Datalagring – brottsbekämpning och integritet

Delbetänkande av
Utredningen om datalagring och EU-rätten

Stockholm 2017

STATENS OFFENTLIGA UTREDNINGAR

SOU 2017:75

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

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

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

ISBN 978-91-38-24676-4
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Regeringen beslutade den 16 februari 2017 att tillkalla en särskild utredare med uppdrag att se över bestämmelserna om skyldighet att lagra uppgifter om elektronisk kommunikation som gäller leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster samt bestämmelserna om de brottsbekämpande myndigheternas tillgång till sådana uppgifter. Utredaren fick även i uppdrag att se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när hemliga tvångsmedel för särskilt allvarlig brottslighet används, vilket redovisas i ett senare betänkande.

Sigurd Heuman, ordförande i Säkerhets- och integritetsskyddsnämnden, förordnades att från och med den 16 februari 2017 vara särskild utredare. Följande personer förordnades att från samma dag som experter biträda utredaren: kriminalkommissarien Anders Ahlqvist och juristen Anna Olander Selldén vid Polismyndigheten, seniora strategiska rådgivaren Kurt Alavaara och chefsjuristen Per Lagerud vid Säkerhetspolisen, juristen Jonas Agnvall vid Datainspektionen, stabsjuristen Katarina Bigovic Apitzsch vid Tullverket, professorn Iain Cameron vid Uppsala universitet, chefsåklagaren Carin Ewald Möller vid Ekobrottsmyndigheten, kammaråklagaren Hans Harding vid Åklagarmyndigheten, enhetschefen Staffan Lindmark vid Post- och telestyrelsen, kanslichefen Eva Melander Tell vid Säkerhets- och integritetsskyddsnämnden, generalsekreteraren Anne Ramberg vid Advokatsamfundet, rådmannen Anna Tansjö vid Helsingborgs tingsrätt samt kanslirådén Linda Rantén vid Justitiedepartementet och Helene Ramqvist Engellau vid Näringsdepartementet.

Som sekreterare anställdes från och med den 16 februari 2017 hovrättsassessorn Christofer Gatenheim och från och med den 23 februari 2017 kanslirådet Mikael Kullberg.

Utredningen har antagit namnet Utredningen om datalagring och EU-rätten. Sigurd Heuman svarar som utredare ensam för innehållet i betänkandet även om också experterna har ställt sig bakom det, i den mån inte annat framgår av ett särskilt yttrande. Särskilda uppfattningar i enskildheter och i formuleringar kan dock förekomma utan sådant yttrande.

Härmed överlämnas delbetänkandet *Datalagring – brottsbekämpning och integritet* (SOU 2017:75).

Utredningen fortsätter nu sitt arbete att se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när hemliga tvångsmedel för särskilt allvarlig brottslighet används.

Stockholm i oktober 2017

Sigurd Heuman

/Mikael Kullberg
Christofer Gatenheim

Innehåll

Förkortningar

2007 års preventivlag	lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott
Artikel 29-gruppen	EU:s arbetsgrupp som bildats med stöd av artikel 29 i dataskyddsdirektivet
dataskydds-konventionen	Europarådets konvention från 1981 om skydd för enskilda vid automatisk behandling av personuppgifter (ETS 108)
Digital Rights-domen	EU-domstolens dom den 8 april 2014 i de förenade målen C-293/12 och C-594/12
direktiv 95/46 eller dataskyddsdirektivet	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 (EGT L 281, 1995, s. 31)
direktiv 2002/58	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) (EGT L 201, 2002, s. 37), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 (EUT L 337, 2009, s. 11)
direktiv 2006/24 eller datalagringsdirektivet	Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lag-

	ring 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 (EUT L 105, 2006, s. 54)
Europadomstolen	den Europeiska domstolen för de mänskliga rättigheterna
Europakonventionen	den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna, med de tillägg och ändringar som gjorts genom de protokoll som Sverige ratificerat
FEK	förordningen (2003:396) om elektronisk kommunikation
FEUF	fördraget om Europeiska unionens funktionssätt
IHL	lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet
JK	Justitiekanslern
JO	Riksdagens ombudsmän
LEK	lagen (2003:389) om elektronisk kommunikation
LSU	lagen (1991:572) om särskild utlänningskontroll
NOA	Nationella operativa avdelningen (del av Polismyndigheten)
NUC	Nationellt underrättelsecenter (del av Polismyndigheten)

PNR-direktivet	Europaparlamentets och rådets direktiv 2016/681/EU av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (EUT L 119, 2016, s. 132)
PTS	Post- och telestyrelsen
RB	rättegångsbalken
RF	regeringsformen
RUC	Regionalat underrättelsecenter (del av Polismyndigheten)
rättighetsstadgan eller stadgan	Europeiska unionens stadga om de grundläggande rättigheterna (EGT C 202, 2016)
SIN	Säkerhets- och integritetsskyddsnämnden
Tele2-domen	EU-domstolens dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15
Tele2-målet	EU-domstolens förenade mål C-203/15 och C-698/15

Sammanfattning

Utredningens uppdrag och arbete

EU-domstolens uttolkning av EU-rätten i Tele2-domen har gjort det nödvändigt att reformera de svenska reglerna kring datalagring, både avseende lagring och åtkomst. Utredningens uppdrag har varit att göra de svenska reglerna förenliga med EU-rätten. Uppdraget har inrymt överväganden inom ett mycket komplext område, både juridiskt och tekniskt. Det har dessutom utförts under stor skyndsamhet eftersom det har varit angeläget att snabbt få en reglering på plats som är förenlig med de uttalanden som EU-domstolen gjort i Tele2-domen. Experter från brottsbekämpande myndigheter, tillsynsmyndigheter, Sveriges domstolar, Sveriges Advokatsamfund, Uppsala universitet och Regeringskansliet har deltagit i utredningen.

