vem personen med smeknamnet var.

Ytterligare ett exempel på en sådan situation är ett ärende där polisen hade fått information från källdrivning om att ett stort parti narkotika skulle transporteras till en viss ort i Sverige av en oidentifierad kurir. Samtalslistor avseende en misstänkt huvudman visade att denne hade gjort en resa till den aktuella orten vid den angivna leveranstidpunkten. Polisen lyckades senare identifiera en person vars signalement väl stämde in på den okände kuriren. Samtalslistor hämtades in för att kontrollera om den personen hade varit på den aktuella orten samtidigt som den misstänkte huvudmannen.

Inhämtningslagen kan också vara ett viktigt verktyg för att få information om vilka telefonnummer som de i ärendet aktuella personerna använder. Som exempel på det kan nämnas ett ärende där en samtalslista innehöll en uppgift om att den misstänkte personen hade haft kontakt med ett utländskt mobiltelefonnummer

vid ett enstaka tillfälle. Polisen misstänkte dock att personen hade haft fler kontakter med det aktuella numret, och att han hade ett annat telefonabonnemang som användes särskilt för dessa kontakter. Uppgifter begärdes då ut angående det utländska telefonnumret för att se om detta hade haft kontakt med något eller några andra svenska telefonnummer.

9.2.3.5 Säkerhetstänkande

Som nämnts varierar det en del hur mycket information myndigheterna har om de personer som ärendena avser i skedet innan inhämtningslagen används. I vissa ärenden har myndigheterna god kännedom om personerna och deras olika strategier för att dölja sin brottslighet och sin kommunikation, men det förekommer också att lagen används mot personer som myndigheten inte känner till sedan tidigare.

Eftersom inhämtningslagen inte ger tillgång till uppgifter om innehållet i kommunikationen har det, i de ärenden där myndigheten inte har haft någon tidigare kännedom om personerna, ofta varit svårt att dra några närmare slutsatser om personernas säkerhetstänkande. I vissa fall har det dock varit mycket tydligt att de aktuella personerna har haft som strategi att regelbundet byta telefonabonnemang i syfte att undvika avlyssning och övervakning. Det är också vanligt att de aktuella personerna har flera olika telefoner eller abonnemang. Det är tydligt att dessa personer räknar med att deras telefoner kan vara avlyssnade eller övervakade av myndigheterna.

I många av de granskade ärendena har myndigheterna tidigare haft kännedom om de aktuella personerna och även om deras förmåga att hemlighålla kommunikation. Hur hög denna förmåga bedömts vara varierar mellan ärendena. I några ärenden, t.ex. där avlyssning tidigare har använts mot personerna i samband med förundersökningar, har det framgått att personerna är relativt öppna i sin kommunikation. I ett ärende uttryckte t.ex. en handläggare att ”de talade mycket öppet på telefon om vad som var på gång”. En annan handläggare uttryckte att ”Det finns en mängd olika sätt att försvåra för polisen. Ofta är dock de kriminella inte så smarta, utan de använder sina mobiler.”

Det vanligaste är dock att personerna är försiktiga. Som en handläggare uttryckte det: ”I samband med narkotikaaffärer finns alltid ett mått av försiktighet och ett speciellt beteende. De som sysslar med sådan brottslighet är generellt försiktiga och använder sig ofta av nya kontantkort. Det telefonnummer som var aktuellt i ärendet var t.ex. nytt”.

I vissa fall har personerna bedömts vara väldigt försiktiga. Ett exempel är ett ärende där polisen hade arbetat med en misstänkt person under flera år utan att komma någon vart. I ett annat ärende gjorde tips och information från en tidigare utredning att polisen bedömde att personen var ”noggrann och mycket försiktig i sin roll vad gäller narkotikahanteringen”. Personen använde sig av flera olika mobiltelefoner; i princip en telefon för varje person han hade kontakt med. Dessa byttes dessutom regelbundet ut. Personen ansågs också vara ”ytterst sparsam” med information under telefonsamtal. Han använde sig i stället av krypterad trafik och av kurirer som lämnade meddelanden muntligt.

Säkerhetstänkandet kan också variera beroende på vilken kriminell gruppering personen eller personerna bedöms tillhöra. En handläggare uttryckte t.ex. att ”Medlemmarna i (en viss gruppering) är de svåraste att arbeta med. De är mycket skolade i polisens arbetsmetoder. De pratar aldrig om brott på telefon, och polisen får därför aldrig särskilt mycket information genom telefonavlyssning. De håller i stället många möten ute i terrängen och de använder krypteringsverktyg”.

9.2.3.6 Omständigheter som gjorde att inhämtningslagen användes

Som redan framhållits är ett vanligt skäl till att inhämtningslagen används att myndigheterna har ett behov av att så långt som möjligt kontrollera och verifiera tillförlitligheten av olika typer av underrättelseinformation, exempelvis information från källor. Om sådana uppgifter t.ex. anger att två personer har kontakt med varandra, är inhämtningslagen ett effektivt verktyg för att kontrollera om informationen stämmer. En handläggare uttryckte det på så sätt att ”inhämtningslagen är det arbetsverktyg som finns för att kunna bedöma och verifiera den information som polisen har”. Det är

således mycket vanligt att det är den information som finns tillgänglig i ärendet som styr uppgiftsinhämtningen enligt lagen.

Vidare är det inte ovanligt att telefonlistor hämtas in i anslutning till någon särskild händelse. Ett exempel på det är ett ärende där en svensk medborgare greps utomlands med en stor mängd narkotika i en väska. Det framgick att personen sannolikt var på väg till Sverige och polisen drog slutsatsen att han knappast agerade ensam. Polisen kände dock inte till några ytterligare misstänkta i Sverige. Det var då av särskilt intresse att undersöka vilka som eventuellt hade försökt kontakta personen i samband med resan och i tiden kring gripandet. I ett annat ärende hade försändelser med narkotika som var adresserade till Sverige tagits i beslag av utländsk tull. I ärendet valdes en tidsperiod i anslutning till att försändelserna skickades och beslagtogs. Handläggaren uttryckte det så att ”när en planerad leverans av narkotika inte kommer som den ska så börjar det ofta hända saker”.

Om myndigheterna har fått information om att en misstänkt person ska göra en resa till ett visst land vid någon viss tidpunkt, så är det vanligt att telefonlistor hämtas in för en period som täcker den tidpunkt då resan ska äga rum.

Det förekommer också i en del ärenden att den tidsperiod som ett beslut avser inte är knuten till någon specifik information eller någon särskild händelse. Ett vanligt svar på frågan om vilka omständigheter som gjorde att inhämtningslagen användes är att det bedömdes nödvändigt att kartlägga kontakter och rörelsemönster för att över huvud taget komma vidare med ärendet. Så kan t.ex. vara fallet när myndigheterna inte känner till identiteten på den person som man intresserar sig för, och uppgiften om telefonnummer kan då vara den enda ledtråd som finns tillgänglig. Ett exempel på det är ett ärende där polisen hade fått information från en utländsk myndighet om att några utländska medborgare stod i begrepp att smuggla stora mängder narkotika till Sverige. Dessa personers identiteter var inte kända. Däremot innehöll informationen ett telefonnummer till en av dem. Inhämtningslagen användes då i syfte att försöka ta reda på vilka personerna var för att på så sätt komma vidare med ärendet.

9.2.3.7 Information

Den information myndigheterna räknar med eller hoppas på att få genom tillämpningen av inhämtningslagen svarar givetvis mot det behov av information som finns i ärendet. Det vanligaste svaret från handläggarna är att myndigheten hoppades på att få in uppgifter som bidrar till att kartlägga den aktuella personens kontakter och rörelsemönster. Syftet med det är ofta att kontrollera och verifiera sådan underrättelseinformation som myndigheten har, vilket sedan ligger till grund för den fortsatta hanteringen av ärendet. Uppgifter om kontakter med andra kända kriminella är av stort intresse. Detsamma gäller uppgifter om resor.

I många ärenden har det också funnits ett behov av att identifiera den person som använder en viss telefon, och myndigheten har då hoppats på att med hjälp av samtalslistor få tillgång till information som kan bidra till detta. Som exempel kan nämnas ett ärende där myndigheten räknade med att få information om vilka kontakter som telefonerna hade haft för att kunna utreda vilka personer som använde telefonerna samt kartlägga och dra slutsatser om deras kontaktnät. I ärendet hade en misstänkt kurir gripits utomlands. Det bedömdes extra intressant att få in uppgifter i anslutning till dennes resa till landet. De frågor man ställde sig var bl.a. ”Vem var den sista person han ringde innan han klev på planet?”, ”Vem var den första person han ringde när han kom fram?” och ”Vilka har han haft kontakt med i samband med möten?”.

En annan vanlig situation är att myndigheten har en förhoppning om att information om en persons rörelser kan bidra till att hitta någon viss plats, t.ex. platsen för en narkotikagömma. Ett exempel på det är ett ärende där det fanns information från källdrivning som angav att en person bedrev brottslig verksamhet i en lokal som skulle vara belägen någonstans inom ett visst område. Polisen hoppades då på att genom tillämpning av inhämtningslagen få uppgifter som kunde bidra till att hitta lokalen. I ett annat ärende hade myndigheten tips från källor om att en angiven person hade en narkotikaodling på en okänd plats. Inhämtningslagen användes bl.a. i syfte att försöka hitta odlingen.

Ett påfallande vanligt svar på frågan om vilken information myndigheten faktiskt fick in genom tillämpningen av inhämtningslagen är att de uppgifter man fick motsvarade förväntningarna, dvs.

myndigheten fick den information som man hoppades på. Det är alltså vanligt att de uppgifter som hämtas in bidrar till att personernas kontakter och rörelsemönster kan kartläggas, eller till att ge ledning i fråga om vem som använder en viss telefon. Ett exempel på det är ett ärende där polisen räknade med att få in uppgifter om var telefoner hade varit uppkopplade för att ta reda på var personerna fanns. Man räknade också med att kunna ta reda på vilka kontakter som telefonerna hade haft för att på så sätt kunna få fram vilka personer som använde telefonerna. Enligt handläggaren blev resultatet av inhämtningen sammantaget att polisen kunde dra slutsatser om vilka som använde telefonerna, vilket nätverk de tillhörde och vilken kriminalitet de sysslade med.

I ett annat ärende hoppades polisen på att genom samtalslistan få träff mot tillgänglig information, att kunna identifiera brukaren av telefonen och att kartlägga dennes kontakter. Handläggaren beskrev resultatet i ärendet som optimalt. Polisen fick genom samtalslistan träff mot färsk underrättelseinformation som angav att en namngiven person skulle genomföra en smugglingsoperation. Man kunde också se att den aktuella personen hade haft kontakt med ett telefonnummer från ett visst land vilket bedömdes som intressant. Tack vare telefonlistorna kunde det vidare klarläggas att telefonen hade kopplat upp på en viss plats där den namngivne personens syster bodde. Detta ledde till att identiteten på brukaren av telefonen kunde fastställas.

Ett annat exempel på ett lyckat resultat är det ovan nämnda ärendet där en kurir hade gripits utomlands. I ärendet lyckades polisen genom samtalslistorna fastställa identiteten på personer som hade haft kontakt med kuriren. Telefonlistorna bekräftade också att dessa personer fungerade som koordinatorer mellan kuriren och nätverket i Sverige. Polisen fick därigenom en bild av nätverket.

I ett annat ärende innebar uppgifterna från inhämtningen att polisen tydligt kunde se att källuppgifter om att två personer hade kontakt med varandra stämde. Vidare innebar uppgifterna att källinformation om att dessa personer skulle göra en resa tillsammans kunde verifieras.

Det förekommer givetvis också att myndigheterna inte hittar något intressant i de uppgifter som hämtas in. I sammanlagt fyra av de ärenden där intervjuer har hållits har handläggarna svarat att telefonlistorna inte gav några uppgifter alls av intresse. I ett ärende

hade man t.ex. räknat med att få uppgifter om kontakter med kriminella personer och om rörelsemönster för att kartlägga ett nätverk. Den inhämtade listan innehöll dock inte några kontakter som bedömdes vara intressanta. I något enstaka fall har det också kommit fram att den inhämtade listan inte innehöll några uppgifter alls eftersom den aktuella personen hade slutat använda det abonnemang som inhämtningsbeslutet avsåg. I övriga ärenden där intervjuer har hållits har det kommit fram att informationen från tillämpningen av inhämtningslagen i olika hög grad har bidragit till att föra ärendet framåt.

9.2.3.8 Resultat och nytta

Målet för den öppna polisens och Tullverkets underrättelseoperationer är att bygga upp ärendena på ett sådant sätt att det finns förutsättningar för att en förundersökning ska kunna inledas. Förhoppningen är att denna sedan ska leda vidare till åtal och fällande dom. I ett förhållandevis stort antal, knappt hälften, av de ärenden där intervjuer har hållits har också förundersökning kunnat inledas. Vidare har resultatet av två av de granskade ärendena delgetts utländska myndigheter varpå förundersökningar har inletts utomlands.

För att kunna analysera nyttan av inhämtningslagen är det emellertid inte tillräckligt att konstatera att tillämpningen av lagen har lett vidare till förundersökning i något visst antal eller någon viss andel fall. Det har inte heller i något av de granskade ärendena varit möjligt att med säkerhet slå fast att det var just den information som hämtades in med stöd av inhämtningslagen som ensamt ledde till detta resultat. Detta beror på att det i allmänhet inte är möjligt att bedöma resultatet av uppgiftsinhämtning enligt inhämtningslagen isolerat från de övriga informationskällor som de brottsbekämpande myndigheterna använder sig av. Tvärtom är det tydligt att myndigheternas underrättelseverksamhet är beroende av flera olika underrättelsekällor vilka samverkar med varandra och därigenom bidrar till att skapa en så bra bild som möjligt av den verksamhet som misstänks. Det står genom kartläggningen klart att uppgifter från inhämtningen utgör en viktig bit i det pusslet tillsammans med uppgifter från t.ex. källdrivning och fysisk spaning.

Att bedöma nyttan av uppgiftsinhämtningen enligt lagen baserat enbart på andelen ärenden som har lett vidare till förundersökning skulle också bli missvisande av andra skäl. Det förhållandet att förundersökning inte har inletts behöver givetvis inte bero på att uppgifter som hämtats in enligt inhämtningslagen inte har varit till nytta, utan kan bero på annat. Till exempel är det i vissa fall tydligt att uppgifterna från samtalslistor har bidragit med relevant information – och därigenom har varit till nytta – men att myndigheten trots detta av olika skäl inte har nått ”hela vägen fram”. Ett annat exempel, som dessutom är ganska vanligt förekommande, är att myndigheten på grund av begränsade resurser helt enkelt har valt att prioritera ned ärendet till förmån för andra ärenden. I flera av de granskade ärenden som inte har lett till förundersökning har det kommit fram att handläggaren har bedömt att det funnits förutsättningar för att arbeta vidare med ärendet, men att så inte har blivit fallet eftersom myndigheten har valt att prioritera andra ärenden. Det är mycket tydligt att resurserna har avgörande betydelse för vilka ärenden myndigheterna arbetar med, och flera av handläggarna har beskrivit att de får kämpa för få resurser till ”sina” ärenden.

Det är mot den angivna bakgrunden lämpligare att föra nytto-resonemangen utifrån den information som söks respektive erhålls genom tillämpningen av inhämtningslagen och om denna information bidrar till att föra ärendet framåt. I den mån så är fallet finns det grund för att påstå att användningen av lagen har varit till nytta i ärendet.

Som framgår av föregående avsnitt är det endast i ett fåtal av de granskade ärendena som uppgifterna från tillämpningen av lagen inte alls har bidragit till att föra ärendet framåt. I många av de granskade ärendena är det tvärtom tydligt att uppgifterna från inhämtningslagen har varit till stor nytta. I regel handlar det då om att uppgifterna har inneburit att de inblandade personernas kontaktnät och rörelsemönster har kunnat kartläggas samt att okända personer har identifierats. Denna information kan sedan användas på olika sätt, bl.a. för att bedöma tillförlitligheten i tips från källor och som grund för att spana fysiskt på personer som misstänks vara inblandade. Ett konkret exempel på detta är ett ärende där uppgifter från samtalslistor användes för att kartlägga kontakter, resor och rörelsemönster i övrigt. Informationen användes därefter

som grund för fysisk spaning. Detta ledde sedan vidare till att förundersökning kunde inledas och till att ett tillslag kunde göras. Mycket stora mängder av ett narkotiskt preparat togs i beslag, och de inblandade dömdes till långa fängelsestraff.

Flera exempel på fall där nyttan av uppgifterna från inhämtningslagen framgår tydligt kan nämnas. I ett ärende fanns det information från en utländsk polismyndighet om att en okänd person med ett visst telefonnummer skulle smuggla en viss sorts narkotika från ett land via Sverige och därefter vidare till ett annat land. Inhämtningslagen användes i ärendet bl.a. för att identifiera den okända personen. Enligt handläggaren var telefonnumret den enda ingång polisen hade, och utan möjlighet att analysera trafik till och från numret hade det inte varit möjligt att komma vidare med ärendet och ta reda på vem som använde numret. Underrättelseärendet ledde sedan till förundersökningar både i Sverige och utomlands vilka ledde vidare till åtal och fällande domar.

Ett annat exempel är det ärende som nämnts ovan där det fanns uppgifter om att brottslig verksamhet bedrevs i en lokal inom ett visst område. Resultatet av ärendet beskrevs av handläggaren som mycket lyckat. Uppgifterna som hämtades in med stöd av inhämtningslagen bidrog till att kartlägga kontakter och positioner. Förundersökning inleddes och den aktuella lokalen hittades, varpå polisen kunde göra tillslag. Även detta ärende ledde vidare till åtal och fällande domar.

I ett ärende hade Tullverket fått uppgifter om att ett internationellt nätverk sysslade med organiserad smuggling av narkotika till Sverige, och att dessa personer hade kopplingar till personer som en utländsk myndighet misstänkte för internationell drog-handel. Samtalslistor som togs in i ärendet gav information om personernas resemönster och kontakter vilket bl.a. gjorde att Tullverket fick fram kopplingar till en misstänkt huvudman och fick belägg för vissa uppgifter om resor. Underrättelseärendet ledde till att förundersökning inleddes och att ett beslag av narkotika kunde göras. Enligt handläggaren var uppgifterna från inhämtningslagen till stor nytta. Utan samtalslistorna hade ärendet enligt hans uppfattning förmodligen lagts ned ganska snabbt.

I ett annat ärende misstänkte Tullverket att en person bedrev storskalig smuggling av ett narkotiskt preparat från ett visst land till Sverige. Samtalslistor hämtades därför in i syfte att kartlägga

personens resemönster. Med ledning av listorna kunde Tullverket dra slutsatser bl.a. i fråga om när personen skulle göra nästa resa till det aktuella landet. Personen påträffades sedan med narkotika, dock inte sådana mängder som förväntat. Handläggaren uttryckte det så att ”I det här ärendet fungerade inhämtningslagen som den ska”.

En annan nyttoeffekt av inhämtningslagen är att den kan användas för att avföra personer från misstankar. Detta för med sig positiva effekter, både genom att den person det gäller slipper bli föremål för ytterligare intresse från myndigheternas sida och genom att myndigheternas resurser kan användas mer effektivt. Ett exempel på det är ett ärende där polisen hade källinformation om att en person (X) sysslade med narkotikahantering. Genom en samtalslista fick polisen klart för sig att X hade kontakt med en annan person (Y) som tidigare dömts för liknande brottslighet i ett ärende där även X var misstänkt. Uppgifterna gjorde att polisen började intressera sig även för Y och en samtalslista togs in avseende Y:s telefon. Av listan kunde polisen emellertid dra slutsatsen att Y sannolikt hade flyttat till en annan ort, och han avfördes därför.