Grundläggande rättigheter

Grundläggande rättigheter som tillförsäkras enskilda finns i bl.a. regeringsformen, Europakonventionen och EU:s rättighetsstadga. Det finns två sidor av enskildas grundläggande rättigheter: dels enskildas rätt att bli fredade från kränkningar från statens sida, dels statens plikt att tillförsäkra enskilda ett skydd mot kränkningar från andra enskilda, t.ex. genom ingripande åtgärder i en brottsutredning. Det ankommer på staten att upprätta ett ramverk som är förenligt med dessa delvis konkurrerande principer.

De rättigheter som främst är av intresse för uppdraget är rätten till privatliv, rätten till skydd för personuppgifter och rätten till yttrandefrihet. Samtliga dessa rättigheter garanteras i regeringsformen, Europakonventionen och EU:s rättighetsstadga.

Integritetsskydd vid elektronisk kommunikation

För att säkerställa full respekt för rätten till privatliv och rätten till skydd för personuppgifter inom sektorn för elektronisk kommunikation har EU antagit direktiv 2002/58. Direktivet ålägger medlemsstaterna att t.ex. säkerställa konfidentialitet vid elektronisk kommunikation och därmed förbundna trafikuppgifter. Uppgifter som inte längre behövs ska enligt direktivet utplånas eller avidentifieras. Medlemsstaterna får dock göra undantag från dessa åligganden om det behövs för bl.a. brottsbekämpande verksamhet. Direktivet är genomfört i svensk rätt främst genom bestämmelser som tagits in i lagen (2003:389) om elektronisk kommunikation.

Brottsbekämpande verksamhet

Brottsbekämpande verksamhet består av två övergripande delar, underrättelseverksamhet och utredande verksamhet. Underrättelseverksamheten 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 brottsbekämpande myndigheterna med kunskap som kan omsättas i operativ verksamhet. Den utredande verksamheten utgår från en redan uppkommen händelse. Myndigheten ska, ofta inom en förundersökning, utreda om brott har begåtts och vem som i så fall skäligen kan misstänkas för brottet samt skaffa tillräckligt material för bedömning av frågan om åtal ska väckas.

I både brottsutredande verksamhet och underrättelseverksamhet används hemliga tvångsmedel. Det tvångsmedel som är av intresse för datalagringsfrågan är hemlig övervakning av elektronisk kommunikation, som regleras i rättegångsbalken. Härtill kommer tvångsmedlen enligt lagen (1991:572) om särskild utlänningskontroll och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, som har sin tillämpning i underrättelseverksamhet. Även inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet utgör ett hemligt tvångsmedel. Inhämtning av abonnemangsuppgifter enligt lagen (2003:389) om elektronisk kommunikation är däremot inte ett hemligt tvångsmedel.

Uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

Uppgifter om elektronisk kommunikation delas in i olika grupper. Med abonnemangsuppgifter avses t.ex. uppgifter om abonnentens nummer, namn, titel och adress. Till sådana uppgifter brukar även räknas uppgifter om exempelvis avtal och fakturering. Vidare innefattas såväl uppgift om vem som använt en fast eller dynamisk ip-adress eller ett IMSI-nummer (ett nummer som är kopplat till abonnentens sim-kort och därmed telefonnummer) som ett flertal andra uppgifter. Den exakta gränsen är svår att dra. 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. Vid sidan av begreppet trafikuppgifter används även uttrycket lokaliseringsuppgifter för att beteckna uppgifter som är knutna till lokaliseringen av en kommunikationsutrustning. Det kan t.ex. vara fråga om vilken cell (antenn på basstation) som utrustningen kopplat upp sig mot.

Nuvarande regleringen av lagring av uppgifter

Uppgifter om elektronisk kommunikation är mycket viktiga för brottsbekämpningen. Det finns därför regler i lagen (2003:389) om elektronisk kommunikation som säkerställer att myndigheterna kan få tillgång till dessa uppgifter. För detta syfte föreskriver lagen om elektronisk kommunikation en lagringsskyldighet för dem som tillhandahåller elektroniska kommunikationstjänster. Lagringsskyldigheten omfattar vissa uppräknade uppgifter som genereras eller behandlas i verksamheten. Lagringsskyldigheten omfattar telefonitjänster (fasta och mobila), meddelandehantering och internetåtkomst.

Nuvarande regleringen av tillgång till uppgifter

Hur myndigheterna kan få tillgång till de uppgifter som omfattas av lagringsskyldigheten – och andra uppgifter som behandlas i verksamheten, t.ex. på grund av operatörernas faktureringsbehov – beror på

vilken typ av uppgift det är och i vilket syfte tillgång begärs. För trafik- och lokaliseringsuppgifter regleras tillgången i rättegångsbalken och lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Härtill kommer lagen (1991:572) om särskild utlänningskontroll och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, som hänvisar till rättegångsbalkens bestämmelser. Tillgången till abonnemangsuppgifter har inte bedömts utgöra ett hemligt tvångsmedel och regleras direkt i lagen om elektronisk kommunikation.

Tillgång till trafik- och lokaliseringsuppgifter i den brottsutredande verksamheten kräver domstolsbeslut och är endast möjlig vid allvarliga brott. I underrättelseverksamheten är tillgången till trafikuppgifter något mer begränsad men kräver som huvudregel inte domstolsbeslut. Tillgången till abonnemangsuppgifter kräver inget domstolsbeslut utan beslutas av den brottsbekämpande myndigheten själv. Det krävs inte heller att brottet är av visst allvar.

För att skydda personers integritet och upprätthålla en hög grad av rättssäkerhet innehåller regelverket kring myndigheternas tillgång till uppgifter om elektronisk kommunikation ett antal kontrollmekanismer och rättssäkerhetsgarantier.

För all användning av tvångsmedel gäller ändamålsprincipen, behovsprincipen och proportionalitetsprincipen. Tvångsmedlen får därmed endast användas för det ändamål som framgår av lagstiftningen, om det finns ett påtagligt behov och en mindre ingripande åtgärd inte är tillräcklig samt om åtgärden står i rimlig proportion både till nyttan av åtgärden och till de intrång eller men som åtgärden innebär.

Nyttan och behovet av uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

Det finns ett påtagligt behov av uppgifter om elektronisk kommunikation för brottsbekämpningen och uppgifterna ger de brottsbekämpande myndigheterna stor nytta. Det gäller samtliga de uppgifter som ska lagras enligt förordningen (2003:396) om elektronisk kommunikation. Däremot är inte nyttan och behovet desamma för alla uppgifter och inte heller desamma över tid, eftersom beteende-

mönster och teknik hela tiden förändras. Som exempel kan nämnas den minskade användningen av fast telefoni, den ökande användningen av internet i mobiltelefoner samt en ökad användning av iptelefoni genom mobilappar.

EU-rättens påverkan på reglerna om datalagring

Med anledning av att datalagringsdirektivet (2006/24) ogiltigförklarades av EU-domstolen den 8 april 2014 (Digital Rights-domen) gav chefen för Justitiedepartementet en utredare i uppdrag att analysera konsekvenserna för den svenska lagstiftningen (Ds 2014:23). Som en uppföljning av analysen i departementspromemorian gav regeringen en utredare i uppdrag att överväga ytterligare rättssäkerhets- och integritetsstärkande åtgärder bl.a. för reglerna om lagring av uppgifter om elektronisk kommunikation (SOU 2015:31). Den svenska lagstiftningen bedömdes i båda analyserna som förenlig med EU-rätten, även om vissa förslag på förändringar presenterades.

Tele2-domen och domen från Kammarrätten i Stockholm

Kammarrätten i Stockholm begärde ett förhandsavgörande av EU-domstolen med anledning av ett överklagat föreläggande från Post- och telestyrelsen mot ett lagringsskyldigt företag om att lagra uppgifter om elektronisk kommunikation. EU-domstolen besvarade kammarrättens begäran genom Tele2-domen. EU-domstolen ansåg att direktiv 2002/58 är tillämpligt på de svenska reglerna om datalagring, även avseende tillgång till uppgifterna. Artikel 15.1 i direktivet, som i viss utsträckning tillåter datalagring, ska enligt domstolen tolkas strikt och mot bakgrund av rättighetsstadgan. De svenska reglerna om datalagring bedömdes utgöra inskränkningar i rättigheterna enligt artiklarna 7, 8 och 11 i stadgan. Inskränkningar i rättigheterna får enligt EU-domstolen endast göras under vissa förutsättningar, däribland att de är proportionella och strängt nödvändiga. EU-domstolen uttalade vidare att en generell och odifferentierad lagring aldrig kan vara strängt nödvändig, inte ens för att bekämpa grov brottslighet. När det gäller tillgång till uppgifterna fastslog EU-domstolen att precisa krav måste föreskrivas, att tillgång endast får ges för att bekämpa grov brottslighet och att tillgången i

princip bara får avse personer som på något sätt är inblandade i grov brottslighet. Tillgång ska enligt EU-domstolen som huvudregel ges först efter förhandskontroll av domstol eller annan oberoende myndighet och berörda ska informeras, så snart det inte längre skadar myndighetens utredningar. Därutöver uttalade domstolen att leverantörerna av elektroniska kommunikationstjänster måste garantera en särskilt hög skydds- och säkerhetsnivå genom lämpliga tekniska och organisatoriska åtgärder, uppgifterna måste förstöras när lagringstiden gått ut och lagringen måste ske inom unionen. EU-domstolens slutsatser är att EU-rätten utgör ett hinder för (1) en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel samt (2) en nationell lagstiftning som inte begränsar tillgången till trafik- och lokaliseringsuppgifter till enbart åtgärder som syftar till att bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet och inte kräver att uppgifterna ska lagras inom unionen.

Med hänvisning till EU-domstolens dom upphävde kammarrätten föreläggandet från Post- och telestyrelsen.

Internationell utblick

Flera länder har påbörjat analyser av Tele2-domen. I betänkandet redovisas gällande rätt och förändringsarbetet i Danmark, Finland, Tyskland, Belgien, Österrike och Portugal. Värt att notera är att översynerna ännu inte lett till lagstiftning i något land.