I flera ärenden har uppgifterna från tillämpningen av inhämtningslagen bedömts medföra nytta, men utan att ärendet har lett hela vägen till förundersökning. Ett exempel på det är ett ärende där Tullverket hade information om att en kriminell organisation regelbundet tog in stora mängder narkotika från ett visst land. Enligt informationen organiserades smugglingen av en till namnet okänd person med en viss nationalitet, bosatt på en viss ort. En annan person vars identitet var känd skulle enligt informationen vara delaktig i hanteringen. Tullverket hämtade in en telefonlista avseende den identifierade personen i syfte att se vilka kontakter han hade och om möjligt identifiera även den okända personen. Listan bekräftade att han hade haft kontakter med det land som narkotikan angavs komma ifrån. Däremot lyckades Tullverket inte ta reda på vem den okända personen var. Bedömningen gjordes att det inte fanns tillräcklig grund för att inleda förundersökning, och underrättelseärendet lades ned.

Ett annat exempel är ett ärende där polisen hade information från en utländsk myndighet om att ett nätverk stod i begrepp att starta smuggling av en viss sorts narkotika till Sverige. Av informationen framgick dock inte identiteten på de inblandade personerna. Däremot fanns en uppgift om svenska telefonnummer. Polisen

använde sig av inhämtningslagen för att få in uppgifter om var telefoner hade varit uppkopplade för att ta reda på var de inblandade personerna fanns samt för att se vilka kontakter telefonerna hade haft för att på så sätt kunna få fram vilka personer som använde telefonerna. Handläggaren beskrev underrättelsevärdet av de uppgifter man fick genom tillämpningen av inhämtningslagen som stort. Polisen fick flera viktiga pusselbitar som ”gav en grund att stå på”. Resultatet av underrättelseärendet blev att informationen sammanställdes och att nätverket därmed kunde kartläggas. Detta räckte dock inte hela vägen till förundersökning.

Det förekommer också i några ärenden att den brottsbekämpande myndigheten har kommit en bit på vägen med underrättelsearbetet när någonting inträffar som gör att myndigheten inte kan gå vidare med ärendet. Det kan t.ex. handla om att en narkotikaleverans som myndigheten avser att arbeta mot tas i beslag av utländsk tull eller att den person som ärendet avser grips för något annat brott. Som exempel kan nämnas ett ärende där polisen hade fått källinformation om att en person distribuerade stora mängder narkotika och narkotikaklassade tabletter. Polisen hämtade in telefonlistor avseende personen i syfte att få uppgifter om hans kontakter och rörelsemönster. Detta ledde enligt handläggaren till nytta på så sätt att personens nätverk kunde kartläggas. Innan polisen hade kommit så långt med underrättelseoperationen avseende den misstänkta narkotikabrottsligheten så greps och dömdes emellertid personen för ett annat allvarligt brott.

Även om ett underrättelseärende inte leder till förundersökning kan resultatet av ärendet vara till nytta på så sätt att det bidrar till att öka myndigheternas kunskap inför framtida ärenden. Ett exempel på det är ett ärende som polisen drev parallellt med en förundersökning om grov narkotikasmuggling. Underrättelseärendet bedrevs – i tät kontakt med åklagaren i förundersökningsärendet – mot sådana personer som inte var misstänkta i förundersökningen. Syftet med underrättelseoperationen var att undersöka om de aktuella personerna sysslade med narkotikasmuggling och om detta i så fall kunde sättas samman med den pågående förundersökningen. Telefonlistorna ledde till att viss fysisk spaning kunde genomföras, men det framkom inte att någon av personerna hade något samband med den pågående förundersökningen. Senare fick myndigheten information om att en annan polismyndighet över-

vägde att inleda förundersökning mot en av de grupperingar som hade varit aktuella i underrättelseärendet. Viss information som kommit fram i ärendet delgavs därför den myndigheten. Förundersökning inleddes vilken senare ledde till att omkring 100 kg narkotika togs i beslag.

Sammanfattningsvis har det genom kartläggningen kommit fram att uppgifter från inhämtningslagen, i en stor majoritet av de granskade underrättelseärendena, har bidragit till att föra ärendet framåt. Det finns därmed grund för att påstå att tillämpningen av lagen har lett till nytta i dessa ärenden. Vår bedömning är därför att tillämpningen sammantaget har lett till beaktansvärd nytta i den öppna polisens och Tullverkets brottsbekämpande verksamhet.

9.2.3.9 Integritetsintrång

Den inverkan på den personliga integriteten som tillämpningen av inhämtningslagen har fört med sig kan i viss utsträckning relateras till uppgifter om tillämpningens omfattning. Av Åklagarmyndighetens redovisning av användningen av vissa hemliga tvångsmedel under 2013 framgår att den öppna polisen och Tullverket under det året fattade sammanlagt 595 beslut enligt inhämtningslagen, varav 553 fattades av den öppna polisen och 42 av Tullverket (ÅM-A 2013/1962). Av motsvarande redovisning för 2012 framgår att det under andra halvåret 2012 (inhämtningslagen trädde i kraft den 1 juli 2012) fattades sammanlagt 369 beslut, varav 333 fattades av den öppna polisen och 36 av Tullverket. I analysen av svensk rätts förhållande till EU-rätten framhölls att den statistik som hittills presenterats visar att inhämtning sker i ett förhållandevis begränsat antal ärenden och vid arbete med mycket grova brott (Ds 2014:23 s. 83). Det finns inte anledning att nu göra någon annan bedömning.

Det står dock klart att det inte är tillräckligt att analysera den inverkan inhämtningslagen har haft på den personliga integriteten enbart baserat på antalet beslut enligt lagen. Det är också av stor betydelse för bedömningen att undersöka frågor om bl.a. vilken typ av kommunikationsutrustning besluten gäller, i vilka situationer och mot vilka personer som lagen används, för vilka tidsperioder beslut

enligt lagen gäller och hur de brottsbekämpande myndigheterna hanterar den information som kommer in.

Som nämnts ovan (avsnitt 9.2.3.2) har besluten i de ärenden som utredningen har granskat i det närmaste uteslutande avsett mobiltelefoner. Detta innebär att integritetsintrånget, jämfört med t.ex. fasta telefoner som används av flera personer, inte blir lika omfattande. Samtidigt kan det givetvis hända att uppgifter hämtas in om samtal med personer som inte har någon koppling till den misstänkta brottsliga verksamheten vilket leder till integritetsintrång för dessa personer.

Många av de intervjuade handläggarna har framhållit att myndigheterna gör vad de kan för att begränsa integritetsintrånget. Ett vanligt svar när vi har bett handläggarna att beskriva de överväganden som görs innan ett beslut enligt inhämtningslagen fattas är t.ex. att tidsperioden begränsas till kortast möjliga för att begränsa integritetsintrånget. Vi har i vår kartläggning inte funnit någonting som talar emot att det förhåller sig på det sättet, utan normalt är den tidsperiod som besluten gäller ganska kort. Detta hänger också samman med att uppgiftsinhämtning enligt lagen är förknippad med kostnader för myndigheterna. Det gäller dels de avgifter som teleoperatörerna debiterar för att lämna ut uppgifter, men framför allt har många av handläggarna framhållit att analys av telefonlistor är resurskrävande.

Resursfrågan har betydelse även för att begränsa det antal personer i ärendet som myndigheterna väljer att hämta in samtalslistor för. En handläggare uttryckte det så att ”det alltid görs en specifik och noggrann avgränsning innan samtalslistor hämtas in. När detta sker finns alltid ett gediget underlag för att den aktuella personen är inblandad i brottslig verksamhet. I detta fall avgränsades inhämtningen till (personen X), exempelvis undersöktes inte (personen Y)”.

Ett annat vanligt svar från handläggarna är att myndigheterna bara är intresserade av ”kriminella” kontakter och att uppgifter om mer sociala kontakter, t.ex. med familj och vänner, därför sållas bort i största möjliga utsträckning. Detta är logiskt även från resurssynpunkt, eftersom myndigheterna rimligtvis varken har tid eller intresse för att analysera sådana kontakter som inte är relevanta för den brottsbekämpande verksamheten. Det finns därför inte någon anledning att ifrågasätta att informationen från inhämtningslagen

hanteras på det beskrivna sättet. En sådan hantering innebär givetvis att integritetsintrånget i viss utsträckning begränsas. Ett problem av integritetskaraktär är dock att myndigheterna normalt sett inte vet vad kommunikationen handlar om. Detta innebär rimligtvis att en del uppgifter om samtal etc. behandlas trots att de inte har någon koppling till brottslig verksamhet. En handläggare uttryckte detta på följande sätt: ”Bekymret med inhämtande av teletrafik är att man får uppgifter om all kommunikation under den tid som beslutet gäller, vilket innebär ett integritetsintrång. Förhoppningsvis är en del av uppgifterna intressanta. Vi försöker att sortera bort så mycket som möjligt innan informationen behandlas vidare.”

Flera handläggare har också betonat att de uppgifter som myndigheterna får del av genom tillämpningen av inhämtningslagen hanteras inom en snäv krets. Detta är säkerligen riktigt så länge informationen hanteras inom ramen för det aktuella underrättelseärendet. Vi har dock uppmärksammat att delar av de inhämtade uppgifterna i många fall vidarebehandlas enligt exempelvis polisdatalagen, vilket rimligtvis borde innebära att de blir tillgängliga i en något bredare krets. Enligt polisdatalagen ska dock tillgången till personuppgifter begränsas till vad varje tjänsteman behöver för att kunna fullgöra sina arbetsuppgifter (11 §).

Många av handläggarna har också beskrivit att de personer som tvångsmedel enligt lagen används mot ofta har flera olika telefoner. Det är t.ex. inte ovanligt att personen har en telefon för kontakt med familj etc. och en annan för de kontakter som har samband med den misstänkta brottsliga verksamheten (en s.k. ful-lur). Flera handläggare har berättat att det är den senare typen som myndigheterna är ute efter och om de i stället råkar få tag i den ”sociala” telefonen så sorteras informationen i allmänhet bort. I vissa fall kan dock information från en sådan telefon användas för att undersöka om personen också har en ful-lur.

Som nämnts ovan är det tydligt att många av de personer som de granskade underrättelseärendena avser har för vana att regelbundet byta telefonabonnemang. Syftet med det torde vara att undgå avlyssning eller övervakning och därigenom försvåra de brottsbekämpande myndigheternas arbete. Man kan alltså dra slutsatsen att dessa personer i viss utsträckning räknar med att deras telefoner kan vara avlyssnade och/eller övervakade, vilket enligt utredningens uppfattning innebär att integritetsintrånget i dessa fall måste anses

vara begränsat. Det kan också ses som en slags bekräftelse på att myndigheterna är rätt ute med sina misstankar.

Sammanfattningsvis har tvångsmedel enligt inhämtningslagen använts av den öppna polisen och Tullverket i ett begränsat antal fall vilka rör mycket allvarlig brottslighet. Användningen har riktats mot ett begränsat antal personer. I de fall tvångsmedel har använts har dock personlig information samlats in i relativt stor utsträckning. Denna information har använts för att kartlägga personernas kontakter och rörelsemönster vilket har inneburit integritetsintrång. Intrången har drabbat såväl de personer som besluten avser som de personer som dessa har haft kontakt med.

Tvångsmedel enligt inhämtningslagen ger inte tillgång till innehållet i kommunikationen. Integritetsintrånget är därför normalt betydligt mindre än vid t.ex. hemlig avlyssning av elektronisk kommunikation. Att innehållet inte är känt kan dock i vissa fall leda till att uppgifter om samtal etc. behandlas trots att de inte har någon koppling till brottslig verksamhet.

Ytterligare två omständigheter av betydelse för det faktiska integritetsintrånget bör påpekas. Dels är antalet s.k. basstationstömningar lågt. Dels avser inhämtningarna så gott som uteslutande mobiltelefoner. Det innebär bl.a. att erhållna uppgifter inte sammanställs med t.ex. data om internetaktivitet.

9.2.3.10 Några sammanfattande slutsatser

Enligt 2 § inhämtningslagen får uppgifter hämtas in endast om åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka viss brottslig verksamhet. Av lagens förarbeten framgår att detta innebär att det ska finnas andra uppgifter som möjliggör en bedömning av uppgifternas förväntade betydelse för att t.ex. förebygga eller förhindra sådan brottslig verksamhet som avses i bestämmelsen. I detta ligger också ett krav på uppgifternas förväntade betydelse för det syfte i vilket de inhämtas. Kravet på särskild vikt innefattar alltså ett kvalitetskrav på de upplysningar som åtgärden kan ge och ett krav på behovet av inhämtningen i det enskilda fallet. Bedömningen får inte bygga enbart på spekulationer eller allmänna antaganden utan måste grundas på faktiska omständigheter (prop. 2011/12:55 s. 121). Vår kartläggning ger stöd för

slutsatsen att myndigheternas tillämpning av inhämtningslagen med viss marginal når upp till dessa krav, både vad gäller kvaliteten på den information som finns i ärendena när beslut enligt inhämtningslagen fattas och när det gäller behovet av information i ärendet. Detta hänger även samman med de begränsningar som myndigheternas resurser sätter. En handläggare uttryckte det så att ”Lagstiftningen ställer upp minimikrav för när det är tillåtet att använda inhämtningslagen. Polisen prioriterar och tar endast in samtalslistor när man med marginal är över den gränsen. Det är en resursfråga”. Vår kartläggning ger dessutom stöd för att den öppna polisen och Tullverket hanterar ärenden om inhämtning av uppgifter enligt inhämtningslagen på ett tillfredsställande sätt. Vi har t.ex. inte kunnat finna några tecken på att lagen överanvänds. Tvärtom framstår det som om användningen begränsas till ett förhållandevis litet antal ärenden som noga valts ut och prioriterats och som samtliga rör mycket allvarlig brottslig verksamhet för vilken samhällsintresset av att brottsligheten upptäcks är betydande. Det framgår också att myndigheterna anstränger sig för att begränsa integritetsintrånget, både vad gäller avgränsning av personkrets, val av tidsperiod och hantering av inhämtad information.

Det står klart att användningen av inhämtningslagen trots detta innebär relativt kännbara integritetsintrång för enskilda. Detta gäller inte minst sådana personer som har kontakt med de personer som är aktuella i ärendena utan att kontakterna har någon koppling till brottslig verksamhet. Att hemliga tvångsmedel leder till integritetsintrång kan dock accepteras, under förutsättning att behovet av att inhämta uppgifter är tillräckligt starkt. Behovet måste med andra ord stå i proportion till intrånget.

När det gäller frågan om proportionalitet finns det anledning att återknyta till vad som sagts ovan under avsnitt 9.2.3.3 och 9.2.3.4 om de indikationer på brottslig verksamhet som finns i ärendena på förhand och om behovet av att hämta in uppgifter. Som framgått har det kommit fram att det underlag som finns om den brottsliga verksamheten i regel är gediget. Vidare är det tydligt hur de uppgifter som hämtas in enligt inhämtningslagen förväntas kunna bidra till att föra ärendet framåt. Behovet av uppgifterna framgår således tydligt. Som flera handläggare har framhållit vid intervjuerna används inhämtningslagen uteslutande i ärenden som avser misstankar om brottslig verksamhet som innefattar mycket allvarliga brott.

Proportionalitetsfrågor är svåra och lämnar med nödvändighet ett visst utrymme för bedömning. Emellertid bör det framhållas att vi under vår kartläggning inte har kunnat finna något ärende där vi kan hävda att uppgiftsinhämtningen enligt inhämtningslagen har framstått som oproportionerlig.

9.3 Åtgärder för att stärka rättssäkerheten eller integritetsskyddet?

9.3.1 Integritetsstärkande åtgärder vidtogs när inhämtningslagen infördes

Som nämnts i avsnitt 3.5.3.2 kunde brottsbekämpande myndigheter före den 1 juli 2012 få tillgång till historiska trafikuppgifter enligt två olika regelverk; bestämmelserna om hemlig övervakning av elektronisk kommunikation i rättegångsbalken och utlämnande av uppgifterna från leverantörer enligt lagen om elektronisk kommunikation. Myndigheterna kunde då få i princip samma uppgifter oavsett vilka bestämmelser som tillämpades.

När inhämtningslagen infördes gjorde regeringen bedömningen att de dåvarande reglerna i LEK om utlämnande av uppgifter inte framstod som ändamålsenligt utformade och att de inte heller i tillräcklig grad uppfyllde de krav på rättssäkerhet och integritetsskydd som måste ställas på sådana åtgärder (se prop. 2011/12:55 s. 66). Ett flertal åtgärder som syftade till att stärka rättssäkerheten och skyddet för den personliga integriteten vidtogs därför med avseende på inhämtning av uppgifter i underrättelseverksamhet. Till exempel infördes det krav på att inhämtningen ska vara av särskild vikt för ändamålet med åtgärden och att den ska vara proportionerlig. Vidare infördes krav på att ett beslut om inhämtning ska innehålla uppgifter om vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet gäller. Det infördes också regler om vilken tidsperiod ett beslut får avse.

Tidigare fanns inte heller några regler om vem som fick fatta beslut om att hämta in uppgifter. Enligt inhämtningslagen gäller däremot att beslut om inhämtning fattas av myndigheten. Det innebär att utgångspunkten är att det är myndighetschefen som ska

besluta om inhämtningen. Myndighetschefen får dock delegera rätten att fatta beslut till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Den som har fått sådan delegation får inte fatta beslut om inhämtning i operativ verksamhet som han eller hon deltar i.

Till skillnad från tidigare utövar Säkerhets- och integritetsskyddsnämnden tillsyn över inhämtningen. Samtliga beslut om inhämtning av uppgifter ska också anmälas till nämnden. Inhämtade uppgifter får användas i en förundersökning endast efter tillstånd av domstol till hemlig övervakning av elektronisk kommunikation.

9.3.2 Bör inhämtningslagens beslutsordning ändras?

Utredningens bedömning: Beslut om inhämtning av uppgifter enligt inhämtningslagen bör även i fortsättningen fattas av Polismyndigheten, Säkerhetspolisen eller Tullverket.

9.3.2.1 Utgångspunkter

EU-domstolen framhöll i domen om datalagringsdirektivet att direktivet inte föreskrev att de behöriga nationella myndigheternas tillgång till lagrade uppgifter skulle vara underkastad någon förhandskontroll utförd av en domstol eller oberoende myndighet, vars beslut avser att begränsa tillgången till och användningen av uppgifterna till vad som kan anses strängt nödvändigt (p. 62).

Eftersom beslut enligt inhämtningslagen fattas av de brottsbekämpande myndigheterna själva bör det, mot bakgrund av EU-domstolens uttalanden, övervägas om lagens beslutsordning bör förändras på något sätt. Vi har mot den bakgrunden och i enlighet med våra direktiv övervägt ett antal åtgärder som skulle kunna komma i fråga för att ytterligare förbättra kontrollen över inhämtningen av uppgifter enligt lagen. Dessa överväganden redovisas i det följande. Dessförinnan ska vi dock göra vissa mer allmänna reflektioner.

I den ovan nämnda analysen av svensk rätts förenlighet med EU-rätten hävdas att den svenska regleringen, trots att uppgifter kan hämtas in enligt inhämtningslagen utan föregående prövning av

en oberoende instans, vid en helhetsbedömning uppfyller kraven på att tillgången till lagrade uppgifter ska vara begränsad till vad som kan anses strikt nödvändigt. Vid den bedömningen beaktades särskilt att inhämtning enligt lagen sker bara för mycket allvarliga brott, att beslut om inhämtning fattas av myndighetschef med snäva möjligheter till delegation, att tillsyn sker i efterhand av SIN samt – inte minst – att uppgifterna måste passera en domstolskontroll för att kunna användas mot den enskilde i en förundersökning (Ds 2014:23 s. 83).