Utredningens överväganden

EU-rätten

Av Tele2-domen framgår att EU-domstolen har ansett sig ha kompetens även på området för lagring av och tillgång till datalagrade uppgifter för brottsbekämpande ändamål och för vitala intressen som nationell säkerhet och försvar (p. 65–81 och 119 i domen).

Slutsatsen kan således dras att oavsett för vilket ändamål uppgifterna används så är operatörernas lagring och myndigheternas tillgång till dessa uppgifter underkastade den reglering som följer av EU-rätten. Det innebär att oavsett om det är fråga om brottsbekämpning som handhas av den öppna polisen, Tullverket eller Ekobrottsmyndigheten eller om det är fråga om Säkerhetspolisens brottsbekämpning så är datalagringsfrågan underkastad samma EU-rättsliga regelverk, låt vara att EU-domstolen öppnar för något mer tillåtande nationella regler när det gäller tillgång till uppgifter inom Säkerhetspolisens verksamhetsområde (p. 119 i domen).

Abonnemangsuppgifter omfattas inte av domen men av EU-rätten

EU-domstolens avgörande berör inte behandlingen av abonnemangsuppgifter utan endast trafik- och lokaliseringsuppgifter. Att EU-domstolen inte berör abonnemangsuppgifter är naturligt eftersom de inte berörs i de artiklar i det direktiv (direktiv 2002/58) som tolkas av domstolen. EU-domstolens uttalanden av mer generellt slag om t.ex. inskränkningar i skyddet för personuppgifter är däremot relevanta även för behandlingen av abonnemangsuppgifter. I utredningen har det väckts frågan om ip-adresser ändå ska anses omfattas av domen. Det skulle i så fall innebära att domens föreskrifter om t.ex. föregående domstolsprövning vid tillgång till information om vem som använt en ip-adress skulle bli tillämpliga. Även reglerna om att tillgång endast skulle kunna beredas de brottsbekämpande myndigheterna vid grova brott skulle behöva beaktas. Som ovan angetts är det dock utredningens bedömning att ip-adresser (och andra abonnemangsuppgifter) inte omfattas av domen.

Det är nödvändigt att reformera svensk lagstiftning

EU-domstolen ställer strängare krav på datalagringen och tillgången till datalagrade uppgifter än vad svensk lag gör. De svenska reglerna måste därför anpassas. Härvid måste dock vissa motstående intressen beaktas. För det första måste beaktas att det brottsbekämpande intresset kräver en fungerande lagstiftning kring datalagring. Vissa brott med internet som arena skulle annars riskera att i praktiken bli

helt straffria. För det andra måste beaktas våra internationella åtaganden. Var och en som vistas i Sverige har nämligen rätt att göra anspråk på att staten vidtar effektiva åtgärder för att skydda hans eller hennes säkerhet. I detta ligger att staten måste anstränga sig för att se till att brott förebyggs och utreds samt att gärningsmän ställs till svars för sina brottsliga handlingar. Staten har alltså en skyldighet att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda och om intrång görs se till att brotten utreds. Det skulle inte vara förenligt med Sveriges åtaganden att inte ge de brottsbekämpande myndigheterna möjlighet att använda spåren från den elektroniska miljön.

Ingen generell och odifferentierad lagring som i dag

EU-domstolen fastslår att EU-rätten utgör hinder för en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel. Det framgår även av domskälen att utrymmet för att över huvud taget föreskriva lagring är begränsat. Frågan är då hur begränsat detta utrymme är. EU-domstolen delar upp sitt resonemang i denna fråga i två delar.

Den första delen handlar om generell lagring. EU-domstolen resonerar här kring den svenska lagstiftningen om datalagring och menar att den föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel och ålägger leverantörer av elektroniska kommunikationstjänster att systematiskt och kontinuerligt lagra dessa uppgifter, utan undantag. Domstolens slutsats, som avslutar det första ledet av resonemanget, är att den svenska lagringen överskrider gränsen för vad som är strängt nödvändigt och därför står i strid med artikel 15.1 i direktivet jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan. Domstolen har nu redovisat alla domskäl som behövs för domslutet i denna del. Domstolen fortsätter emellertid sina överväganden i en andra del av resonemanget. Denna andra del har ingen koppling till domslutet utan är närmast att se som ett *obiter*

dictum (dvs. ett uttalande vid sidan om själva saken). Resonemanget här handlar om riktad lagring som ett exempel på en möjlig form av lagring. I denna del resonerar domstolen kring hur en sådan lagring skulle kunna vara utformad. Bland kraven på en riktad lagring märks särskilt att den berörda personkretsen måste vara avgränsad.

Utredningens bedömning är att det finns ett fortsatt utrymme för en begränsad lagringsskyldighet. Men lagringsskyldigheten måste göras mindre omfattande än i dag och anpassas till vad som är strängt nödvändigt.

Olika modeller för lagring

Det bör föreskrivas en viss begränsad och differentierad lagring. De övriga modeller för lagring som kan tänkas (riktad lagring, bevarandeföreläggande, lagring av senaste aktivitet och bibehållen lagring med kryptering eller maskering) är behäftade med sådana svagheter att de inte är rimligt att föreskriva någon av dem i stället.

En begränsad lagringsskyldighet

Utredningens förslag innebär att nuvarande modell för lagringsskyldigheten reformeras kraftigt för telefonitjänst och meddelandehantering samt i viss utsträckning för internetåtkomst. Genom de föreslagna förändringarna blir lagringsskyldigheten inte längre generell; en stor del av trafikuppgifterna kommer inte att omfattas av skyldigheten liksom alla lokaliseringsuppgifter som inte är trafikuppgifter. Lagringen blir därmed undantag och inte huvudregel (Tele2-domen p. 104). Dessutom blir lagringsskyldigheten differentierad genom att den anpassas till att omfatta endast de uppgifter som är strängt nödvändiga att lagra för att bekämpa grov brottslighet, med beaktande av nytta, behov, integritet och proportionalitet (Tele2-domen p. 105). Samtidigt differentieras lagringstiderna utifrån skillnader i behov och uppgifternas integritetskänslighet.

Förslaget innebär att integritetsintrånget för abonnenterna blir lägre men även att möjligheterna att förebygga, förhindra och utreda brott i vissa fall torde försämras.

Redaktionella ändringar och teknikneutralitet

Utredningen föreslår att lagringsskyldigheten delas upp i två delar, dels telefonitjänst och meddelandehantering, dels internetåtkomst. Bestämmelserna görs teknikneutrala. Det betyder bl.a. att operatörernas användning av NAT-teknik (en teknik för att tillåta att flera abonnenter delar på en och samma publika ip-adress) inte påverkar möjligheterna till identifiering av abonnenten.

Telefonitjänst och meddelandehantering

För telefonitjänst och meddelandehantering föreslås att endast uppgifter om kommunikation via en mobil nätanslutningspunkt ska lagras. Det betyder att det inte kommer att lagras några uppgifter vid telefoni eller meddelandehantering som sker inom det fasta telefoninätet eller genom fasta internetanslutningar. Om någon av parterna kommunicerar via en mobil nätanslutningspunkt kommer däremot information att lagras, men bara hos den partens operatör. Trafikuppgifter ska fortfarande lagras. Men lagringsskyldigheten begränsas till uppgifter om vem som kontaktat vem (nummer och abonnent samt för telefonitjänst även abonnemangsidentitet och utrustningsidentitet) och vid vilken tidpunkt. Uppgifter om ip-adress ska i sig inte lagras vid telefonitjänst och meddelandehantering. Uppgift om vilken tjänst som använts, tid för på- och avloggning i tjänsten och uppgift om utrustning där kommunikationen vid ip-telefoni slutligt avskiljs (se dock nedan om internetåtkomst) ska inte omfattas av lagringsskyldigheten. Lokaliseringsuppgifter ska fortfarande lagras vid ett samtals början och slut. Men precis som tidigare ska inga andra lokaliseringsuppgifter lagras. För förbetalda anonyma tjänster (dvs. oregistrerade kontantkort) ska uppgift om kommunikationsutrustning och första aktivering fortfarande lagras. Lagringsskyldigheten ska fortfarande omfatta misslyckade uppringningar, t.ex. obesvarade samtal – men inte samtal som inte kopplas fram.

Internetåtkomst

För internetåtkomst föreslår utredningen att lagringsskyldigheten ska omfatta uppgifter som gör det möjligt att identifiera abonnenten eller den registrerade användaren. Därmed ska det lagras ip-adress och annan teknisk uppgift som är nödvändig för att identifiera abonnenten eller den registrerade användaren, tidsuppgifter för på- och avloggning i tjänsten som ger internetåtkomst, uppgifter om abonnent och registrerad användare och uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs. Det ska däremot inte längre finnas någon skyldighet att lagra uppgifter om anslutningskapacitet.

Inget undantag för personer med tystnadsplikt

Det bör inte införas något undantag från lagringen för personer med tystnadsplikt. Datalagringsutredningens förslag om att införa en förstörandeskyldighet för uppgifter som omfattas av yrkesmässig tystnadsplikt bör övervägas.

Lagringskyldighetens ramar bör framgå av lag

Lagringsskyldighetens yttre ramar bör framgå av lag och de mer detaljerade föreskrifterna av förordning. I viss utsträckning bör regeringen kunna delegera denna föreskriftsrätt.

En differentierad lagringstid

Det ska i lag anges att de uppgifter som omfattas av lagringsskyldigheten ska lagras den tid regeringen föreskriver dock som längst i tio månader räknat från den dag då kommunikationen avslutades. Regeringen ska föreskriva följande. Lokaliseringsuppgifter vid samtal ska lagras i två månader. Uppgifter om internetåtkomst, förutom uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs, ska lagras i tio månader. Övriga uppgifter ska lagras i sex månader.

Tillgången till trafik- och lokaliseringsuppgifter

Endast för att bekämpa grov brottslighet

Tillgång till lagrade trafik- och lokaliseringsuppgifter ska endast ges för bekämpning av grov brottslighet. Med grov brottslighet avses samma kategorier av brott som i dag möjliggör hemlig övervakning av elektronisk kommunikation och inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Svensk rätt är således förenlig med EU-rätten i detta hänseende.

Tillgång bara till uppgifter om personer som på något sätt är inblandade i brott – som huvudregel

Tillgång till lagrade uppgifter kan enligt domstolen i princip bara beviljas till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. I vissa fall kan tillgång ges även till uppgifter om andra personer. De svenska reglerna om tillgång till uppgifter uppfyller EU-rättens krav i detta hänseende.