De brottsbekämpande myndigheternas verksamhet inom ramen för en förundersökning är noga reglerad och tydligt inriktad på ett redan begånget konkret brott. I underrättelseverksamheten är syftet däremot att genom en bred informations- och kunskapsinsamling ge underlag för bearbetning och analys. Utgångspunkten är, ofta utifrån en mer övergripande ansats, att studera och kartlägga en befarad brottslig verksamhet för att förebygga eller förhindra att brottsligheten genomförs (se SOU 2010:103 s. 311 f.). Underrättelseverksamheten är till största delen inte reglerad i lag och bedrivs därför inte inom sådana fasta ramar som gäller för förundersökning. Eftersom underrättelseverksamheten inte är inriktad mot någon specifik brottslig gärning – och ofta inte heller mot någon särskild utpekad person – gör sig inte heller partsintresset gällande på samma sätt i underrättelseverksamheten som under en förundersökning. Den information som på underrättelsestadiet finns om den brottsliga verksamhet som undersöks är också betydligt vagare.

Bland annat av dessa anledningar har det ansetts nödvändigt att upprätthålla en klar gräns mellan den brottsutredande verksamheten inom ramen för en förundersökning och underrättelseverksamheten. Till exempel har det i flera olika sammanhang bedömts mindre lämpligt att tilldela åklagare eller domstolar en beslutsfunktion i de brottsbekämpande myndigheternas allmänna underrättelsearbete (se t.ex. SOU 2009:1 s. 128 ff., SOU 2010:103 s. 311 ff. och prop. 2011/12:55 s. 88 f.). Det har också ansetts finnas en risk för att åklagarnas och domstolarnas objektivitet skulle kunna ifrågasättas om de skulle ha till uppgift att pröva och godkänna olika åtgärder i underrättelseverksamheten. Detta hänger samman med att underrättelseåtgärderna kan leda vidare till förundersökning och rättegång, vilket innebär att frågorna på nytt skulle hamna

på åklagarnas och domstolarnas bord. Det skulle därmed finnas en risk för att det tidigare ställningstagandet skulle påverka också det senare skedet.

Vi har vid kartläggningen funnit att de brottsbekämpande myndigheterna hanterar ärenden om inhämtning av uppgifter enligt inhämtningslagen på ett tillfredsställande sätt. Denna bedömning överensstämmer även med SIN:s uppfattning enligt nämndens redovisning av tillsynsverksamheten under år 2013 (nämndens uttalande den 22 maj 2014 i ärende med dnr 891-2014). Mot den bakgrunden bedömer vi att systemet med myndighetsbeslut, inklusive den kontrollmekanism som SIN:s tillsyn utgör, på det hela taget fungerar väl. I det sammanhanget bör det också framhållas att de brottsbekämpande myndigheterna givetvis har ett eget intresse av att ärenden om tillämpning av integritetskänslig lagstiftning handläggs på ett så bra sätt som möjligt.

Av SIN:s redovisning av tillsynsverksamheten för 2013 framgår dock att nämnden har uppmärksammat att det förekommer vissa brister i myndigheternas hantering av ärenden enligt inhämtningslagen, bl.a. att underrättelseskyldigheten till nämnden i ett inte obetydligt antal ärenden fullgjorts för sent. Nämnden har också på senare tid gjort några uttalanden om tillämpningen av reglerna i inhämtningslagen i vissa specifika fall som handlagts av den öppna polisen, vilka också visar på att brister förekommer (se avsnitt 3.5.4.2). I ett av dessa fall får bristerna dessutom betecknas som allvarliga (nämndens uttalande den 11 september 2014 i ärende med dnr 156-2014). Emellertid är det fråga om enstaka felaktigheter i en tillämpning som i övrigt fungerar väl. Besluten i det sist nämnda ärendet fattades också när inhämtningslagen hade varit i kraft under endast ett drygt halvår. Av nämndens uttalande framgår att de granskade besluten var bland de första som den aktuella beslutsfattaren fattade enligt inhämtningslagen. Det finns därför mycket som talar för att felaktigheterna berodde på bristande vana av att hantera ärenden enligt lagen. Vidare framgår av nämndens uttalande att den aktuella polismyndigheten har vidtagit åtgärder i form av utbildningsinsatser och nya rutiner för att säkerställa att beslut om inhämtning enligt inhämtningslagen fattas och dokumenteras på ett korrekt sätt.

9.3.2.2 Domstolsbeslut

Enligt våra direktiv är ett av de alternativ som ska övervägas om domstol bör tilldelas uppgiften att fatta beslut om inhämtning av uppgifter enligt inhämtningslagen. En sådan ordning skulle innebära att besluten skulle fattas av en från de brottsbekämpande myndigheterna utomstående och oberoende instans (jfr EU-domstolens dom om datalagringsdirektivet, p. 62).

Alternativet med domstolsprövning övervägdes i samband med att inhämtningslagen infördes. Regeringen uttalade då följande (prop. 2011/12:55 s. 88 f.):

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

angivna bakgrunden anser regeringen att allmänna domstolar inte bör ges beslutanderätten för inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Frågan om allmän domstol som beslutsinstans utanför en förundersökning diskuterades även i förarbetena till lagen om preventiva tvångsmedel (prop. 2005/06:177 s. 64 f.). Frågan var då om det i stället för allmän domstol var lämpligt att inrätta en särskild nämnd som skulle kunna fatta beslut om tvångsmedelsanvändning enligt lagen. Regeringen bedömde dock att ett system med en särskild nämnd har nackdelar och att det torde vara svårt att inom ramen för en nämndprövning skapa en ordning som på samma påtagliga sätt kan ta till vara integritetsintresset. Ett system med en nämnd skulle också enligt regeringen kunna bli sårbart genom att det skulle kunna uppstå svårigheter att med kort varsel samla nämnden för föredragning och beslut. Regeringen menade därför att övervägande skäl talade mot ett införande av en nämnd som fattar beslut i dessa frågor och föreslog att prövningen i stället skulle göras av allmän domstol (se 6 § lagen om preventiva tvångsmedel). Det bör emellertid i detta sammanhang betonas att det rör sig om en lagstiftning som tillämpas i en jämförelsevis mycket blygsam omfattning (se SOU 2012:44 s. 316 f.) och i situationer där det handlar om att bedöma en på visst sätt konkretiserad risk för att exempelvis ett terrorattentat ska inträffa (se prop. 2013/14:237 s. 195 f.). De åtgärder som står till buds enligt den lagen innefattar dessutom de betydligt mer integritetskänsliga tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning.

Enligt vår uppfattning saknas det skäl att nu göra någon annan bedömning än den regeringen gjorde när inhämtningslagen infördes. De argument som tidigare förts fram mot en domstolsprövning och som nyss återgetts har fortfarande bärkraft. Underrättelseverksamheten är sådan att den inte kan bedrivas inom sådana fasta ramar som gäller för förundersökningsförfarandet. Vidare är underrättelseverksamheten, till skillnad från sådana utredningar som bedrivs inom ramen för en förundersökning, inte primärt inriktad på någon viss gärning eller någon viss person.

Till detta kommer den omständigheten att det är tveksamt om domstolarna, inom ramen för den nuvarande jourorganisationen,

skulle kunna tillgodose de brottsbekämpande myndigheternas behov av snabba beslut. Utredningen instämmer i att en ordning med dygnetruntberedskap för de allmänna domstolarna för att pröva frågor om inhämtande av uppgifter i underrättelseverksamhet inte framstår som vare sig rimlig eller ändamålsenlig. Däremot skulle behovet av snabba beslut kunna tillgodoses genom att de brottsbekämpande myndigheterna får en möjlighet att i brådskande fall fatta interimistiska beslut, med en efterföljande prövning av beslutet i domstol. En sådan ordning är dock inte heller helt oproblematisk. Dels kvarstår övriga argument mot en domstolsprövning. Dels gäller i princip samtliga beslut enligt inhämtningslagen uppgifter i förfluten tid. När domstolen väl överprövar ett interimistiskt beslut skulle därför i de allra flesta fall uppgifterna redan vara levererade till den brottsbekämpande myndighet som begärt dem. I sådana fall skulle det behövas regler om vad följden blir om domstolen upphäver det interimistiska beslutet, i likhet med de som gäller i fråga om interimistiska beslut om hemliga tvångsmedel under en förundersökning (se 27 kap. 21 a § rättegångsbalken). Att föreskriva att inhämtade uppgifter i en liknande situation inte får användas i en förundersökning är logiskt, eftersom det får den konsekvensen att uppgifterna inte kan användas som bevisning. I underrättelseverksamhet är det dock mer oklart vad en motsvarande bestämmelse skulle få för praktiska följder. En bestämmelse som exempelvis innebär att myndigheten i sådan verksamhet måste bortse från information som den faktiskt känner till framstår inte som förtroendeingivande.

Ett annat skäl som talar mot att beslutskompetensen anförtros domstol, eller någon annan myndighet som är fristående från de brottsbekämpande myndigheterna, är intresset av att kunna hålla den information som finns i underrättelseärendena inom en så snäv personkrets som möjligt. Som nämnts innehåller den information som ligger till grund för beslut enligt inhämtningslagen ofta uppgifter från källdrivning och tipsare. Om det blev känt att dessa personer har lämnat den aktuella typen av uppgifter till de brottsbekämpande myndigheterna, finns det givetvis en stor risk för att personerna skulle kunna utsättas för repressalier. Även om domstolarna naturligtvis har stor vana av att hantera sekretesskyddat material på ett säkert sätt, går det inte att bortse från att risken för

spridning av informationen ökar ju större personkrets som får tillgång till den.

Sammantaget – och i ljuset av att vi vid vår undersökning inte funnit några tecken på att nuvarande befogenheter missbrukas – överväger de skäl som talar emot att införa ett system där domstol fattar beslut om tillstånd till inhämtning av uppgifter enligt inhämtningslagen fördelarna med en sådan ordning.

9.3.2.3 En möjlighet att överklaga

Ett annat alternativ skulle kunna vara att konstruera ett system med en möjlighet att överklaga de brottsbekämpande myndigheternas beslut enligt inhämtningslagen till domstol.

Det finns en hel del praktiska problem förknippade med en sådan ordning. Eftersom de personer som besluten gäller förutsätts inte känna till dem, måste någon annan anförtros uppgiften att granska samtliga beslut för att avgöra vilka som eventuellt bör överklagas. Detta förutsätter alltså att ett offentligt ombud eller motsvarande involveras i beslutsprocessen hos myndigheterna. Dessutom är det sannolikt att relativt få beslut skulle överklagas. Svårigheten för tingsrätterna att arbeta upp en vana av att handlägga ärenden enligt inhämtningslagen är därför än mer tydlig med ett sådant system än med en ordning med generell domstolsprövning av samtliga beslut. Det skulle också behövas regler om vad konsekvensen blir om domstolen ändrar ett överklagat beslut, vilket leder till samma problem som diskuterats ovan beträffande interimistiska beslut. Enligt utredningens mening bör det inte införas regler om överklagande av beslut enligt inhämtningslagen.

9.3.2.4 Åklagarbeslut

Regeringen konstaterade i förarbetena till inhämtningslagen att åklagare som regel inte deltar i polisens eller Tullverkets underrättelseverksamhet och att åklagarinträde sker först i samband med att förundersökning inletts och någon är skäligen misstänkt för brottet. Regeringen ansåg vidare att det bör krävas starka skäl för att åklagare ska tilldelas en roll i de brottsbekämpande myndig-

heternas allmänna underrättelsearbete. Beslutanderätten borde därför enligt regeringen inte läggas hos åklagare (prop. 2011/12:55 s. 89).

Liknande synpunkter framfördes av både Åklagarmyndigheten och Ekobrottsmyndigheten i myndigheternas remissvar över det betänkande som låg till grund för propositionen (SOU 2009:1). Åklagarmyndigheten pekade också på att en viktig förutsättning för att åklagaren ska kunna leva upp till sin objektivitetsplikt är att han eller hon skapar distans till underrättelseverksamheten.

Frågan om att tilldela åklagare en roll i polisens underrättelseverksamhet övervägdes redan i samband med att lagen om preventiva tvångsmedel infördes (prop. 2005/06:177 s. 67 f.). Regeringen angav då att det som talar för att polisen skulle kunna ansöka om tillstånd till de aktuella tvångsmedlen är att ärendena befinner sig på ett spaningsstadium och att det därför skulle innebär ett avsteg från den rådande ansvarsfördelningen mellan polis och åklagare om åklagare tilldelas en roll i polisens underrättelsearbete. Det skulle därför, menade regeringen, krävas starka skäl för att införa en sådan ordning. Emellertid anförde regeringen också att polis och åklagare redan i dag i samråd bedömer om det finns tillräckliga skäl för att inleda förundersökning i ärenden om allvarlig brottslighet eller om det krävs ytterligare underrättelse- eller spaningsåtgärder. Regeringen nämnde också att, i de större utredningar om allvarlig brottslighet som utförts med framgång, så har regelmässigt åklagare, spanings- och underrättelseavdelning samt utredningsenheter samarbetat på ett mycket tidigt stadium.

Åklagare har som huvudsakliga uppgifter att leda förundersökningar, väcka åtal och föra talan i domstol. Åklagarens roll och beslutsfunktioner i den verksamheten är noga reglerade.

Till skillnad från förundersökningsverksamheten är underrättelsearbetet en renodlad polisiär verksamhet som till stora delar inte är reglerad i lag. Det arbete som bedrivs i den verksamheten, där man t.ex. i ett tidigt skede kartlägger och analyserar företeelser som senare kan komma att utvecklas till konkreta brott, skiljer sig många gånger till sin karaktär från förundersökningsverksamheten. Det rör sig alltså i dessa fall om informationsinsamling på ett betydligt tidigare stadium där det inte finns någon anknytning till ett särskilt brott eller en särskild brottsutredning. Att anförtro åklagare en beslutsfunktion i sådan verksamhet skulle innebära att åklagaren behöver ta ansvar för åtgärder långt innan det finns förutsättningar

för att inleda förundersökning. En sådan uppgift är därför svår att förena med den roll som åklagarna har i det nuvarande straffprocessuella systemet.

Mot den angivna bakgrunden instämmer vi i att det bör krävas starka skäl för att frångå den rådande ansvarsfördelningen mellan polis och tull respektive åklagare. Ett sådant skäl skulle t.ex. kunna vara om det hade funnits tydliga indikationer på att det nuvarande systemet missbrukas. Genom vår kartläggning har det emellertid kommit fram klara indikationer på att systemet med myndighetsbeslut fungerar väl. Det saknas därför sådana starka skäl som bör krävas för att föreslå att beslutsbefogenheten enligt inhämtningslagen ska anförtros åklagare. Också de resonemang som vi fört beträffande domstolar i avsnitt 9.3.2.2 har därvid relevans.

Som nämnts tillämpas lagen om preventiva tvångsmedel i en jämförelsevis mycket blygsam omfattning och i situationer där det handlar om att bedöma en på visst sätt konkretiserad risk. I dessa fall handlar det också om att tillstånd till tvångsmedel söks hos domstol. Betänkligheterna mot att åklagare har en roll i ett sådant förfarande är betydligt mindre.

9.3.2.5 Ett nytt beslutsorgan

Som redan har framgått övervägdes frågan om det är lämpligt att inrätta särskilda nämnder för beslut om inhämtning av uppgifter i underrättelseverksamhet i samband med att lagen om preventiva tvångsmedel infördes. Regeringen bedömde dock att ett system med en särskild nämnd har nackdelar, bl.a. att det skulle vara svårt att inom ramen för en nämndprövning skapa en ordning som på samma påtagliga sätt kan ta tillvara integritetsintresset. Ett system med nämnd skulle också kunna bli sårbart genom att det skulle kunna uppstå svårigheter att med kort varsel samla nämnden för föredragning och beslut. Regeringen menade därför att övervägande skäl talade mot att införa en nämnd som fattar beslut i dessa frågor (prop. 2005/06:177 s. 64 f.).

Frågan övervägdes på nytt i samband med att inhämtningslagen infördes. Regeringen hänvisade då till de överväganden som gjorts i samband med införandet av lagen om preventiva tvångsmedel och

framhöll att det saknades skäl att göra en annan bedömning (prop. 2011/12:55 s. 89).

Fördelen med en nämndprövning skulle vara att besluten skulle fattas av en oberoende myndighet, samtidigt som man i huvudsak undviker de invändningar som finns mot att förlägga beslutskompetensen hos ett organ som senare skulle få befattning med ärendena. Även med ett sådant system kan dessa principiella invändningar emellertid inte undvikas fullt ut. Exempelvis skulle en sådan nämnd sannolikt ledas av en ordinarie domare, vilket även det skulle kunna leda till risk för att domstolens roll som oberoende prövningsinstans i brottmålsförfarandet ifrågasätts. Härtill kommer de övriga skäl som vi har anfört mot prövning i domstol och av åklagare.

Utredningen instämmer vidare i regeringens tidigare bedömning att ett nämndsystem innebär vissa praktiska nackdelar. Prövningens i många fall brådskande natur i kombination med en spridd geografisk förekomst gör att det inte framstår som realistiskt att inrätta ett sådant organ på en enda plats i landet. Att i stället inrätta flera nämnder eller liknande organ på olika platser för att kunna tillgodose behovet av närhet till lokala brottsbekämpande myndigheter framstår ur verksamhets- och effektivitetsperspektiv inte heller som särskilt lämpligt.

En annan fråga är också hur ett nämndsystem skulle behöva organiseras för att de brottsbekämpande myndigheternas behov av snabba beslut ska kunna tillgodose. Det är knappast rimligt att tänka sig att ett antal nämnder av det aktuella slaget ska vara tillgängliga dygnet runt för att snabbt kunna fatta beslut i frågor om inhämtning av uppgifter enligt inhämtningslagen. Visserligen kan det övervägas att lösa det problemet med en möjlighet till interimistiska beslut. Det skulle dock innebära att man ställs inför samma svårigheter som behandlats ovan i anslutning till frågan om domstolsprövning (se avsnitt 9.3.2.2).

Som redan har framgått är det vår bedömning att den nuvarande beslutsordningen i huvudsak fungerar väl. Mot den bakgrunden – och med hänsyn till de nackdelar med ett nämndsystem som påtalats ovan – finns det inte tillräckliga skäl som talar för att föreslå att ett sådant system införs.

9.3.3 Åtgärder inom ramen för den befintliga beslutsordningen

9.3.3.1 Beslutsnivån inom myndigheterna

Myndighetschefen får, enligt 4 § inhämtningslagen, delegera rätten att fatta beslut om inhämtning till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Den till vilken rätten att fatta beslut har delegerats får inte fatta beslut om inhämtning i sådan operativ verksamhet som han eller hon deltar i. I lagens förarbeten anges att delegation bör kunna ske till t.ex. myndighetschefens ställföreträdare, rikskriminalchefen, biträdande rikskriminalchefen, biträdande säkerhetspolischefen biträdande länspolismästare, länskriminalchefer, chefer för operativ verksamhet och chefer för underrättelseverksamhet (prop. 2011/12:55 s. 123).

Utredningen har inhämtat uppgifter från de aktuella myndigheterna i fråga om hur delegationsfrågan hanteras inom respektive myndighet.

Säkerhetspolisen har angett att det är den operativa chefen (OPC) på Säkerhetspolisen som fattar beslut om inhämtning av uppgifter enligt inhämtningslagen. Den operativa chefen, som är direkt underställd myndighetschefen, Generaldirektören, fick en grundutbildning då lagen infördes. Myndighetens chefsjurist sitter i samma ledningsgrupp som den operativa chefen och kan vägleda och uppdatera vid eventuella tveksamheter. Myndighetens rättsenhet finns därutöver som ett stöd.