Förhandskontroll av domstol eller oberoende myndighet

EU-rätten kräver att de brottsbekämpande myndigheternas tillgång till datalagrade uppgifter, utom i motiverade brådskande fall, ska föregås av en kontroll av domstol eller en oberoende myndighet. Det svenska regelverket uppfyller detta krav utom vid inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. Utredningen föreslår därför att åklagare utses som oberoende myndighet att fatta beslut om sådan inhämtning efter ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket.

Information till de berörda

EU-domstolen fastslår att EU-rätten kräver att de myndigheter som har beviljats tillgång till lagrade uppgifter, enligt tillämpliga nationella bestämmelser, informerar de berörda personerna om detta så

snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar. De svenska reglerna om information till de berörda uppfyller EU-rättens krav i detta hänseende.

Tillgången ska avse även uppgifter som lagras för operatörernas egna ändamål

De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation ska alltjämt avse inte bara de uppgifter som sparas enligt datalagringsreglerna utan också den information som sparas för operatörernas egna ändamål, t.ex. uppgifter som behövs för fakturering.

Tillgången till abonnemangsuppgifter

Som nämns ovan omfattar inte Tele2-domen behandling av abonnemangsuppgifter. Med den breda omfattning som skyddet för privatliv har, får tillgången till abonnemangsuppgifter ändå anses innebära ett ingrepp i skyddet enligt Europakonventionen och rättighetsstadgan. Det krävs därför att tillgången är begränsad till vad som är strängt nödvändigt och proportionerligt i ett demokratiskt samhälle. Sammantaget är det utredningens bedömning att varken EU-domstolens dom eller Sveriges internationella åtaganden ger anledning att förändra förutsättningarna för de brottsbekämpande myndigheternas tillgång till uppgifter om abonnemang.

Skydds- och säkerhetsnivåer, lagring inom Sverige och utplåning

Uppgifterna som omfattas av lagringsskyldigheten ska inte få lagras utanför Sverige. EU-domstolen anger i och för sig endast att den nationella lagstiftningen måste föreskriva att datalagrade uppgifter inte ska få lagras utanför unionen. Genom att lagringen begränsas till Sverige uppnås emellertid en mer potent tillsyn samtidigt som både enskilda personers konfidentialitet och nationell säkerhet skyddas på ett bättre sätt. Eftersom den nu aktuella frågan rör centrala intressen

för staten finns inga EU-rättsliga hinder för att föreskriva att uppgifterna endast ska få lagras i Sverige.

Reglerna om skydds- och säkerhetsnivå uppfyller de krav som EU-rätten ställer. Reglerna om utplåning uppfyller de krav som EU-rätten ställer.

Konsekvenser och genomförande

Förslagen om en ändrad lagringsskyldighet, förbud mot lagring utanför Sverige och förhandsprövning vid beslut enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet kommer att stärka integritets- och personuppgiftsskyddet. Förslaget om en ändrad lagringsskyldighet kommer möjligen att innebära att de brottsbekämpande myndigheternas förmåga att bekämpa brottslighet försämras i någon mån men torde inte innebära att brottsligheten kommer att öka. Miljön kommer inte att påverkas av förslagen. Förslaget om förhandsprövning av beslut enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet innebär att Åklagarmyndigheten kommer att behöva ett större årligt anslag (1 miljon kronor) och ett engångsbelopp (3 miljoner kronor) som bör finansieras med neddragning av anslagen för Polismyndigheten (500 000 kronor för den löpande ramhöjningen och 1,5 miljoner kronor för engångsbeloppet), Säkerhetspolisen (200 000 kronor för den löpande ramhöjningen och 600 000 kronor för engångsbeloppet) och Tullverket (300 000 kronor för den löpande ramhöjningen och 900 000 kronor för engångsbeloppet). Den kostnadsökning som drabbar de lagringsskyldiga för lagring, säkerhet och anpassning ska de själva stå för.

Förslagen i betänkandet ska träda i kraft den 1 december 2018.

Summary

The Commission's mandate and work

The interpretation of EU law by the Court of Justice of the European Union (CJEU) in its Tele2 judgment has necessitated reform of the Swedish rules on data retention, regarding both retention and access. This Commissions mandate has been to make these Swedish rules compatible with EU law. This mandate has included considerations in an area that is highly complex, both legally and technically. It has also been carried out with great promptness owing to the urgency of putting in place regulation consistent with the CJEU's statements in the Tele2 judgment. Experts from Swedish law enforcement and supervisory agencies, Sweden's courts, the Swedish Bar Association, Uppsala University and the Swedish Government Offices have served as experts in the Commission.

Fundamental rights

Fundamental rights that are guaranteed to individuals are laid down in Sweden's Instrument of Government (part of the Constitution), the European Convention on Human Rights and the Charter of Fundamental Rights of the EU. Individuals' fundamental rights are twofold: first, their right to be protected from violations by the state, and, second, the state's duty to ensure – by, for example, a crime investigation – individuals' protection against violations by other individuals. It is incumbent on the state to establish a framework that is reconcilable with these partially competing principles.

The rights that are of primary interest for the mandate are the right to private life, the right to protection of personal data and the right to freedom of expression. All these rights are guaranteed by

Sweden's Instrument of Government, the European Convention on Human Rights and the Charter of Fundamental Rights of the EU.

Privacy protection in electronic communications

To ensure full respect for the right to private life and the right to protection of personal data in the electronic communications sector, the EU adopted Directive 2002/58. This Directive requires member states to, for example, ensure confidentiality in electronic communications and associated traffic data. Data that are no longer needed must, under the Directive, be destroyed or de-identified. However, the member states may make exceptions to these obligations if it is necessary for e.g. crime fighting activities. The Directive has been implemented in Swedish law mainly through provisions in the Electronic Communications Act (2003:389).

Crime fighting

Crime fighting activities consist of two main parts: intelligence and investigative work. Intelligence activities focus mainly on revealing whether particular crimes, not specified in detail, have taken or are taking place, or may be expected to be committed. One overall goal of intelligence work is to supply law enforcement agencies with knowledge that can be brought to bear in their operations. Investigative activity, in contrast, is based on an event that has already occurred. The agency's task is to find out, often in a preliminary investigation, whether crimes have been committed and, if so, who may be reasonably suspected of committing them, and to obtain enough material to assess the question of whether to prosecute.

In both criminal investigation and intelligence work, secret coercive measures are used. One such measure relevant to the issue of data retention is secret monitoring of electronic communications, which is regulated by the Swedish Code of Judicial Procedure. In addition, there are coercive measures under the Act (1991:572) concerning Special Controls in Respect of Aliens and the Act (2007:979) on the Use of Measures to Prevent Certain Serious Crimes that are applicable in intelligence activities. Data retrieval under the Act (2012:278) on Acquiring Information about Electronic

Communications in the Law Enforcement Agencies' Intelligence Activities also constitutes a secret coercive measure. However, collection of subscription data under the Electronic Communications Act (2003:389) is not a secret coercive measure.

Data on electronic communication in crime fighting

Data on electronic communications are divided into various categories. Subscription data comprise, for example, subscribers' numbers, names, titles and addresses. Such data are also usually deemed to include information about contracts and billing, for example. Moreover, this category includes information on which fixed or dynamic ip address a subscriber has used or IMSI numbers (those are associated with subscribers' SIM cards and thus telephone numbers), and several other particulars. The exact boundary is difficult to draw. Traffic data refers in this context, simply expressed, to the data needed to convey an electronic message in an electronic communications network, or to invoice for such a message. Besides the concept of 'traffic data', the expression location data is also used, to denote data associated with the location of a communication device. It may, for example, be about the cell (base station antenna) to which the equipment is connected.

Current regulation of data retention

Data on electronic communications are very important for crime fighting. There are therefore rules in the Electronic Communications Act (2003:389) to ensure that public agencies can access such data. To this end, the Electronic Communications Act prescribes a retention obligation for those providing electronic communications services. This obligation includes certain listed data generated or processed by the provider. The obligation to retain includes telephony (fixed and mobile), messaging and Internet access.

Current regulation of data access

How public agencies can access the data covered by the obligation to retain – and other data processed in their work, for example owing to billing requirements – depends on what type of information is involved and the purpose for which access is requested. For traffic and location data, access is regulated in the Code of Judicial Procedure and the Act (2012:278) on Gathering of Data relating to Electronic Communications as Part of Intelligence Gathering by Law Enforcement Authorities. In addition, there are the Act (1991:572) concerning Special Controls in Respect of Aliens and the Act (2007:979) on Measures to Prevent Certain Particularly Serious Crimes, which refer to the provisions of the Code of Judicial Procedure. Access to subscription data has not been considered to be a secret coercive measure, and is regulated directly in the Electronic Communications Act (2003:389).

Access to traffic and location data in the criminal investigative process requires court decisions and is possible only in cases of serious crime. In intelligence activities, access to traffic data is more limited but, as a main rule, does not require court decisions. Access to subscription data does not require any court decision; the decision is taken by the law enforcement agency itself. Nor is the crime required to be of a particular degree of seriousness.

To protect individuals' data privacy and maintain a high level of legal certainty, the regulations governing public agencies' access to electronic communications data contain a number of control mechanisms and guarantees of legal certainty.

For all use of coercive measures, the principles of purpose, need and proportionality apply. Consequently, the coercive measures may be used only for the purpose specified in the legislation, if there is an obvious need and a smaller intervention measure is insufficient. In addition, the measure must be in reasonable proportion to both the benefit resulting from, and the intrusion or harm entailed by, the measure.

Benefit of and need for electronic communication data in crime fighting

To combat crime, there is an obvious need for data on electronic communications, and these data are immensely useful to law enforcement agencies. This applies to all data to be retained pursuant to the Electronic Communications Ordinance (2003:396). However, benefit and need are not the same for all data, nor constant over time, since behaviour patterns and technology are constantly changing. Examples are the decline of fixed telephony, growing Internet access in mobile phones and increased use of IP telephony through mobile apps.

Impact of EU law on data retention rules

The EU Data Retention Directive (2006/24/EC) was annulled by the CJEU on 8 April 2014 (the Digital Rights judgment) and, for this reason, the head of the Ministry of Justice tasked an investigator with analysing the implications for Swedish legislation (Ministry Publication Series, Ds 2014:23). To follow up the analysis in the departmental memorandum, the Government instructed a special investigator to consider further measures to boost legal certainty and data privacy for such rules as those on retention of data concerning electronic communication (Swedish Government Official Report, SOU 2015:31). In both analyses, the Swedish legislation was judged to be compatible with EU law, although some reform proposals were presented.