Sedan den 1 januari 2015 har Säkerhetspolisen en egen funktion som ska omhänderta metodprocessen enligt inhämtningslagen. Ett beslut enligt inhämtningslagen går allt som oftast igenom en kedja av kontroller, där arbetsgruppsledare (AGL) och därefter operativ ledare (OPL) har granskat beslutsunderlag utifrån kraven på rättssäkerhet och integritet, innan ärendet föredras för den operativa chefen. Majoriteten av de funktioner som är en del av processen har genomgått en tvångsmedelsutbildning där inhämtningslagen var en del av utbildningspaketet.

Polismyndigheten har framfört att beslutsbefogenheten i den tidigare organisationen var delegerad till sektionschef eller biträdande sektionschef hos underrättelsesektionen vid respektive polismyndighet. Rekommendationen från dåvarande Rikspolisstyrelsen

(RPS) var att varje polismyndighet skulle upprätta egna tjänsteföreskrifter när det gäller rutinerna för handläggningen av ärenden enligt inhämtningslagen. Utredningen har tagit del av den tjänsteföreskrift som beslutats av RPS (TjF 2012:4 102). Den innehåller bestämmelser bl.a. om hur en begäran och beslut om uppgifter ska hanteras, vilka befattningar som har befogenhet att fatta beslut, hur diarieföring och dokumentation ska gå till samt hur underrättelse till SIN och intern uppföljning ska hanteras. Vid sidan av det finns även rutindokument där rutinerna beskrivs på en mer detaljerad nivå.

Enligt Polismyndigheten finns det inte någon formell utbildning för beslutsfattarna. Däremot har dessa bedrivit självstudier av regelverk och rutiner. Information om regler och rutiner har också getts till handläggare. Vidare har både RPS, Säkerhetspolisen och SIN tidigare skickat ut promemorior med rutiner m.m. till de dåvarande polismyndigheterna.

Polismyndigheten har också framhållit att ett av syftena med den nya polisorganisationen är att skapa förutsättningar för större enhetlighet inom organisationen. Den Nationella Operativa Avdelningen (NOA) har fått ett processansvar för polisens underrättelseverksamhet i stort. Detta innebär att avdelningen har mandat att arbeta för att skapa enhetlighet och att följa upp hur frågor i underrättelseverksamheten hanteras inom Polismyndigheten. Samtliga tjänsteföreskrifter som funnits på området är under bearbetning, och avsikten är att NOA ska gå ut med riktlinjer och föreskrifter som ska gälla för hela myndigheten.

Hur beslutskompetensen enligt inhämtningslagen kommer att delegeras i den nya organisationen är i dagsläget inte helt klart. Det är tänkbart att befogenheten kommer att koncentreras till den regionala snarare än den lokala nivån. Den regionala nivån har också daglig kontakt med NOA, vilket skulle innebära att det finns en ”kedja” mellan central-regional-lokal underrättelseverksamhet.

Tullverket har angett att beslutsbefogenheterna enligt inhämtningslagen regleras av myndighetens arbetsordning. Enligt denna är det endast ett fåtal befattningshavare som har befogenhet att fatta beslut enligt lagen. Sådan befogenhet tillkommer chefen och biträdande chefen för Kompetenscenter (KC) Analys och Underrättelse, biträdande chefen för KC Nord, cheferna för tullkriminalavdelningarna, biträdande chefen för Tullkriminalavdelningen Malmö,

utredningschefen och projektchefen för KC Nord samt cheferna för underrättelseenheterna.

Beslutsfattarna har enligt Tullverket inte genomgått någon formell utbildning. Däremot diskuteras frågor om hanteringen löpande inom myndigheten. Beslutsfattarna har vid behov stöd av myndighetens rättsenhet.

Sedan den 1 januari 2015 ansvarar KC Analys och Underrättelse för hanteringen av ärenden enligt inhämtningslagen varför det interna regelverket samt delegationsbesluten håller på att uppdateras. KC Analys och Underrättelse ansvarar också för att underrätta SIN om beslut om inhämtning senast en månad efter det att inhämtningsärendet avslutades, dvs. efter att uppgifterna inkommit till Tullverket.

Enligt utredningens uppfattning innebär den nuvarande bestämmelsen i 4 § inhämtningslagen att de krav som rimligen kan ställas i författning på den som beslutskompetens delegeras till också ställs. Det är helt enkelt svårt att se vad som skulle kunna krävas, utöver att den som fattar beslut ska ha den särskilda kompetens, utbildning och erfarenhet som behövs för uppgiften och att vederbörande dessutom inte får delta operativt i den underrättelseoperation där han eller hon beslutar. Det är inte heller lämpligt att i författning peka ut någon eller några särskilt angivna typer av befattningshavare som beslutskompetens får delegeras till. En sådan regel riskerar att bli alltför stelbent och kan dessutom påverkas av förändringar i myndigheternas organisation. Utredningen har därför valt att inte lämna några förslag till förändringar av den delegationsbestämmelse som gäller i dagsläget.

En annan sak är hur delegationsfrågorna hanteras av myndigheterna i praktiken. Det system som Säkerhetspolisen har beskrivit innebär att besluten fattas på en mycket hög nivå inom myndigheten. Att samma befattningshavare fattar samtliga myndighetens beslut enligt lagen innebär också att denne får stor vana av att hantera dessa frågor, vilket skapar goda förutsättningar för enhetlighet och hög kvalitet i beslutsfattandet. Utredningen kan därför inte se att det skulle finnas anledning att förändra det system som Säkerhetspolisen tillämpar.

Enligt utredningens uppfattning framstår vidare den ordning som f.n. övervägs inom Polismyndigheten som ändamålsenlig. Om beslutsbefogenheten koncentreras till en eller ett fåtal befattningar

på en hög nivå inom den regionala organisationen, innebär det att även dessa kommer att få god vana av att hantera ärenden enligt inhämtningslagen. Detta kan med stor sannolikhet bidra till att höja och garantera kvaliteten i beslutsprocessen hos Polismyndigheten. Det är också sannolikt att det övergripande ansvar som NOA har fått kommer att innebära att ärendena handläggs mer enhetligt och med hög kvalitet. Vi förutsätter att Polismyndigheten kommer att välja en lösning som tillgodoser dessa intressen.

Det system som Tullverket har beskrivit innebär även det att besluten fattas av ett fåtal befattningshavare på hög nivå inom organisationen. I likhet med hur det förhåller sig hos Polismyndigheten finns numera inom Tullverket en central funktion med ett övergripande ansvar för hanteringen av ärenden enligt inhämtningslagen.

Av dessa skäl och eftersom bestämmelsen om delegation har en så strikt utformning som man rimligen kan begära föreslår vi på den här punkten inga författningsändringar. Vi anser oss dock kunna utgå från att Polismyndigheten i sitt vidare arbete med egna föreskrifter kommer att uppmärksamma dessa frågor för att garantera en beslutsordning som uppfyller höga krav på rättssäkerhet. Enligt vad vi inhämtat finns dessutom en förbättringspotential vad gäller kvaliteten på polisens framställningar om att få ut data. Också den frågan bör kunna hanteras på detta sätt.

Det finns i sammanhanget anledning att framhålla vikten av att de befattningshavare som anförtros uppgiften att fatta beslut enligt inhämtningslagen får ändamålsenlig utbildning och fortbildning i frågor om hemliga tvångsmedel. Detta gäller inte minst integritetsfrågorna.

9.3.3.2 Underrättelseskyldigheten till Säkerhets- och integritetsskyddsnämnden

Utredningens förslag: Säkerhets- och integritetsskyddsnämnden ska underrättas om beslut enligt inhämtningslagen genom att den beslutande myndigheten ska ge in själva beslutet till nämnden.

SIN:s tillsyn över de brottsbekämpande myndigheternas tillämpning av reglerna om hemliga tvångsmedel, inklusive reglerna i inhämtningslagen, har behandlats i avsnitt 3.5.4.2. Bedömningen har tidigare gjorts att nämndens tillsynsverksamhet har utgjort en väl fungerande kontrollmekanism som i de fall brister har kommit fram har lett till att åtgärder vidtagits med anledning av dessa (se SOU 2012:44 s. 667). Det saknas skäl att nu göra någon annan bedömning.

Utredningen har ställt frågan till SIN om det finns några åtgärder som enligt nämndens uppfattning skulle kunna vidtas för att göra tillsynen än mer effektiv. Nämnden har då framfört bl.a. att bestämmelsen i 6 § inhämtningslagen om underrättelseskyldighet till nämnden skulle kunna förtydligas. Enligt nämnden framgår det inte tydligt, vare sig av bestämmelsens ordalydelse eller av några skrivningar i förarbetena, att underrättelseskyldigheten tar sikte på själva beslutet. I de allra flesta fall fullgör de beslutande myndigheterna visserligen sin underrättelseskyldighet genom att ställa sina beslut till SIN. Det har dock hänt att SIN underrättats om fattade beslut på ett annat sätt, t.ex. genom en särskild skrivelse som sannolikt inte utgör beslutet, och i vissa fall uppkommer frågan om SIN verkligen fått del av beslutet. Enligt nämnden ska följderna av otydligheten i detta avseende inte överdrivas. Enligt nämnden kan dock underrättelseskyldigheten, om det bedöms lämpligt, förtydligas.

Det är rimligt att underrättelseskyldigheten fullgörs på det sätt som SIN har förordat, dvs. genom att den brottsbekämpande myndigheten ger in själva beslutshandlingen till nämnden. Vi föreslår därför att 6 § inhämtningslagen ändras så att detta krav framgår tydligt.

9.3.3.3 Beslutens innehåll

Enligt 5 § inhämtningslagen ska beslut enligt lagen innehålla uppgift om vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet avser. Av författningskommentaren till bestämmelsen framgår att kravet på att ange den brottsliga verksamheten innebär att det, vid inhämtning som sker enligt 2 §, ska anges vilket eller vilka brott som inne-

fattas i verksamheten och att det vid inhämtning enligt 3 § ska anges vilken av punkterna 1–5 som ligger till grund för beslutet (prop. 2011/12:55 s. 123).

SIN har framfört till utredningen att skrivningen i författningskommentaren är något otydlig eftersom den ger vid handen att det är brottet eller brotten – och inte den brottsliga verksamheten – som ska anges i besluten. Enligt nämnden anger de beslutande myndigheterna i dagsläget i sina underrättelser ofta endast det eller de brott som innefattas i den brottsliga verksamhet som åtgärden syftar till att förebygga, förhindra eller upptäcka, och inte den brottsliga verksamheten som sådan. För att SIN i samtliga fall ska kunna kontrollera att inhämtningen avser sådana brott som omfattas av inhämtningslagen (jfr 2 och 3 §§) och att överskottsinformation samt förstöring av materialet hanteras rättsenligt (jfr 7 och 9 §§) kan det finnas anledning att överväga om den aktuella bestämmelsen uttryckligen ska ta sikte på både den brottsliga verksamheten och det eller de brott som ingår i denna.

Av förarbetena till polisdatalagen framgår att begreppet brottslig verksamhet syftar på verksamhet av viss konkretion (prop. 2009/10:85 s. 362). Däremot krävs inte att misstanken avser en konkretiserad gärning på samma sätt som vid förundersökning. Hur konkret den brottsliga verksamheten kan beskrivas i ett underrättelseärende varierar i hög grad från fall till fall och även beroende på i vilket skede ärendet befinner sig. Det kan också ha betydelse vilken myndighet det är som handlägger ärendet. För Säkerhetspolisens del rör det sig t.ex. ofta om företeelser och verksamheter där anknytningen till urskiljbara brott inte är lika tydlig som när det gäller den öppna polisens verksamhet. Säkerhetspolisens underrättelseverksamhet har således en bredare inriktning än motsvarande verksamhet hos den öppna polisen eftersom den senare är tydligare inriktad på vissa brottstyper eller brottsliga företeelser (a. prop. s. 362 f.).

Utredningen har även vid kartläggningen uppmärksammat att det varierar en del hur den brottsliga verksamheten beskrivs i beslut enligt inhämtningslagen. I vissa fall anges endast det eller de brott som verksamheten bedöms innefatta, medan besluten i andra fall innehåller mer konkreta beskrivningar. Ett exempel på det senare är t.ex. att det i beslutet anges att den brottsliga verksamheten utgörs av grovt narkotikabrott genom hantering av en viss mängd av ett angivet preparat. I vilken mån den brottsliga verksamheten kan

konkretiseras på ett sådant sätt är givetvis beroende av vilken information som finns i ärendet vid tidpunkten för beslutet.

Vi har förståelse för att det kan finnas ett behov från kontrollsynpunkt av att den brottsliga verksamheten specificeras i så hög utsträckning som möjligt i besluten. I många fall torde det dock inte vara möjligt att beskriva verksamheten särskilt mycket mer ingående än genom att ange det eller de brott som den innefattar. En ändring av det slag som SIN har föreslagit skulle innebära att detta inte längre skulle vara tillräckligt. Frågan inställer sig då om det i sådana fall inte längre är tillåtet att hämta in uppgifter enligt inhämtningslagen. En sådan ändring skulle således kunna få effekter i fråga om vilket krav på konkretion som ställs för att det ska anses vara fråga om brottslig verksamhet vilka kan vara svåra att överblicka. Krav på beskrivningar av mer konkret angiven brottslighet hör hemma på förundersökningsstadiet. Enligt vår mening är det därför inte lämpligt att föreslå någon ändring i fråga om kraven på hur den brottsliga verksamheten ska anges.

9.3.3.4 Dokumentationskrav

Bestämmelser om skyldighet att dokumentera beslut som fattas i den brottsbekämpande verksamheten ökar möjligheterna till kontroll i efterhand.

En bestämmelse om dokumentationsskyldighet i myndigheters verksamhet i stort finns i 15 § förvaltningslagen (1986:223). Enligt den bestämmelsen ska en myndighet anteckna uppgifter som den får på annat sätt än genom en handling och som kan ha betydelse för utgången i ärendet, om ärendet avser myndighetsutövning mot någon enskild. Brottsbekämpande verksamhet är emellertid undantagen från bestämmelsens tillämpningsområde (32 § förvaltningslagen).

I Förvaltningslagsutredningens betänkande SOU 2010:29 lämnas förslag till en ny förvaltningslag. Enligt förslaget ska någon motsvarighet till det nuvarande undantaget för brottsbekämpande verksamhet inte tas in i den nya lagen (a. SOU s. 123 f.). Betänkandet innehåller också förslag som syftar till att utvidga kraven på dokumentation vid myndigheternas ärendehandläggning. Syftet med förändringen är bl.a. att kravet ska omfatta inte endast sådana

uppgifter som har betydelse för det slutliga beslutet i ärendet utan även uppgifter som har betydelse för beslut under handläggningen. Enligt Förvaltningslagsutredningen skulle det till och med kunna övervägas att kräva att alla uppgifter som tillförts ett ärende muntligen eller vid syn ska dokumenteras, dvs. oberoende av om det rör sig om ett möjligt beslutsunderlag eller inte. En sådan ordning har dock tidigare avfärdats av regeringen med hänvisning till att det skulle vara allt för betungande för myndigheterna (se prop. 1985/86:80 s. 66). Utredningen framhöll i stället att det väsentliga är att inget beslut fattas utan att beslutsunderlaget finns dokumenterat och föreslog därför att kravet ska omfatta alla uppgifter som myndigheten får på annat sätt än genom en handling, om de kan ha betydelse för ett beslut i ärendet (se a. SOU s. 465 ff.).

Bestämmelsen i 5 § inhämtningslagen om vilka uppgifter som ska anges i ett beslut enligt lagen innehåller inte något krav på att de skäl som ligger till grund för beslutet ska dokumenteras i beslutet. Frågan är då om det finns anledning att ändra bestämmelsen så att det blir tydligare att så ska ske. Enligt uppgifter som utredningen har inhämtat bereds Förvaltningslagsutredningens betänkande för närvarande inom Regeringskansliet. Om de nu nämnda förslagen genomförs, kommer dokumentationsskyldigheten enligt förvaltningslagen att gälla även i de brottsbekämpande myndigheternas underrättelseverksamhet. Något ytterligare förslag om dokumentationsskyldighet skulle i sådana fall inte fylla någon större funktion. Förslaget om att brottsbekämpande verksamhet ska omfattas av den nya lagens tillämpningsområde har dock mött en hel del remisskritik (se Ds 2010:47 s. 149 ff.). Det framstår därför som osäkert om och i så fall när en sådan ordning kan träda i kraft. Utredningens förslag utgör därför inte tillräckliga skäl för att vi ska avstå från att överväga om det finns anledning att förändra dokumentationsskyldigheten enligt inhämtningslagen.

Vi delar Förvaltningslagsutredningens uppfattning att det väsentliga är att sådana omständigheter som läggs till grund för myndigheternas beslut dokumenteras. Detta är av avgörande betydelse, inte minst för att SIN:s efterhandskontroll ska kunna bedrivas så effektivt som möjligt. Av förarbetena till inhämtningslagen framgår att ett beslut om inhämtning bör läggas upp som ett särskilt inhämtningsärende där skälen för beslutet framgår (prop. 2011/12:55 s. 85). Om SIN väljer att granska ett enskilt beslut, finns alltså skälen

för åtgärden på ett eller annat sätt tillgängliga i ett ärende vid den beslutande myndigheten. Enligt uppgift från SIN visar erfarenheterna från den tid som inhämtningslagen har varit i kraft att denna ordning fungerar förhållandevis väl och att skälen för besluten i regel finns där de bör finnas. Ur SIN:s perspektiv bör alltså ingenting ändras med avseende på dokumentation av beslutsskäl. Mot den bakgrunden anser inte heller utredningen att det finns skäl att föreslå några förändringar som tar sikte på dokumentationsskyldigheten.

9.3.3.5 Tystnadsplikten enligt lagen om elektronisk kommunikation

Enligt 6 kap. 20 § LEK har den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till vissa uppgifter tystnadsplikt för dessa. Tystnadsplikten omfattar uppgift om abonnemang, innehållet i ett elektroniskt meddelande samt andra uppgifter som angår ett särskilt elektroniskt meddelande. Den omfattar också uppgifter som hänför sig till åtgärder för att hålla kvar försändelser enligt 27 kap. rättegångsbalken samt angelägenheter som avser bl.a. hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, inhämtning av uppgifter enligt inhämtningslagen eller utlämnande av uppgift om abonnemang för brottsbekämpande verksamhet (6 kap. 21 §). Operatörernas tystnadsplikt gäller även i förhållande till SIN. Detta innebär alltså att det inte är tillåtet för anställda hos operatörerna att vidarebefordra information som de får del av vid verkställighet av beslut om hemliga tvångsmedel till nämnden.

Vi har mot den bakgrunden övervägt om bestämmelserna om tystnadsplikt borde ändras i syfte att göra det möjligt för anställda hos operatörerna att vända sig till SIN för att påtala sådana felaktigheter som de eventuellt kan uppmärksamma vid verkställighet av beslut enligt inhämtningslagen. Detta skulle onekligen vara en något okonventionell lösning och det bör därför krävas starka skäl som talar för ett sådant förslag. Ett sådant skäl skulle t.ex. kunna vara att det finns anledning att förvänta sig att en möjlighet att lämna uppgifter till SIN leder till att effektiviteten i nämndens

tillsynsverksamhet förbättras. Avgörande för om en sådan möjlighet kan få den effekten är vilka iakttagelser anställda hos operatörerna eventuellt kan komma att göra i samband med verkställigheten.

Den information som operatörerna får del av i samband med beställningar av uppgifter är begränsad till i huvudsak information om vilken lagstiftning som ligger till grund för beställningen och sådana uppgifter som är nödvändiga för att ett beslut ska kunna verkställas. När det t.ex. gäller beställningar av historiska trafikuppgifter får operatören reda på om begäran avser ett beslut om hemlig övervakning av elektronisk kommunikation eller ett beslut enligt inhämtningslagen. Därutöver lämnas information om vilken teleadress eller vilken elektronisk kommunikationsutrustning beslutet avser, vilka uppgifter operatören ska lämna ut (t.ex. uppgifter om meddelanden till eller från ett visst telefonnummer) samt vilken tidsperiod beställningen gäller. Dessutom ska ett referensnummer på ärendet anges. Någon information om vilket brott eller vilken brottslig verksamhet som ligger till grund för beslutet lämnas dock inte. Inte heller lämnas någon information om syftet med åtgärden.

Möjligen kan man tänka sig att en anställd hos en operatör utifrån denna information skulle kunna uppmärksamma om en beställning enligt inhämtningslagen avser inhämtning av trafikuppgifter i realtid vilket inte är tillåtet enligt lagen. Denna information skulle således kunna vidarebefordras till SIN. Enligt uppgift från SIN är detta emellertid ett förhållande som nämnden i sådana fall ändå skulle uppmärksamma genom myndigheternas underrättelser till nämnden.

I övrigt är det enligt vår mening svårt att se vad anställda hos operatörerna – med utgångspunkt i de begränsade uppgifter de får del av – skulle kunna komma att reagera på. Utan tillgång till uppgifter om vilken brottslighet en begäran gäller eller vilket syfte den har är det t.ex. inte möjligt att bedöma om inhämtningen är tillåten enligt den lagstiftning som åberopas. Inte heller är det möjligt att ta ställning till frågor om proportionalitet och liknande. Det är givetvis inte heller operatörernas uppgift att göra den typen av bedömningar.

SIN har mot den angivna bakgrunden ställt sig tveksam till en ordning av det slag som nu diskuteras. Nämnden har också påtalat att uppgifter förmodligen i många fall skulle komma att lämnas rätt formlöst, vilket kan innebära risker för att känslig information

sprids på ett olämpligt sätt. Detta kan få negativa konsekvenser både för myndigheternas underrättelsearbete och för t.ex. källor.

Av dessa skäl bedömer vi att en lättnad av tystnadsplikten enligt LEK i förhållande till SIN inte skulle fylla någon större funktion. Som framgått kan det också finnas vissa risker förknippade med en sådan ordning. Sammantaget anser vi därför att det inte finns tillräckliga skäl för att föreslå någon ändring av bestämmelserna om tystnadsplikt i LEK.

9.4 Säkerhetspolisens behov av en särskild möjlighet att inhämta uppgifter om viss brottslig verksamhet

9.4.1 Nuvarande ordning

Enligt inhämtningslagens huvudregel får uppgifter hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, under förutsättning skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse (2 §). Under samma förutsättningar får uppgifter också hämtas in om den brottsliga verksamhet som åtgärden syftar till att förebygga, förhindra eller upptäcka innefattar vissa särskilt angivna brott med lägre straffminimum än fängelse i två år (3 §). De brott som omfattas av bestämmelsen är:

1. sabotage enligt 13 kap. 4 § brottsbalken,
2. kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
3. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,
4. spionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5 eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken, eller

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

Bestämmelsen i 3 § är tidsbegränsad och upphör att gälla vid utgången av 2016.

9.4.2 Tidigare överväganden

Regeringen anförde följande i förarbetena till inhämtningslagen (prop. 2011/12:55 s. 86 f.).

> Säkerhetsunderrättelseverksamheten vid Säkerhetspolisen skiljer sig från den övriga polisverksamheten bl.a. på så sätt att Säkerhetspolisens uppdrag främst är inriktat på att förhindra brott och i mindre utsträckning på att utreda brott som redan har begåtts. För att kunna förhindra särskilt samhällsfarlig brottslighet har Säkerhetspolisen därför i vissa fall, som utredningen har konstaterat, ett särskilt behov av tillgång till övervakningsuppgifter i ett tidigt skede även då den brottsliga verksamheten inte innefattar brott med ett minimistraff om två års fängelse. Ingen remissinstans har invänt mot den bedömningen.
>
> Frågan är då vid vilka brott en sådan inhämtning ska vara möjlig. Som framgår ovan har utredningen föreslagit att inhämtning ska kunna ske vid brottslig verksamhet som innefattar något av de brott som kan föranleda hemlig teleövervakning enligt 2008 års tvångsmedelslag. Även i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott finns en brottskatalog som upptar vissa brott vid vilka hemlig teleövervakning under särskilda förutsättningar är möjlig, trots att förutsättningarna för inhämtning enligt rättegångsbalken inte är uppfyllda. Vid en jämförelse mellan de båda lagarna kan det konstateras att det för vissa av de brott för vilka hemlig teleövervakning kan beslutas i en förundersökning enligt 2008 års lag inte finns någon motsvarande möjlighet i underrättelseskedet enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Detta gäller bl.a. olovlig kårverksamhet. Båda dessa lagar är som tidigare sagts tidsbegränsade till utgången av år 2013 och föremål för utvärdering (dir. 2010:62). Möjligheten att enligt den nu föreslagna lagen inhämta uppgifter i fråga om den aktuella brottsligheten bör mot den bakgrunden tills vidare begränsas till att avse de brott som omfattas av båda dessa lagar och ges samma giltighetstid som dem. Sedan utredningen lämnat sitt betänkande har lagen om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig

> brottslighet trätt i kraft. Grovt brott enligt 6 § den lagen omfattas numera av regleringen i såväl 2008 års tvångsmedelslag som lagen om åtgärder för att förhindra vissa särskilt allvarliga brott.
>
> Även det brottet bör enligt regeringen omfattas av den reglering som nu föreslås. Frågan om Säkerhetspolisens fortsatta tillgång till övervakningsuppgifter för tiden efter utgången av år 2013 bör övervägas i det sammanhang som en framtida reglering av hemliga tvångsmedel för särskilt allvarlig eller samhällsfarlig brottslighet övervägs.

Mot den bakgrunden fick utredningen om vissa hemliga tvångsmedel i uppdrag att analysera Säkerhetspolisens behov av att i underrättelseverksamhet kunna inhämta uppgifter om elektronisk kommunikation för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar vissa samhällsfarliga brott med ett lägre straffminimum än två års fängelse (dir. 2012:9). Utredningen, som lämnade sitt betänkande i juni 2012, gjorde bedömningen att det bör finnas en permanent möjlighet enligt inhämtningslagen att hämta in uppgifter om vissa brott inom Säkerhetspolisens verksamhetsområde vilka inte har ett straffminimum som uppgår till två års fängelse. När det gäller vilka brott som skulle omfattas av bestämmelsen uttalade utredningen att den gjorde samma bedömning som den hade gjort i fråga om 2007 års lag om preventiva tvångsmedel. Detta innebar att utredningen föreslog att inhämtningslagens 3 § skulle utökas till att – även när dessa inte är grova brott – omfatta även obehörig befattning med hemlig uppgift, olovlig underrättelseverksamhet, s.k. terrorismfinansiering och brott enligt lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet. Vidare föreslog utredningen att s.k. statsstyrt företagsspionerі skulle läggas till bestämmelsen (se SOU 2012:44 s. 629 ff.).

I den efterföljande propositionen konstaterade regeringen att inhämtningslagen inte omfattades av den kartläggning av vissa andra hemliga tvångsmedel som utredningen hade genomfört. Enligt regeringen borde den hittillsvarande tillämpningen av lagen kartläggas och analyseras ytterligare innan slutlig ställning tas till hur Säkerhetspolisens behov av övervakningsuppgifter i underrättelseverksamhet bör tillgodoses. Av den anledningen ansåg regeringen att det, i avvaktan på en sådan kartläggning och analys, inte borde göras några förändringar i inhämtningslagen. Däremot föreslog regeringen

att bestämmelsens giltighetstid skulle förlängas till utgången av 2016 (prop. 2013/14:237 s. 116).

9.4.3 Säkerhetspolisens behovsbeskrivning

Säkerhetspolisen har uppgett i huvudsak följande i fråga om myndighetens behov av en möjlighet att hämta in uppgifter om brottslig verksamhet som innefattar brott med lägre minimistraff än fängelse två år.

De brott som i dagsläget omfattas av bestämmelsen i 3 § inhämtningslagen får anses vara särskilt allvarliga för rikets säkerhet. De aktörer som Säkerhetspolisen följer har alla en förmåga att begå de typer av brott som finns omnämnda i paragrafen. Vissa av dessa aktörer har därutöver en faktisk och potentiell avsikt att begå dessa brott.

När det gäller de brott som nämns i den första och andra punkten (sabotage, kapning m.m.) så har ideologiskt motiverade aktörer i dag en bred agenda. Säkerhetspolisen förhåller sig till dessa aktörer, vilka bl.a. innefattar den autonoma miljön, vitmakt-miljön, djurrättsaktivister, miljörättsaktivister, Counter Jihad rörelsen och enfrågerörelser som riktar sig mot exempelvis migrationsfrågor. Säkerhetspolisen har exempelvis kunnat konstatera att några av dessa aktörer varit föremål för förundersökning vad avser bland annat flygplatssabotage. Det finns också anledning att anta att aktörer som kopplas till våldsbejakande religiös extremism kan ha avsikt och förmåga att begå dessa brott. Detta betyder inte att Säkerhetspolisen haft anledning att inhämta uppgifter enligt dessa punkter i paragrafen, men det finns aktörer som potentiellt kan tänkas begå denna typ av brott i syfte att uppnå sina mål.

När det gäller brott mot medborgerlig frihet (tredje punkten) så bedriver Säkerhetspolisen ett omfattande arbete i syfte att förhindra att politiskt eller ideologiskt motiverade aktörer begår allvarlig eller systematisk otillåten påverkan mot viktiga samhällsfunktioner. Förtroendevalda, myndighetspersoner och journalister är en faktisk och potentiell måltavla bl.a. för våldsbejakande aktörer i den autonoma miljön och vitmakt-miljön. En relativt stor mängd brott begås mot sådana funktioner främst i syfte att påverka den allmänna åsiktsbildningen eller inkräkta på handlingsfriheten inom viss poli-

tisk organisation. Säkerhetspolisen har ett stort behov av att kartlägga dessa grupperingar i syfte att förhindra och förebygga sådan brottslighet.

Vad avser brott som räknas upp i den fjärde punkten (spioneri m.m.) har Säkerhetspolisen anfört att underrättelseverksamhet mot Sverige och svenska intressen pågår ständigt och är både långsiktig och systematisk. Aktörer som bedriver olaglig underrättelseverksamhet använder ofta täckmantel och utger sig ofta för att vara diplomater, journalister eller affärsmän. Dessa underrättelseofficerare använder sig regelmässigt av andra människor, agenter, för att få ut hemliga uppgifter från myndigheter eller företag. Säkerhetspolisen motverkar främmande underrättelseverksamhet dels genom att följa upp kända underrättelseaktörer och hot, dels genom att leta efter hittills okända hot. Genom detta säkerhetsunderrättelsearbete ges stöd för bedömningar av hot och sårbarheter. Säkerhetspolisen har således ett stort behov av att kartlägga de aktörer som kan utgöra underrättelseofficerare eller agenter och som kan utgöra ett hot mot rikets säkerhet. Inhämtningslagen är ett mycket viktigt verktyg i arbetet att kartlägga dessa aktörer innan brott begås som kan få allvarliga konsekvenser för Sverige.

Brotten under punkten fem (terrorismfinansiering m.m.) är enligt Säkerhetspolisen stödverksamhet till sådana aktörer som har avsikt och förmåga att begå terroristattentat. Det är därför av stor vikt att Säkerhetspolisen har en förmåga att kartlägga dessa aktörer i syfte att förhindra och förebygga att sådan verksamhet leder till terroristbrott i eller utanför Sverige. Den senaste utvecklingen i omvärlden, inte minst i Syrien och Irak, gör att Säkerhetspolisen har ett stort behov av att kartlägga aktörer eller nätverk som skapar finansiella förutsättningar, rekryterar eller uppmanar aktörer att begå sådan brottslighet.

Vidare har Säkerhetspolisen framfört att det finns behov av att kunna hämta in uppgifter om vissa brott som i dagsläget inte omfattas av bestämmelsen i 3 § inhämtningslagen. De brott som angetts är s.k. statsstyrt företagsspioneri samt grov misshandel och olaga frihetsberövande som begås i systemhotande syfte. Beträffande statsstyrt företagsspioneri har Säkerhetspolisen pekat på att myndigheten känner till att stater i omvärlden ger sina underrättelseorgan i uppdrag att på laglig och olaglig väg hämta in underrättelser om teknik och vetenskap i syfte att gynna det egna näringslivet. Även om skade-

rekvisitet enligt nuvarande spioneribestämmelse (men för Sveriges säkerhet) saknas när det gäller statsstyrt företagsspioneri som bedrivs av konkurrensskäl, finns det en påtaglig negativ, om än indirekt, effekt. Sveriges ekonomiska säkerhet kan skadas. På lång sikt kan det svenska näringslivets konkurrenskraft urholkas och Sveriges attraktionskraft som investeringsland minska vilket i ett litet, starkt exportberoende land som Sverige får konsekvenser för det framtida välståndet. Just inom det försvarsmateriella området förekommer misstänkt statsstyrt spioneri mot företag, bl.a. i syfte att vinna upphandlingar.

Mot denna bakgrund är det viktigt att Säkerhetspolisen ges möjligheter att använda inhämtningslagen för att dels i underrättelseverksamhet leta efter statsstyrt företagsspioneri, dels så tidigt som möjligt kunna kartlägga om främmande makt eller renodlat kommersiella aktörer ligger bakom spioneriet.[3]

Vad gäller grov misshandel och olaga frihetsberövande som begås i s.k. systemhotande syfte (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) har Säkerhetspolisen framfört samma skäl som när det gäller brott mot medborgerlig frihet (se ovan).

9.4.4 Utredningens förslag

Utredningens förslag: Inhämtningslagens bestämmelse om inhämtning av uppgifter om brottslig verksamhet som innefattar vissa brott med lägre minimistraff än fängelse i två år ska göras permanent. Möjligheten att hämta in uppgifter ska gälla de brott som den omfattar i dagsläget. Därutöver ska den gälla även s.k. statsstyrt företagsspioneri samt grov misshandel och olaga frihetsberövande som begås 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.

[3] Enligt Säkerhetspolisen var en av huvudfrågorna i det s.k. SAAB-målet (Göteborgs tingsrätts dom den 10 november 2008 i mål nr B 7226-08) huruvida främmande makt låg bakom eller om gärningsmännen agerade ensam.

De brott som i dagsläget omfattas av bestämmelsen i 3 § inhämtningslagen är sådana som har ansetts vara särskilt allvarliga eftersom de är samhällsfarliga, dvs. de hotar direkt eller indirekt vitala samhällsintressen. Beträffande flera av brotten har dessutom framhållits att de regelmässigt är svåra att utreda. Behovet av att använda olika hemliga tvångsmedel för att utreda brotten har därför ansetts vara särskilt stort (se t.ex. prop. 2013/14:237 s. 81). Vi gör inte någon annan bedömning. Av vår kartläggning framgår också att tillämpningen av inhämtningslagen har lett till beaktansvärd nytta i samband med underrättelsearbete avseende brottslig verksamhet som innefattar flera av de aktuella brotten. Enligt utredningens uppfattning bör därför möjligheten att inhämta uppgifter om brottslig verksamhet som innefattar dessa brott finnas kvar.

Av Säkerhetspolisens uppgifter framgår att myndigheten dessutom har ett behov av att kunna hämta in uppgifter om brottslig verksamhet som innefattar s.k. statsstyrt företagsspionerі och vissa brott med systemhotande syfte.

Statsstyrt företagsspionerі innebär att främmande makt bedriver spionage mot svenska företag med avsikt att få tillgång till företagshemligheter. Till skillnad från traditionellt spionage, som syftar till att underminera ett lands säkerhet är företagsspionerіets motiv främst att skaffa ekonomisk vinning och inhämta teknisk kunskap. Som framgår av Säkerhetspolisens beskrivning kan sådant spionerі få allvarliga konsekvenser för svenska företag och i förlängningen kan viktiga svenska samhällsintressen som är avgörande för vårt välstånd drabbas. Brottsligheten kan även försämra förutsättningarna att utveckla och upprätthålla skyddet för landets säkerhet. Civil forskning har fått allt större betydelse för att driva teknikutvecklingen och även för att ta fram teknik som kan användas i militära syften. Exempel på detta är bioteknisk forskning som kan användas för att utveckla och tillverka biologiska och kemiska massförstörelsevapen. Bland annat av den anledningen har regeringen nyligen gjort bedömningen att statsstyrt företagsspionerі är så allvarligt att såväl hemlig rumsavlyssning som tvångsmedel enligt lagen om preventiva tvångsmedel bör tillåtas för att bekämpa brottet (se prop. 2013/14:237 s. 89 och 114 f.). Vidare är de personer som deltar i spioneriverksamhet ofta välutbildade underrättelseofficerare som tränats och dessutom understöds av främmande makt. Dessa personer är i allmänhet mycket säkerhetsmedvetna vilket gör brottslig-

heten svår att upptäcka och förhindra. Det står således klart att det finns ett stort behov av att kunna inhämta uppgifter enligt inhämtningslagen beträffande brottslig verksamhet som innefattar statsstyrt företagsspionerі.

Ytterligare ett skäl som talar för att inhämtningsmöjligheten bör omfatta även statsstyrt företagsspionerі är att det kan vara svårt, särskilt i ett tidigt skede, att i praktiken dra en klar gräns mellan detta brott och traditionellt spionerі (se prop. 2007/08:163 s. 55).

När det sedan gäller grov misshandel och olaga frihetsberövande som begås med ett systemhotande syfte framgår av Säkerhetspolisens uppgifter att ett relativt stort antal brott begås mot förtroendevalda, myndighetspersoner och journalister främst i syfte att påverka eller hämnas framtida eller genomförda myndighetsbeslut eller nyhetsrapportering och fokusering. Det saknas anledning att ifrågasätta att Säkerhetspolisens har ett stort behov av att kunna kartlägga grupperingar som har avsikt och förmåga att begå sådan brottslighet. Den aktuella brottsligheten är också mycket allvarlig eftersom den syftar till att påverka de aktuella personerna i utövandet av deras samhällsfunktioner. På så sätt utgör brottsligheten ett hot mot vårt demokratiska system. Det är därför av största vikt att den effektivt kan förebyggas och förhindras.

Det finns också vissa systematiska skäl för att statsstyrt företagsspionerі och de systemhotande brotten ska läggas till i katalogen. Dessa brott omfattas av lagen om preventiva tvångsmedel. Detta innebär att det är möjligt att, redan i ett skede innan förundersökning har inletts, använda de betydligt mer integritetskänsliga tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. Det är därför såväl rimligt som logiskt att de nu aktuella brotten omfattas även av den särskilda inhämtningsmöjligheten enligt inhämtningslagen.

En fråga som emellertid kan ställas är om Säkerhetspolisens behov av övervakningsuppgifter i underrättelseverksamheten i tillräcklig utsträckning uppfylls genom möjligheten till hemlig övervakning av elektronisk kommunikation enligt lagen om preventiva tvångsmedel. Som utredningen om vissa hemliga tvångsmedel tidigare har konstaterat skiljer sig emellertid rekvisiten för att myndigheterna ska få tillgång till information väsentligt mellan de två lagarna. En viktig skillnad är att det i inhämtningslagen – till skillnad från i lagen om preventiva tvångsmedel – inte finns något krav på att inhämtningen

ska kunna kopplas till en viss person. Informationsinhämtning utan ett krav på koppling till en viss person är särskilt ägnad att tillgodose vissa behov hos Säkerhetspolisen, t.ex. att ”identifiera det okända hotet” genom att identifiera okända aktörer och bedöma vilket hot de utgör (SOU 2012:44 s. 630). Att det förhåller sig på det sättet stöds även av det som har kommit fram under vår kartläggning. Lagen om preventiva tvångsmedel är inte heller något allmänt underrättelseverktyg, utan när den lagen tillämpas är det uteslutande i situationer där det handlar om att förhindra att en på visst sätt konkretiserad risk förverkligas.

Mot den angivna bakgrunden bedömer vi att behovet av en möjlighet att hämta in uppgifter enligt inhämtningslagen inte påverkas i någon större utsträckning av att lagen om preventiva tvångsmedel innehåller en möjlighet att använda hemlig övervakning av elektronisk kommunikation beträffande de aktuella brotten.

Sammanfattningsvis anser vi att behovet av att kunna hämta in uppgifter om brottslig verksamhet som innefattar statsstyrt företagsspionerі och de systemhotande brotten väger tyngre än integritetsintresset hos de personer som kan komma att drabbas av inhämtningen. Vi föreslår därför att de aktuella brotten ska omfattas av den särskilda inhämtningsmöjligheten enligt inhämtningslagen.

Det har inte kommit fram någonting under utredningens kartläggning som tyder på att Säkerhetspolisens behov av en särskild inhämtningsmöjlighet avseende den nu behandlade brottsligheten skulle minska inom överskådlig tid. Inte heller i övrigt har det kommit fram något som ger skäl att anta att de sakförhållanden som ligger till grund för utredningens ställningstaganden är av tillfällig natur. Utredningen anser därför att den nu behandlade möjligheten att inhämta uppgifter om brott med lägre minimistraff än två års fängelse inte bör vara tidsbegränsad.

10 Övriga frågor

10.1 Tystnadsplikt för kvarhållande av försändelse enligt lagen om preventiva tvångsmedel

Utredningens förslag: En uttrycklig regel införs i postlagen om att den som i postverksamhet har fått del av eller tillgång till en uppgift som handlar om att undersöka, öppna, granska eller kvarhålla en försändelse enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott har tystnadsplikt för uppgiften.

Leverantörer av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster har tystnadsplikt för uppgifter som hänför sig till verkställandet av beslut om hemliga tvångsmedel (6 kap. 20 och 21 §§ LEK). Tystnadsplikten innebär att leverantören som huvudregel inte obehörigen får föra vidare eller utnyttja det som han eller hon fått del av eller tillgång till. En liknande regel finns i 2 kap. 14 § postlagen. Enligt den bestämmelsen får den som i postverksamhet har fått del av eller tillgång till bl.a. uppgifter som handlar om att kvarhålla eller beslagta försändelser enligt 27 kap. rättegångsbalken inte obehörigen röja eller utnyttja vad han eller hon därigenom har fått veta. Under utredningens arbete har det uppmärksammats att motsvarande bestämmelse saknas beträffande kvarhållande och kontroll av försändelse enligt lagen om preventiva tvångsmedel.

När det gäller hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation och hemlig kameraövervakning så hänvisar lagen om preventiva tvångsmedel till rättegångsbalkens bestämmelser om dessa tvångsmedel. Det är därför inte nödvändigt med några särskilda bestämmelser om tystnadsplikt för uppgifter om sådana åtgärder enligt lagen eftersom åtgärderna alltså omfattas av den tystnadsplikt som gäller för samma åtgärder enligt rättegångsbalken. Lagens regler om kvarhållande och

kontroll av försändelse innehåller däremot inte någon motsvarande hänvisning till rättegångsbalken, och det är därför tveksamt om postlagens regler om tystnadsplikt kan anses gälla för dessa åtgärder.

När lagen om preventiva tvångsmedel infördes uttalade regeringen att reglerna om kvarhållande och kontroll av försändelse bör utformas så att avsändaren och mottagaren normalt inte får kännedom om postkontrollen (prop. 2005/06:177 s. 50 f.). Det är mot den bakgrunden tydligt att avsikten var att det skulle gälla tystnadsplikt för dessa åtgärder på samma sätt som för postkontroll enligt rättegångsbalken. En sådan ordning är både logisk och rimlig. Någon bestämmelse om tystnadsplikt kom dock aldrig att införas i postlagen. Av allt av att döma berodde detta på ett rent förbiseende.

Regler om tystnadsplikt bör givetvis utformas på ett sådant sätt att det inte råder någon tvekan om vilka uppgifter som omfattas av tystnadsplikten. Vi föreslår därför att bestämmelsen i 2 kap. 14 § första stycket postlagen kompletteras med en uttrycklig bestämmelse om att tystnadsplikten omfattar även sådana åtgärder som vidtas med stöd av 4 § lagen om preventiva tvångsmedel. Detta leder också till att en följdändring bör göras i 44 kap. 4 § offentlighets- och sekretesslagen (2009:400).

10.2 Ekobrottsmyndighetens behov av en möjlighet att hämta in uppgifter enligt inhämtningslagen

Ekobrottsmyndigheten har framfört till utredningen att myndigheten har ett behov av en möjlighet att hämta in uppgifter enligt inhämtningslagen. Myndigheten har beskrivit detta behov på följande sätt.

> Enligt Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet får Polismyndigheten, Tullverket och Säkerhetspolisen inhämta uppgifter om elektronisk information i ett underrättelseskede. Detta om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Grovt bokföringsbrott och grovt skattebrott uppnår inte denna miniminivå då lägsta straff är sex månaders fängelse. Därav kan inte en sådan inhämtning utföras i nuläget. Ekobrottsmyndighetens underrättelseverksamhet har dock ett behov av en sådan inhämtning för en effektiv och rättssäker utredningsprocess.

Grunden för detta behov listas nedan.

- Ekonomisk brottslighet har ofta en nära koppling till systemhotande grov och organiserad brottslighet. Personer inom grov och organiserad brottslighet tenderar att i större utsträckning ägna sig åt ekonomisk brottslighet och det finns stora möjligheter att med rätt förutsättningar kunna lagföra dem för ekonomiska brott. En ökad möjlighet att kartlägga dessa personer ökar möjligheten till lagföring av personerna i fråga.
- Såväl grova skatte- och bokföringsbrott som grov oredlighet har relativt höga straffmaximum och betraktas av rättsordningen som allvarlig brottslighet.
- Brotten begås ofta systematiskt och avser många brottsmisstankar med omfattande skatteundandraganden.
- Ekonomiska brottslingar samarbetar ofta i nätverk. För att identifiera de kontakter som finns inom nätverken är kartläggning via telefonlistor av signifikant betydelse. Att upptäcka kontaktnätverk och kartlägga dess förgreningar genom traditionell spaning är i princip omöjligt. Eftersom personer idag vanligen sköter sina kontakter via telefon eller mail är det svårt att utan trafikdata, genom traditionell spaning, uppnå tillräckliga skäl för att inleda förundersökning. Underrättelseärendena tenderar då istället att fokusera isolerat på individer som det redan finns uppgifter om. Det är ofta frågan om mindre centrala aktörer som mot ersättning utför vissa centrala uppgifter. Andra – ofta mer relevanta personer – undgår då upptäckt.
- De personer som Ekobrottsmyndigheten utreder kan vara personer som utför kriminella handlingar eller hjälper andra att utföra desamma inom ramen för sina ordinarie arbetsuppgifter, t.ex. genom att övervärdera fastigheter, bevilja lån på osäkra grunder, bistå med ekonomisk rådgivning eller hantera misstänkta penningtransaktioner utan att anmäla misstänkt penningtvätt. Dessa personer fungerar ofta som ”spindeln i nätet”. För att kunna kartlägga deras kontaktnät och därefter besluta om andra åtgärder är elektronisk inhämtning central.
- De grundläggande punkterna för telefonanalysen i ett underrättelseskede bedöms vara geografisk lokalisering, kontaktmönster och identifiering av för myndigheten eventuella okända viktiga aktörer, modus och för att hitta nya vägar.

- En ökad möjlighet till elektronisk inhämtning ger möjlighet att få mer konkretiserade uppgifter om exempelvis faktiska företrädare, rörelsemönster, kontakter, såväl fasta som mer adhoc-kontakter, mellan aktörer eller meddelandeinformation om faktiska brott. Olika individers roller och inblandning i en verksamhet kan klargöras. Exempelvis kan detta användas i underrättelseärenden avseende punktskattebrott där en kartläggning av vilka som vistats i närheten av ett skatteupplag hade kunnat uppdaga fler misstänkta eller huvudmännen.
- Det är viktigt att framhålla att inhämtning av trafikdata också kan användas i syfte att kunna avskriva personer som inte är intressanta. Exempelvis kan vi ha fått indikatorer via källor om att personer begår ekonomisk brottslighet. Om inte slagningar och inre spaning kan avfärda detta kan elektronisk inhämtning vara enda möjligheten att verifiera eller förkasta sådana uppgifter.
- Ett mål för Ekobrottsmyndigheten, tillsammans med många andra myndigheter, är återvinning av brottsutbyte. Användandet av målvakter, elektroniska valutor eller andra hjälpmedel för att dölja penningtransaktioner samt bolag där vinsterna hanteras utgör ett stort hinder i att skaffa information som möjliggör ett framgångsrikt arbete med återvinning av brottsutbyte. Det är helt enkelt mycket svårt att fysiskt följa pengarnas väg, elektronisk information kan användas exempelvis till att lokalisera fastigheter/bostäder.

Utifrån Ekobrottsmyndighetens beskrivning – och utifrån de uppgifter som genom vår kartläggning har kommit fram i fråga om hur inhämtningslagen används och vilken nytta den leder till i den brottsbekämpande verksamheten – är det inte svårt att se att en möjlighet att hämta in uppgifter enligt inhämtningslagen skulle kunna vara till stor nytta även i Ekobrottsmyndighetens verksamhet. Det ingår emellertid inte i vårt uppdrag att överväga den typen av förändringar i lagens tillämpningsområde. Enligt utredningens uppfattning kan det dock finnas anledning att överväga den frågan i ett annat sammanhang.

10.3 Brottslig verksamhet som innefattar spridning av massförstörelsevapen

Säkerhetspolisen har påtalat att det finns ett behov av att kunna hämta in uppgifter enligt inhämtningslagen i underrättelsearbete avseende brottslig verksamhet som innefattar vissa brott mot lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd (PDA-lagen) och mot lagen (1996:95) om vissa internationella sanktioner. Myndigheten har utvecklat detta behov enligt följande.

> Säkerhetspolisen har i uppdrag att förhindra spridning och anskaffning av produkter, kunskaper och ämnen från Sverige eller via Sverige som kan användas av stater eller ickestatliga aktörer för utveckling av massförstörelsevapen. I uppdraget ingår även att förhindra finansiering av sådan spridning samt att förhindra att svensk spetskompetens används för att utveckla massförstörelsevapen i andra länder.
>
> Ickespridning är internationellt sett en högt prioriterad verksamhet och anses vara en global angelägenhet. Sverige har sedan 1945 arbetat mycket aktivt internationellt för rustningskontroll och nedrustning. Detta har kunnat ske mot bakgrund av en djupgående teknisk kunskap om massförstörelsevapen. Men den utrikespolitiska retoriken har inte åtföljts av motsvarande ansträngningar att från Sverige förhindra utflödet av känsliga eller hemliga kunskaper, produkter eller ämnen. I ett internationellt perspektiv har Sverige låga straffsatser för brott mot lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd (PDA-lagen) samt lagen (1996:95) om vissa internationella sanktioner, vilket gör att Sverige blir en attraktivt och sårbart för olika länders anskaffningsverksamhet. I Sverige kan de rättsvårdande myndigheterna inte ens få tillgång till telefonavlyssning eller andra hemliga tvångsmedel (pga. för låga straffsatser) för att förhindra att proliferatörer[1] skaffar sig komponenter för att bygga exempelvis kärnvapen. Detta är oacceptabelt i en tid då FN, EU m.fl. talar om massförstörelsevapen och terrorister som ett av de största hoten mot världens säkerhet.
>
> Den svaga svenska lagstiftningen får flera konsekvenser. För det första har Säkerhetspolisen observerat att proliferatörer dras till Sverige i takt med att andra stater skärper sina lagstiftningar, dvs. anskaffningsverksamheten i Sverige ökar trots en politisk vilja i motsatt riktning. Sveriges relativa andel i bidraget till uppbyggnaden av andra staters massförstörelsevapenprogram ökar därmed. För det andra har inter-

[1] Proliferatör = en person som illegalt anskaffar produkt alternativt kunskap som senare nyttjas i ett massförstörelsevapenprogram.

nationella samarbetspartner uppmärksammat detta. Det medför en påtaglig risk att även samarbetspartner kommer att bedriva olaglig underrättelseverksamhet i Sverige för att på egen hand stoppa utflödet ur Sverige, dvs. den olagliga underrättelseverksamheten i Sverige riskerar att öka trots att Säkerhetspolisen har i uppdrag att minska densamma. För det tredje riskerar Sverige att få dåligt rykte internationellt när det blir alltmer uppenbart att Sverige i realiteten inte lever upp till sina internationella åtaganden och den deklarerade politiken.

En viktig del av ickespridningsarbetet är även att förhindra finansiering av spridning av produkter från och via Sverige. Otillåten anskaffning bedrivs idag oftast med hjälp av aktörer som har ett eget vinningssyfte och inte nödvändigtvis drivs av ideologiska skäl. Sveriges låga straffsatser gör att möjligheten till ekonomisk vinning överväger risken för lagföring.

Sverige har en hög teknologisk nivå inom civil och militär industri. Med anledning av detta är svenska företag och lärosäten attraktiva för länder som vill framställa massförstörelsevapen. Från Sverige försöker flera länder skaffa produkter och kunskap till stöd för egen forskning och utveckling samt tillverkning av kärnvapen, biologiska vapen, kemiska vapen samt bärare av dylika vapen, dvs. missiler. I denna typ av verksamhet nyttjas olika länders underrättelseorganisationer eller andra statliga eller kommersiella strukturer kopplade till staten och dess underrättelsetjänst. Andra staters underrättelsetjänst samt motsvarande icke-statliga aktörer arbetar för att kringgå internationella sanktioner i syfte att komma åt de produkter de behöver för att utveckla massförstörelsevapen.

Säkerhetspolisen har idag otillräckliga egna verktyg att i ett tidigt skede upptäcka och motverka otillåten anskaffning. Säkerhetspolisen måste i alltför hög grad förlita sig på information från samverkande underrättelseorganisationer i andra länder. Vidare har Säkerhetspolisen begränsade möjligheter att med hjälp av signalspaning inhämta information avseende anskaffningsnätverk och deras verksamhet i Sverige. Säkerhetspolisen har behov av att öka den egna underrättelseförmågan i syfte att förebygga och förhindra denna typ av brottsliga handlingar samt att kartlägga de aktörer som bedriver sådan brottslig verksamhet i Sverige. Säkerhetspolisen bedömer att inhämtningslagen ett mycket viktigt verktyg i arbetet att kartlägga dessa aktörer innan brott begås som kan få allvarliga konsekvenser för Sverige eller omvärlden.

Proliferation är att betrakta som vilken annan form av spionerі som helst, men omfattas idag inte av BrB 19 kap. Aktörerna och deras tillvägagångssätt är desamma som vid andra former av spionerі. Vid översynen av spionerilagstiftningen 2010–2012 framförde Säkerhetspolisen ett behov av att inkorporera proliferationsbrottet i spionerilagstiftningen. Alla rekvisit enligt BrB 19 kap 5 § är uppfyllda (uppsåt att gå

främmande makt tillhanda, inhämtning av öppna, känsliga eller hemliga uppgifter etc.) utom ett. Det är som regel mycket svårt att påvisa ett direkt men för Sveriges säkerhet. Stöld av exempelvis en vakuumpump kan inte hänföras till ett sådant men. Men indirekt kan effekterna vara högst påtagliga: ökat svenskt bidrag till uppbyggnad av massförstörelsevapen som kan utnyttjas för att hota andra stater, bedömd ökad olaglig underrättelseverksamhet i Sverige när svenska myndigheter inte har egen förmåga att motverka utflöde av kunskaper, produkter eller ämnen samt försämrat internationellt anseende.

Den enda lagstiftning som finns att tillgå i dag är

- Brott mot 18–22 §§ lag (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd.
- Brott mot 8–9 §§ lag (1996:95) om vissa internationella sanktioner.

Brottslig verksamhet som innebär att någon sprider produkter, kunskaper och ämnen i syfte att dessa ska användas för att framställa massförstörelsevapen är uppenbarligen mycket allvarlig. Av Säkerhetspolisens beskrivning framgår vidare att det finns ett stort behov av att öka myndighetens egen underrättelseförmåga när det gäller sådan brottslighet. Mot bakgrund av vad som kommit fram vid vår kartläggning finns det mycket som talar för att en möjlighet att hämta in uppgifter enligt inhämtningslagen skulle kunna vara till stor nytta vid bekämpning av brottsligheten.

Frågor om hur intresset av en effektiv brottsbekämpning bör balanseras mot integritetsintresset i reglerna om hemliga tvångsmedel kräver noggranna överväganden. Frågan om inhämtningslagens användningsområde bör utökas med något eller några av de aktuella brotten har väckts i ett sent skede av utredningen. Av den anledningen har vi inte haft möjlighet att tillräckligt noggrant överväga alla de frågor som skulle behöva övervägas, innan ett förslag i den riktningen eventuellt skulle kunna lämnas. Exempelvis har vi inte haft tillräcklig möjlighet att analysera vilka effekter ett sådant förslag skulle kunna få för enskildas personliga integritet. Inte heller har vi haft tillräcklig tid för att göra de bedömningar som krävs i fråga om vilka av de aktuella brotten som i sådana fall bör omfattas av möjligheten. Av dessa skäl har vi valt att inte föreslå några förändringar i den här delen. Enligt vår uppfattning finns det emellertid starka skäl som talar för att frågan bör övervägas vidare.

10.4 NAT-teknik

Network Address Translation (NAT) är en teknik som gör det möjligt att ansluta många datorer/terminaler till internet med användning av en eller några få gemensamma publika ip-adresser. NAT är en funktion som vanligen byggs in i en brandvägg eller router som ansluter ett lokalt nätverk till internet. I det lokala nätverket används ip-adresser reserverade för detta ändamål, som inte kan användas på det öppna publika nätet (s.k. privata adresser eller svarta adresser).

NAT-tekniken används vanligen av privatpersoner och företag, som kopplar upp sitt lokala nätverk mot internet. På grund av brist på ip-adresser enligt den ursprungliga standarden (IPv4) så har emellertid NAT även kommit att användas av internetleverantörer, för att de tillgängliga ip-adresserna ska räcka till att koppla upp alla abonnenter. När internetleverantörer använder NAT kallas detta vanligen för Carrier Grade NAT (CGN) eller Large Scale NAT (LSN).

Såväl Polismyndigheten som Säkerhetspolisen har framfört att det är ett problem att internetleverantörerna, i de fall tekniken används, i dagsläget inte lagrar alla de uppgifter som behövs för att knyta trafiken till specifika abonnenter. Eftersom en publik ip-adress i teorin kan delas av upp till 65 536 abonnenter med privata ip-adresser, är det enligt myndigheterna inte möjligt att hitta källan och slutmålet för kommunikationen med ledning av enbart den publika ip-adressen (jfr 6 kap. 16 a § LEK). Att få tillgång till uppgift om den publika ip-adressen blir i sådana fall meningslöst.

Myndigheterna har mot den bakgrunden ifrågasatt om inte bestämmelserna i lagen och förordningen om elektronisk kommunikation bör tolkas så att lagringsskyldigheten i dessa fall omfattar samtliga uppgifter som behövs för att kunna knyta trafiken till specifika abonnenter. Frågan har såvitt kommit fram inte prövats rättsligt. Däremot har PTS i en skrivelse till Ekobrottsmyndigheten nyligen gett uttryck för uppfattningen att lagringsskyldigheten inte omfattar alla dessa uppgifter (dnr. 15-1185).

Det ingår inte i vårt uppdrag att föreslå åtgärder som innebär att lagringsskyldighetens omfattning utökas. Däremot kan det finnas anledning att överväga frågan i ett annat sammanhang i syfte att säkerställa att lagringen av uppgifter om ip-adresser inte blir meningslös.

11 Genomförande och konsekvenser

11.1 Ikraftträdande m.m.

Utredningens förslag: Den föreslagna regleringen ska träda i kraft den 1 juli 2016.

Utredningens bedömning: Det finns inte behov av några övergångsbestämmelser.

Den nya regleringen bör träda i kraft så snart som möjligt. Vi föreslår att detta sker den 1 juli 2016.

När det gäller processrättslig lagstiftning är utgångspunkten att nya regler ska tillämpas genast efter ikraftträdandet. Det innebär att de nya reglerna ska tillämpas även i förundersökningar och underrättelseärenden som inletts innan reglerna trätt i kraft. Detta är en lämplig ordning avseende de förändringar som vi föreslår. Det finns därför inte behov av några övergångsbestämmelser.

11.2 Konsekvenser

Utredningens bedömning: Förslagen medför inte några kostnadsökningar.

Våra förslag i fråga om möjligheten att hämta in uppgifter om brottslig verksamhet som innefattar vissa brott med lägre minimistraff än fängelse i två år får konsekvenser för brottsligheten och det brottsförebyggande arbetet. Konsekvenserna består i att brottslig verksamhet som innefattar statsstyrt företagsspionerи och vissa s.k. systemhotande brott mer effektivt kommer att kunna förebyggas, förhindras och upptäckas.

I övrigt bedöms förslagen inte få några konsekvenser av de slag som anges i kommittéförordningen.

11.2.1 Inledning

Enligt direktiven ska vi redovisa de kostnader och konsekvenser i övrigt som förslagen kan komma att medföra. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna ska vi föreslå hur dessa ska finansieras.

Enligt kommittéförordningen (1998:1474) ska det anges också om förslagen får konsekvenser i vissa andra avseenden.

11.2.2 Ekonomiska konsekvenser

Våra förslag rör huvudsakligen förfarandet när brottsbekämpande myndigheter begär tillgång till olika typer av uppgifter om elektronisk kommunikation. Några av dessa förslag, t.ex. vad gäller krav på att beslut om inhämtning av abonnemangsuppgifter ska fattas på en viss nivå inom den myndighet som begär uppgiften, kan komma att leda till en något ökad administrativ börda för de myndigheter som berörs av förslagen. Dessa ändringar bedöms emellertid vara så marginella att effekterna för myndigheternas kostnader blir försumbara.

Vi föreslår emellertid också vissa förändringar när det gäller möjligheten enligt inhämtningslagen att hämta in uppgifter om brottslig verksamhet som innefattar vissa brott med lägre minimistraff än två år. Förändringarna innebär att uppgifter kommer att kunna hämtas in även om sådan brottslig verksamhet som innefattar statsstyrt företagsspioneri samt grov misshandel och olaga frihetsberövande som begås 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. Inte heller denna förändring kan förväntas leda till annat än rent marginella kostnadsökningar.

11.2.3 Övriga konsekvenser

Förslaget i fråga om inhämtning av uppgifter om brottslig verksamhet som innefattar statsstyrt företagsspioneri och vissa systemhotande brott får konsekvenser för brottsligheten och det brottsförebyggande arbetet. Konsekvenserna består i att sådan brottslighet mer effektivt kommer att kunna förebyggas, förhindras och upptäckas.

I övrigt bedöms förslagen inte få några sådana konsekvenser som anges i kommittéförordningen (se 14–16 §§).

12 Författningskommentar

12.1 Förslaget till lag om ändring i rättegångsbalken

27 kap.

22 §
Hemlig avlyssning av elektronisk kommunikation får inte avse telefonsamtal eller andra meddelanden där någon som yttrar sig, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena, inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram. Om det under avlyssningen kommer fram att det är fråga om ett sådant samtal eller meddelande, ska avlyssningen omedelbart avbrytas.

Hemlig rumsavlyssning får inte avse samtal eller annat tal där någon som angetts i första stycket talar. Om det under rumsavlyssningen kommer fram att det är fråga om ett sådant samtal eller tal, ska avlyssningen omedelbart avbrytas.

Upptagningar och uppteckningar ska omedelbart förstöras i de delar som de omfattas av förbud enligt första eller andra stycket.

Uppteckningar från hemlig övervakning av elektronisk kommunikation ska omedelbart förstöras i de delar innehållet avser uppgifter som, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena, inte skulle ha kunnat inhämtas genom vittnesförhör i domstol.

Paragrafen reglerar bl.a. det s.k. avlyssningsförbudet.

Det *fjärde stycket* är nytt. Övervägandena finns i avsnitt 8.3.2. Bestämmelsen i det nya stycket innebär att uppteckningar från hemlig övervakning av elektronisk kommunikation i vissa fall ska förstöras omedelbart. Förstörandeskyldigheten gäller om uppteckningarna innehåller sådana uppgifter som på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken (det s.k. frågeförbudet) inte hade kunnat inhämtas genom vittnesförhör i domstol, dvs. om uppgifterna omfattas av vissa former av yrkesmässig tystnadsplikt. Eftersom möjligheten att avgöra om s.k. metadata –

uppgifter som visar att kommunikation har förekommit men inte vad den innehöll – omfattas av sådan tystnadsplikt normalt är beroende av att man känner till innehållet i kommunikationen torde det endast sällan bli aktuellt att tillämpa bestämmelsen. Ett exempel på en situation där bestämmelsen bör kunna användas kan vara om uppteckningarna visar att en person har haft kontakt med en journalist. Om den myndighet som har hämtat in uppgiften får kännedom om att det vid kommunikationen överlämnades ett meddelande eller liknande för publicering, kan uppgiften om att kommunikationen förekommit innebära att det s.k. meddelarskyddet hotas.

12.2 Förslaget till lag om ändring i lagen om elektronisk kommunikation

6 kap.

22 §

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

1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (2010:1932), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,

2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott *eller brottslig verksamhet* till en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet *eller den brottsliga verksamheten*,

3. uppgift som avses i 20 § första stycket 1 och 3 samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits till Polismyndigheten, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det finns fara för deras liv eller allvarlig risk för deras hälsa,

4. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,

5. uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner att uppgiften är av väsentlig betydelse för handläggningen av ett

ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),

6. uppgift som avses i 20 § första stycket 1 till Polismyndigheten, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),

7. uppgift som avses i 20 § första stycket 1 till Polismyndigheten eller en åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna fullgöra underrättelseskyldighet enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och

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

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

Paragrafen innehåller bestämmelser om operatörers skyldighet att på begäran lämna ut vissa uppgifter utan hinder av tystnadsplikt.

En mindre justering har gjorts i *första stycket 2*. Övervägandena finns i avsnitt 7.5.7. Syftet med ändringen är att förtydliga att operatörernas skyldighet att lämna ut uppgifter om abonnemang gäller även i de fall en brottsbekämpande myndighet behöver uppgiften i myndighetens underrättelseverksamhet.

12.3 Förslaget till lag om ändring i lagen om åtgärder för att förhindra vissa särskilt allvarliga brott

11 §

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

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

Uppteckningar från hemlig övervakning av elektronisk kommunikation ska omedelbart förstöras i de delar innehållet avser uppgifter som, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat inhämtas genom vittnesförhör i domstol.

Paragrafen reglerar bl.a. det s.k. avlyssningsförbudet enligt lagen.

Det *tredje stycket,* som är nytt, motsvarar den förändring som föreslås i 27 kap. 22 § rättegångsbalken. Se vidare i kommentaren till den paragrafen. De överväganden som ligger till grund för förändringen finns i avsnitt 8.3.2.

12.4 Förslaget till lag om ändring i offentlighets- och sekretesslagen

44 kap.

4 §

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

1. 2 kap. 14 § första stycket 1, 3 *och 4* postlagen (2010:1045),

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

3. 6 kap. 21 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på grund av beslut av domstol, undersökningsledare eller åklagare eller om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Paragrafen reglerar i vilken mån tystnadsplikt enligt postlagen och LEK inskränker den rätt att meddela och offentliggöra uppgifter som följer av 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen.

En mindre justering görs i *punkten 1* som en följd av den förändring som föreslås i postlagen. Skälen för förslaget behandlas i avsnitt 10.1.

12.5 Förslaget till lag om ändring i postlagen

2 kap.

14 §
Den som i postverksamhet har fått del av eller tillgång till någon av de uppgifter som anges i 1–*4* får inte obehörigen röja eller utnyttja vad han eller hon därigenom har fått veta. De uppgifter som omfattas av tystnadsplikten är

1. uppgifter som rör ett särskilt brev som befordras inom verksamheten,

2. andra uppgifter som rör en enskild persons förbindelse med verksamheten när det gäller befordran av brev,

3. uppgifter som handlar om att kvarhålla eller beslagta försändelser enligt 27 kap. rättegångsbalken, *eller*

4. uppgifter som handlar om att undersöka, öppna, granska eller kvarhålla försändelser enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Tystnadsplikten enligt första stycket 1 och 2 gäller inte i förhållande till avsändaren och mottagaren av brevet.

För uppgifter om en enskild persons adress gäller tystnadsplikt endast om det kan antas att ett röjande av adressen skulle medföra fara för att någon utsätts för övergrepp eller annat allvarligt men.

Paragrafen innehåller bestämmelser om tystnadsplikt i postverksamhet.

En ny punkt föreslås i det *första stycket.* Förändringen innebär att det blir tydligt att tystnadsplikten enligt lagen omfattar även uppgifter som handlar om att undersöka, öppna, granska eller kvarhålla försändelser enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Skälen för förslaget behandlas i avsnitt 10.1.

12.6 Förslaget till lag om ändring i lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

2 §
Uppgifter får hämtas in om omständigheterna är sådana att *åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar*

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

2. *sabotage enligt 13 kap. 4 § brottsbalken,*

3. *kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,*

4. *brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,*

5. *spionerі, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5 eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,*

6. *företagsspionerі enligt 3 § lagen (1990:409) om skydd för företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understödjs av en främmande makt eller av någon som agerar för en främmande makts räkning,*

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

8. *grov misshandel eller olaga frihetsberövande enligt 3 kap. 6 § eller 4 kap. 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.*

Uppgifter får hämtas in bara om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

Paragrafen innehåller förutsättningarna för att uppgifter enligt lagen ska få hämtas in.

De överväganden som ligger till grund för de förändringar som föreslås i paragrafen finns i avsnitt 9.4. Förändringarna innebär att uppgifter om brottslig verksamhet som innefattar statsstyrt företagsspionerі samt grov misshandel eller olaga frihetsberövande i s.k.

systemhotande syfte i fortsättningen kommer att kunna hämtas in enligt lagen. Övriga brott som nämns i första stycket 2–5 och 7 återfinns i dagsläget i 3 §.

Förändringen innebär vidare att möjligheten att hämta in uppgifter om brottslig verksamhet som innefattar vissa brott med lägre minimistraff än fängelse två år inte längre ska vara tidsbegränsad.

Beträffande placeringen av den aktuella brottskatalogen kan noteras att Lagrådet i sitt yttrande med anledning av förslagen i prop. 2011/12:55 ansåg att denna borde finnas i samma lagrum som där de övriga förutsättningarna för inhämtning ställs upp. Vi instämmer i att det är lämpligt att samla regleringen på det sättet.

5 §

Säkerhets- och integritetsskyddsnämnden ska underrättas om ett beslut om inhämtning av uppgifter enligt denna lag. *Underrättelseskyldigheten ska fullgöras genom att beslutet* lämnas *till nämnden* senast en månad efter det att ärendet om inhämtning avslutades.

Paragrafen reglerar de brottsbekämpande myndigheternas skyldighet att underrätta SIN om beslut enligt lagen.

En mindre justering görs i paragrafen i syfte att förtydliga att underrättelseskyldigheten ska fullgöras genom att myndighetens beslut lämnas till nämnden. De skäl som ligger till grund för förslaget finns i avsnitt 9.3.3.2.

8 §

Uppteckningar av uppgifter ska granskas snarast möjligt.

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

Uppteckningar ska dock omedelbart förstöras i de delar innehållet avser uppgifter som, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena rättegångsbalken, inte skulle ha kunnat inhämtas genom vittnesförhör i domstol.

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

Paragrafen innehåller bestämmelser om hanteringen av uppteckningar av uppgifter som hämtats in enligt lagen. Den föreslagna förändringen innebär att ett nytt *tredje stycke* införs i paragrafen. Det nya

stycket motsvarar den förändring som föreslås i 27 kap. 22 § rättegångsbalken. Se vidare i kommentaren till den paragrafen. De överväganden som ligger till grund för förändringen finns i avsnitt 8.3.2.

12.7 Förslaget till förordning om ändring i förordningen om elektronisk kommunikation

36 b §

Beslut om inhämtning av uppgifter enligt 6 kap. 22 § första stycket 2 lagen (2003:389) om elektronisk kommunikation fattas av den myndighet som ska ingripa mot brottet eller den brottsliga verksamheten. Myndighetschefen får delegera rätten att fatta beslut om inhämtning till annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Ett beslut om att delegera beslutsbefogenhet ska dokumenteras av myndigheten.

Även utan särskild delegation enligt första stycket får förundersökningsledaren fatta beslut om sådan inhämtning av uppgifter som sker inom ramen för en förundersökning.

I ett beslut om inhämtning av uppgifter enligt 6 kap. 22 § första stycket 2 lagen (2003:389) om elektronisk kommunikation ska det anges vem som har fattat beslutet samt vilket brott eller vilken brottslig verksamhet och vilka abonnemangsuppgifter beslutet avser. Skälen för beslutet ska också anges.

Paragrafen är ny. Den innehåller bestämmelser om vem som enligt 6 kap. 22 § första stycket 2 LEK får fatta beslut om inhämtning av abonnemangsuppgifter och vad ett sådant beslut ska innehålla. Övervägandena finns i avsnitt 7.5.4 och 7.5.5.

Av det *första stycket* framgår att det är den myndighet som ska ingripa mot brottet eller den brottsliga verksamheten som beslutar om inhämtningen. Detta innebär att huvudregeln är att det är myndighetschefen som ska fatta beslutet. Myndighetschefen får emellertid delegera rätten att fatta beslut om inhämtning till annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Delegation bör kunna ske till exempelvis chefer för operativ verksamhet och chefer för underrättelseverksamhet.

Ett beslut om delegation av beslutsbefogenhet ska dokumenteras. Detta kan ske t.ex. genom att delegationsbesluten tas in i myndighetens arbetsordning eller nedtecknas i en särskild beslutshandling.

I det *andra stycket* finns en undantagsregel som innebär att den som är förundersökningsledare alltid får fatta beslut om sådan inhämtning av uppgifter som sker inom ramen för en förundersökning. I dessa fall behövs således inte något särskilt delegationsbeslut.

Av det *tredje stycket* framgår att inhämtningsbeslut enligt den aktuella bestämmelsen i LEK ska dokumenteras. I beslutet ska det anges vem som har fattat beslutet samt vilket brott eller vilken brottslig verksamhet och vilka abonnemangsuppgifter beslutet avser. Skälen för beslutet ska också anges.

Eftersom bestämmelsen riktar sig till de brottsbekämpande myndigheterna är placeringen i förordningen om elektronisk kommunikation inte idealisk. Såväl lagen som förordningen om elektronisk kommunikation riktar sig i övrigt huvudsakligen till leverantörer av elektroniska kommunikationsnät och kommunikationstjänster. Vi bedömer emellertid att den föreslagna placeringen är det bästa alternativ som står till buds.

Kommittédirektiv 2014:101

Översyn av vissa bestämmelser om elektronisk kommunikation i brottsbekämpningen

Beslut vid regeringssammanträde den 26 juni 2014

Sammanfattning

En särskild utredare ska utvärdera lagen om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Utredaren ska också föreslå de förändringar som bedöms lämpliga för att stärka skyddet för den personliga integriteten vid tillämpningen av bestämmelserna om elektronisk kommunikation i brottsbekämpningen.

Utredaren ska bl.a.

- kartlägga tillämpningen av inhämtningslagen,
- överväga om de rättssäkerhetsåtgärder och integritetsstärkande åtgärder som vidtogs när inhämtningslagen infördes har varit tillräckliga eller om det finns behov av ytterligare sådana åtgärder, t.ex. införande av domstolskontroll,
- analysera Säkerhetspolisens behov av en möjlighet enligt inhämtningslagen att inhämta uppgifter om brottslig verksamhet som innefattar vissa samhällsfarliga brott,
- föreslå de förändringar som bedöms lämpliga för att stärka skyddet för den personliga integriteten i förhållande till reglerna om lagring av uppgifter enligt 6 kap. 16 a–f §§ lagen om elektronisk kom-

munikation, samt övriga bestämmelser om tillgång till och behandling av sådana uppgifter, och

- lämna förslag på de författningsändringar eller andra förändringar som behövs.

Uppdraget ska redovisas senast den 31 mars 2015.

Uppdraget att utvärdera inhämtningslagen

Rätten till personlig integritet

Var och en som vistas i riket har rätt att göra anspråk på att staten vidtar effektiva åtgärder till skydd för hans eller hennes säkerhet. I detta ligger bl.a. att staten måste anstränga sig för att se till att brott förebyggs och utreds och att gärningsmän ställs till svars för sina brottsliga handlingar. En effektiv brottsbekämpning är en förutsättning för att rättstryggheten för enskilda ska kunna upprätthållas. Det är samtidigt viktigt i en rättsstat att den offentliga maktutövningen är bunden av förutsebara normer och underkastad vissa begräsningar. Staten måste respektera enskildas berättigade krav på skydd mot godtycke och krav på respekt för de grundläggande fri- och rättigheterna.

Var och en är gentemot det allmänna enligt grundlag skyddad mot bl.a. hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande (2 kap. 6 § första stycket regeringsformen). Därtill gäller ett skydd mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (andra stycket). Detta skydd får begränsas endast genom lag. Begränsningar får göras endast för att tillgodose ett ändamål som är godtagbart i ett demokratiskt samhälle och får inte gå utöver vad som är nödvändigt för att uppnå syftet med begränsningen (2 kap. 20 och 21 §§).

Av artikel 8 i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen), som gäller som lag i Sverige, följer vidare att var och en har rätt till respekt för sitt privat- och familjeliv och sin korrespondens. Begränsningar i denna rättighet får göras bl.a. för att förebygga oordning eller brott. En begränsning får dock göras bara om

den är nödvändig i ett demokratiskt samhälle. Det innebär att den måste kunna motiveras av ett angeläget allmänt intresse och inte får gå utöver vad som behövs för att uppnå sitt syfte. Av regeringsformen följer att en föreskrift i lag eller annan författning inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Rätten till respekt för privatlivet slås även fast i artikel 7 i EU:s stadga om de grundläggande rättigheterna (EU-stadgan). Enligt artikel 8 i EU-stadgan har var och en vidare rätt till skydd för sina personuppgifter.

De brottsbekämpande myndigheternas underrättelseverksamhet

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

Tidigare regler om inhämtning av uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

Före den 1 juli 2012 kunde de brottsbekämpande myndigheterna få tillgång till historiska uppgifter om meddelanden direkt från den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst (t.ex. en teleoperatör) enligt lagen (2003:389) om elektronisk kommunikation. Förutsättningen för

att få ut uppgifter var att det var fråga om misstanke om brott med lägsta föreskrivna straff fängelse i två år. Däremot fanns det inte några krav på att åtgärden skulle vara proportionerlig eller på att uppgifterna skulle vara av någon viss vikt för en brottsutredning eller ett underrättelseändamål. Det fanns inte heller några regler om vem som fick besluta om inhämtning eller om tillsyn över inhämtningen.

Inhämtningslagen

Bestämmelserna om utlämnande av uppgifter om meddelanden i lagen om elektronisk kommunikation ersattes den 1 juli 2012 av lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Enligt lagen får en polismyndighet eller Tullverket, under de förutsättningar som anges i lagen, i underrättelseverksamhet i hemlighet hämta in uppgifter om elektronisk kommunikation från den som enligt lagen om elektronisk kommunikation tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. De uppgifter som får hämtas in med stöd av lagen är s.k. trafikuppgifter och lokaliseringsuppgifter. Trafikuppgifter kan t.ex. vara uppgifter om ett meddelandes ursprung, destination, färdväg, datum, tid, varaktighet, storlek eller typ av kommunikationstjänst. Lokaliseringsuppgifter är uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller uppgifter om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Lagen ger däremot inte någon möjlighet att få tillgång till innehållet i meddelanden.

Enligt inhämtningslagens huvudregel får uppgifter hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Vidare gäller att inhämtning av uppgifter bara är tillåten om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.

En tidsbegränsad bestämmelse om inhämtning av uppgifter i Säkerhetspolisens underrättelseverksamhet

Eftersom flera av de brott som Säkerhetspolisen bekämpar har lägre minimistraff än fängelse i två år kan inhämtningslagens huvudregel inte tillämpas på brottslig verksamhet som innefattar dessa brott. Trots att dessa brott har lägre minimistraff är de dock särskilt angelägna att upptäcka och förhindra eftersom de riktar sig mot samhällsstrukturen och mot rikets säkerhet. Enligt en särskild tidsbegränsad bestämmelse (3 §) får uppgifter därför även hämtas in om brottslig verksamhet som innefattar

- sabotage,
- kapning, sjö- eller luftfartssabotage eller flygplatssabotage, om brottet innefattar sabotage,
- brott mot medborgerlig frihet,
- spioneri, grov obehörig befattning med hemlig uppgift eller olovlig underrättelseverksamhet, grovt brott, eller
- grovt brott enligt 3 § andra stycket lagen (2002:444) om straff för finansiering av särskilt allvarlig brottslighet i vissa fall eller grovt brott enligt 6 § lagen (2010:299) om straff för offentlig uppmaning, rekrytering och utbildning avseende terroristbrott och annan särskilt allvarlig brottslighet.

När inhämtningslagen trädde i kraft gavs den aktuella bestämmelsen begränsad giltighetstid till utgången av 2013. Som skäl för att tidsbegränsa bestämmelsen angavs att frågan om Säkerhetspolisens fortsatta tillgång till övervakningsuppgifter för tiden därefter borde övervägas i det sammanhang som en framtida reglering av hemliga tvångsmedel för särskilt allvarlig eller samhällsfarlig brottslighet övervägs (prop. 2011/12:55 s. 87).

Integritetsstärkande åtgärder vidtogs när inhämtningslagen infördes

Vid införandet av inhämtningslagen gjorde regeringen bedömningen att de dåvarande reglerna i lagen om elektronisk kommunikation om utlämnande av uppgifter inte framstod som ändamålsenligt utformade och att de inte heller i tillräcklig grad uppfyllde de krav på

rättssäkerhet och integritetsskydd som måste ställas på sådana åtgärder (se prop. 2011/12:55 s. 66). Ett flertal åtgärder som syftade till att stärka rättssäkerheten och skyddet för den personliga integriteten vidtogs därför. Till exempel infördes de ovan nämnda kraven på att inhämtningen ska vara av särskild vikt för ändamålet med åtgärden och att den ska vara proportionerlig. Vidare infördes krav på att ett beslut om inhämtning ska innehålla uppgifter om vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet gäller. Det infördes också regler om vilken tidsperiod ett beslut får avse.

Tidigare fanns inte heller några regler om vem som fick fatta beslut om att hämta in uppgifter. Enligt inhämtningslagen gäller numera att beslut om inhämtning fattas av myndigheten, vilket innebär att utgångspunkten är att det är myndighetschefen som beslutar om inhämtningen. Myndighetschefen får dock delegera rätten att fatta beslut till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Den som har fått sådan delegation får inte fatta beslut om inhämtning i operativ verksamhet som han eller hon deltar i.

Till skillnad från tidigare utövar Säkerhets- och integritetsskyddsnämnden tillsyn över inhämtningen. Samtliga beslut om inhämtning av uppgifter ska också anmälas till nämnden. Inhämtade uppgifter får användas i en förundersökning endast efter tillstånd till hemlig övervakning av elektronisk kommunikation.

Senare överäganden

Den 2 februari 2012 beslutade regeringen att ge Utredningen om vissa hemliga tvångsmedel i tilläggsuppdrag att bl.a. analysera Säkerhetspolisens behov av uppgifter i underrättelseverksamhet avseende viss brottslig verksamhet (dir. 2012:9). Utredningen presenterade sina förslag i juni 2012 i betänkandet Hemliga tvångsmedel mot allvarliga brott (SOU 2012:44) och gjorde då bedömningen att det bör finnas en möjlighet att hämta in uppgifter om elektronisk kommunikation i underrättelseverksamhet avseende vissa brott inom Säkerhetspolisens verksamhetsområde vilka inte har ett straffminimum som uppgår till två års fängelse. Utredningen föreslog samman-

fattningsvis att inhämtningslagens 3 § skulle permanentas och utvidgas till att gälla samtliga brott som omfattas av lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott, med undantag för olovlig kårverksamhet (nämnda SOU s. 629 f.).

Regeringen konstaterade dock i den efterföljande propositionen att inhämtningslagen inte omfattades av den kartläggning som utredningen med bistånd av Brottsförebyggande rådet hade genomfört av tillämpningen av hemliga tvångsmedel enligt vissa andra lagar. Enligt regeringen borde den hittillsvarande tillämpningen av inhämtningslagen kartläggas och analyseras ytterligare innan slutlig ställning tas till hur Säkerhetspolisens behov av övervakningsuppgifter i underrättelseverksamhet bör tillgodoses. Enligt regeringens mening fanns det även anledning att undersöka om de rättssäkerhetsåtgärder och integritetsstärkande åtgärder som vidtogs när lagen infördes har varit tillräckliga eller om det finns behov av andra sådana åtgärder, t.ex. införande av domstolskontroll. Mot den bakgrunden ansåg regeringen att det i det sammanhanget inte borde göras några förändringar i lagen. Däremot föreslogs att 3 § ska fortsätta att gälla till utgången av 2016 (prop. 2013/14:237 s. 116).

Tillämpningen av inhämtningslagen bör kartläggas och analyseras

En effektiv brottsbekämpning förutsätter att de brottsbekämpande myndigheterna har tillgång till verkningsfulla tvångsmedel. Möjligheten att inhämta uppgifter om elektronisk kommunikation är ett viktigt verktyg i myndigheternas underrättelseverksamhet. Utgångspunkten är att sådana åtgärder samtidigt innebär ett intrång i enskildas rätt till personlig integritet enligt regeringsformen, Europakonventionen och EU-stadgan. Utformningen av regler om hemliga tvångsmedel förutsätter att en avvägning görs mellan å ena sidan nyttan och behovet av tvångsmedlet och å andra sidan omfattningen och arten av det intrång i den personliga integriteten som tvångsmedlet innebär. För att en sådan avvägning ska kunna göras krävs att nyttan och behovet av tvångsmedlet, ändamålet med tvångsmedelsregleringen samt omfattningen och arten av intrånget i den personliga integriteten kan klarläggas med sådan konkretion att det finns ett fullgott underlag för bedömningen av om befogenheten att använda tvångsmedlet är proportionerlig. Ett sådant underlag

bör, när det är möjligt, bygga på uppgifter om den hittillsvarande tillämpningen av det tvångsmedel som avses.

Mot den bakgrunden ska utredaren

- kartlägga den hittillsvarande tillämpningen av inhämtningslagen,
- analysera vilken nytta tvångsmedelsanvändningen enligt lagen har inneburit för den brottsbekämpande verksamheten,
- analysera vilken inverkan lagen har haft på enskildas personliga integritet,
- överväga om de rättssäkerhetsåtgärder och integritetsstärkande åtgärder som vidtogs när inhämtningslagen infördes har varit tillräckliga eller om det finns behov av andra sådana åtgärder, t.ex. införande av domstolskontroll,
- analysera Säkerhetspolisens behov av en möjlighet enligt inhämtningslagen att inhämta uppgifter om elektronisk kommunikation för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar vissa samhällsfarliga brott med lägre straffminimum än två års fängelse, och
- lämna förslag på hur detta behov bör tillgodoses och balanseras mot integritetsintresset.

Utredaren ska lämna de fullständiga författningsförslag som krävs.

Uppdraget med anledning av EU-domstolens dom om datalagringsdirektivet

Datalagringsdirektivet

Europaparlamentet och rådets direktiv 2006/24/EG om lagring av trafikuppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (datalagringsdirektivet) syftar till att harmonisera medlemsstaternas regler om skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra trafik- och lokaliseringsuppgifter samt

uppgifter som behövs för att identifiera en abonnent eller användare för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal av allvarliga brott. Direktivet har genomförts i svensk rätt genom ändringar i bl.a. lagen om elektronisk kommunikation (prop. 2010/11:46, bet. 2011/12:JuU28, rskr. 2011/12:166).

EU-domstolens dom

Den 8 april 2014 meddelade EU-domstolen dom i målen C-293/12 och C-594/12, Digital Rights Ireland m.fl., angående giltigheten av datalagringsdirektivet med anledning av begäran om förhandsavgörande från nationella domstolar i Irland respektive Österrike. EU-domstolen förklarade i domen datalagringsdirektivet ogiltigt.

I domen slog EU-domstolen fast att direktivet innebär ett omfattande och särskilt allvarligt intrång i rätten till privatliv och skyddet av personuppgifter. Domstolen konstaterade dock att en skyldighet att lagra uppgifter är en ändamålsenlig åtgärd för att uppnå syftet att bekämpa allvarlig brottslighet och upprätthålla allmän säkerhet, vilket skulle kunna motivera ett intrång i rättigheterna. Eftersom direktivet i vissa avseenden inte fastställer tydliga och preciserade regler för omfattningen av intrånget i de aktuella rättigheterna begränsas emellertid inte direktivet till vad som är absolut nödvändigt för att uppnå syftet. Domstolen fann vid en samlad bedömning att EU:s lagstiftande församlingar överskridit sina befogenheter då direktivet antogs eftersom det inte lever upp till proportionalitetsprincipen med avseende på artiklarna 7, 8 och 52.1 i EU-stadgan.

Utredning med anledning av domen

Den 29 april 2014 gav chefen för Justitiedepartementet en utredare i uppdrag att biträda departementet med att, i ljuset av EU-domstolens dom, grundligt analysera reglerna om lagring av uppgifter enligt 6 kap. 16 a–f §§ lagen om elektronisk kommunikation, samt övriga bestämmelser om tillgång till och behandling av sådana uppgifter, och deras förhållande till unionsrätten. Utredaren fick även i uppdrag att föreslå de ändringar som han finner lämpliga för att stärka skyddet av den personliga integriteten samt, om resultatet av analysen visar på brister i förhållande till unionsrätten, för att leva

upp till unionsrättens krav. Redovisningen av uppdraget delades upp i två steg, varvid analysen redovisades den 13 juni 2014 (Ds 2014:23). Uppdraget i övrigt ska redovisas den 1 oktober 2014.

Av analysen framgår att utredarens samlade bedömning är att det svenska regelverket om lagring och utlämnande av uppgifter ryms inom de ramar som ställs upp av unions- och Europarättens allmänna principer och kravet på respekt för grundläggande rättigheter. Mot bakgrund av att unionsrätten och Europarätten endast ställer upp vissa minimikrav för skydd av privatlivet som måste uppfyllas i den nationella lagstiftningen gör utredaren trots det bedömningen att det finns skäl att närmare överväga några regelförändringar för att ytterligare stärka skyddet för den personliga integriteten. Enligt utredaren finns det skäl att närmare överväga om lagringsskyldighetens omfattning när det gäller vissa uppgiftskategorier bör begränsas i något avseende. Vidare har utredaren kommit fram till att det finns skäl att noga överväga om den externa kontrollen över inhämtning av abonnemangsuppgifter och inhämtning av uppgifter i underrättelseskedet bör stärkas. Enligt utredaren ter det sig också som befogat att ytterligare överväga om det bör ställas krav på att uppgifterna ska lagras inom EU eller EES.

Frågor som rör brottsbekämpande myndigheters tillgång till uppgifter om elektronisk kommunikation bör övervägas i ett sammanhang

Av den analys som redovisades den 13 juni 2014 framgår alltså att en av de frågor som utredaren har ansett att det finns skäl att närmare överväga är om den externa kontrollen över inhämtning av uppgifter i underrättelseskedet bör stärkas. Eftersom inhämtningslagen reglerar frågor om tillgång till uppgifter i underrättelseverksamheten kommer sådana överväganden att innebära en bedömning av om det finns behov av att förändra inhämtningslagen för att stärka integritetsskyddet.

Enligt regeringens mening bör frågan om det finns behov av rättssäkerhets- eller integritetsstärkande åtgärder när det gäller regleringen i inhämtningslagen övervägas i ett sammanhang. Det är naturligt att i det sammanhanget också överväga frågan om hur Säkerhetspolisens behov av uppgifter om elektronisk kommunikation i underrättelseverksamhet bör tillgodoses. Det är vidare lämpligt att dessa överväganden görs inom ramen för ett fristående utredningsuppdrag.

De frågor som föranleds av den gjorda analysen bör därför tas om hand inom ramen för det nu aktuella uppdraget.

Utredaren ska därför

- föreslå de förändringar som utifrån den utförda analysen bedöms lämpliga för att stärka skyddet för den personliga integriteten i förhållande till reglerna om lagring av uppgifter enligt 6 kap. 16 a–f §§ lagen om elektronisk kommunikation, och övriga bestämmelser om tillgång till och behandling av sådana uppgifter, och
- lämna de fullständiga författningsförslag som krävs för sådana ändringar.

Konsekvensbeskrivningar

Utredaren ska redovisa de kostnader och konsekvenser i övrigt som förslagen kan komma att medföra. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Samråd och redovisning av uppdraget

Vid genomförandet av uppdraget ska utredaren samverka med Brottsförebyggande rådet vid genomförandet av utvärderingen av inhämtningslagen. Utredaren ska vidare samråda med Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Tullverket, Post- och telestyrelsen samt med andra myndigheter i den utsträckning utredaren finner det lämpligt.

Uppdraget ska redovisas senast den 31 mars 2015.

(Justitiedepartementet)

Statens offentliga utredningar 2015

Kronologisk förteckning

1. Deltagande med väpnad styrka i utbildning utomlands. En utökad beslutsbefogenhet för regeringen. Fö.
2. Värdepappersmarknaden MiFID II och MiFIR. + Bilagor. Fi.
3. Med fokus på kärnuppgifterna. En angelägen anpassning av Polismyndighetens uppgifter på djurområdet. Ju.
4. Ett svenskt tonnageskattesystem. Fi.
5. En ny svensk tullagstiftning. Fi.
6. Mer gemensamma tobaksregler. Ett genomförande av tobaksproduktdirektivet. S.
7. Krav på privata aktörer i välfärden. Fi.
8. En översyn av årsredovisningslagarna. Ju.
9. En modern reglering av järnvägstransporter. Ju.
10. Gränser i havet. UD.
11. Kunskapsläget på kärnavfallsområdet 2015. Kontroll, dokumentation och finansiering för ökad säkerhet. M.
12. Överprövning av upphandlingsmål m.m. Fi.
13. Tillämpningsdirektivet till utstationeringsdirektivet – Del I. A.
14. Sedd, hörd och respekterad. Ett ändamålsenligt klagomålssystem i hälso- och sjukvården. S.
15. Attraktiv, innovativ och hållbar – strategi för en konkurrenskraftig jordbruks- och trädgårdsnäring. N L.
16. Ökat värdeskapande ur immateriella tillgångar. N.
17. För kvalitet – Med gemensamt ansvar. S.
18. Lösöreköp och registerpant. Ju.
19. En ny ordning för redovisningstillsyn. Fi.
20. Trygg och effektiv utskrivning från sluten vård. S.
21. Mer trygghet och bättre försäkring. Del 1 + 2. S.
22. Rektorn och styrkedjan. U.
23. Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. Ju Fö.
24. En kommunallag för framtiden. Del A + B . Fi.
25. En ny säkerhetsskyddslag. Ju.
26. Begravningsclearing. Ku.
27. Skatt på dubbdäcksanvändning i tätort? Fi.
28. Gör Sverige i framtiden – digital kompetens. N.
29. En yrkesinriktning inom teknikprogrammet. U.
30. Kemikalieskatt. Skatt på vissa konsumentvaror som innehåller kemikalier. Fi.
31. Datalagring och integritet. Ju.

Statens offentliga utredningar 2015

Systematisk förteckning

Arbetsmarknadsdepartementet

Tillämpningsdirektivet till utstationeringsdirektivet – Del I [13]

Finansdepartementet

Värdepappersmarknaden MiFID II och MiFIR. + Bilagor [2]

Ett svenskt tonnageskattesystem. [4]

En ny svensk tullagstiftning. [5]

Krav på privata aktörer i välfärden. [7]

Överprövning av upphandlingsmål m.m. [12]

En ny ordning för redovisningstillsyn. [19]

En kommunallag för framtiden. Del A + B. [24]

Skatt på dubbdäcksanvändning i tätort? [27]

Kemikalieskatt. Skatt på vissa konsumentvaror som innehåller kemikalier. [30]

Försvarsdepartementet

Deltagande med väpnad styrka i utbildning utomlands. En utökad beslutsbefogenhet för regeringen. [1]

Justitiedepartementet

Med fokus på kärnuppgifterna. En angelägen anpassning av Polismyndighetens uppgifter på djurområdet. [3]

En översyn av årsredovisningslagarna. [8]

En modern reglering av järnvägstransporter. [9]

Lösöreköp och registerpant. [18]

Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. [23]

En ny säkerhetsskyddslag. [25]

Datalagring och integritet. [31]

Kulturdepartementet

Begravningsclearing. [26]

Miljö- och energidepartementet

Kunskapsläget på kärnavfallsområdet 2015. Kontroll, dokumentation och finansiering för ökad säkerhet. [11]

Näringsdepartementet

Attraktiv, innovativ och hållbar – strategi för en konkurrenskraftig jordbruks- och trädgårdsnäring. [15]

Ökat värdeskapande ur immateriella tillgångar. [16]

Gör Sverige i framtiden – digital kompetens. [28]

Socialdepartementet

Mer gemensamma tobaksregler. Ett genomförande av tobaksproduktdirektivet. [6]

Sedd, hörd och respekterad. Ett ändamålsenligt klagomålssystem i hälso- och sjukvården. [14]

För kvalitet – Med gemensamt ansvar. [17]

Trygg och effektiv utskrivning från sluten vård. [20]

Mer trygghet och bättre försäkring. Del 1 + 2. [21]

Utbildningsdepartementet

Rektorn och styrkedjan. [22]

En yrkesinriktning inom teknikprogrammet. [29]

Utrikesdepartementet

Gränser i havet. [10]