The Tele2 judgment and the Administrative Court of Appeal in Stockholm judgment

The Administrative Court of Appeal in Stockholm requested a preliminary ruling by the CJEU on an injunction, which had been appealed, from the Swedish Post and Telecom Authority against a company obliged to retain data about storing data on electronic communication. The CJEU's response to the request was the Tele2 judgment. The CJEU considered Directive 2002/58 to be applicable to the Swedish rules on data retention, with respect to data access as

well. According to the CJEU, Article 15.1 of the Directive, which to some extent allows data retention, should be interpreted strictly and in light of the Charter of Fundamental Rights. The Swedish rules on data retention were judged to constitute restrictions on the rights under Articles 7, 8 and 11. According to the CJEU, restrictions on rights may be imposed only under certain conditions, including their being proportionate and strictly necessary. The CJEU further stated that general and indiscriminate retention can never be strictly necessary – not even to fight serious crime. Regarding access to data, the Court states that precise requirements must be prescribed, that access may be given only for the purpose of fighting serious crime and that access may, in principle, relate only to people involved in some way in serious crime. According to the Court, access should, as a main rule, be granted only after prior judicial review by a court or other independent agency, and the people concerned should be informed as soon as this is no longer detrimental to the agency's investigations. In addition, the Court states that providers of electronic communications services must guarantee a particularly high level of protection and security through appropriate technical and organisational measures; that the data must be destroyed when the retention period expires; and that the data must be stored in the EU. The CJEU's conclusions are that EU law precludes (1) national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication and (2) national legislation that does not restrict access to traffic and location data solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union.

With reference to the CJEU's judgment, the Administrative Court of Appeal suspended the injunction from the Swedish Post and Telecom Authority.

International outlook

Several countries have started analysing the Tele2 judgment. The Commission's report gives an account of current law and reform under way in Denmark, Finland, Germany, Belgium, Austria and Portugal. It is worth noting that these reviews have not yet led to legislation in any country.

The Commission's considerations

EU law

The Tele2 judgment shows that the CJEU has deemed its own legal competence to include retention of and access to electronically retained data for the purpose of preventing crime, and also vital interests such as national security and defence (pp. 65–81 and 119 of the judgment). The conclusion may thus be drawn that, regardless of the purpose for which the data are used, the operators' retention of and the agencies' access to these data are subject to the rules pursuant to EU law. This means that, irrespective of whether the crime fighting is pursued by the Police Authority, Swedish Customs, the Swedish Economic Crime Authority or the Swedish Security Service, the issue of data retention is subject to the same EU legal framework, although the CJEU allows slightly more leeway for national rules regarding access to data in the Security Service's area of operations (p. 119 of the judgment).

Subscription data excluded from judgment but covered by EU law

The CJEU's decision does not concern processing of subscriber data, but only traffic and location data. The fact that the Court does not touch on subscription data is natural since they are not dealt with in the articles of the Directive (2002/58) that the Court interprets. The Court's more general statements on, for example, limitations on protection of personal data are, on the other hand, also relevant to processing of subscription data. In the Commission, the question has been raised of whether IP addresses should nevertheless be regarded as covered by the judgment. If so, it would

mean that the provisions in the judgment concerning prior review by a court or an independent administrative authority when there is access to information on who has used an IP address, for example, would be applicable. The rules that access might be made available to law enforcement agencies only in cases of serious crime would also need to be considered. As stated above, however, the Commission's view is that neither IP addresses nor any other subscription data are covered by the judgment.

Necessity of Swedish legislative reform

The CJEU imposes more stringent requirements than Swedish law on data retention and access to electronically retained data. The Swedish rules must therefore be reformed. However, certain opposed interests must be considered. First, it must be taken into account that the interest of law enforcement calls for effective legislation on data retention. Otherwise, there would be a risk of complete impunity in practice for certain crimes with the Internet as their arena. Second, our international commitments must be taken into account. Every single resident in Sweden is entitled to demand effective measures by the state to protect his or her safety. Accordingly, the state must strive to ensure that crime is prevented and investigated, and that perpetrators are held accountable for their criminal acts. The state thus has an obligation to protect individuals' private life and data privacy against intrusions by other individuals and, in the event of intrusions, ensure that these crimes are investigated. Failing to enable law enforcement agencies to effectively collect evidence in the electronic environment would not be compatible with Sweden's commitments.

No general and indiscriminate retention as at present

The CJEU has stated that the EU law constitutes an obstacle to national legislation that, for crime fighting purposes, prescribes general and indiscriminate retention of all traffic and location data concerning all subscribers and registered users, and for all electronic means of communication. It is also clear from the grounds for the judgment that the scope for generally prescribing retention is limited.

The question is then how limited this scope is. The CJEU sets out its reasoning on this issue in two sections.

The first section of the reasoning is about general retention. Here, in considering Swedish legislation on data retention, the CJEU takes the view that existing legislation provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions. The Court's conclusion, at the end of the first section of its reasoning, is that Swedish retention exceeds the limit of what is strictly necessary and therefore contravenes Article 15.1 of the Directive, compared with Articles 7, 8, 11 and 52.1 in the Charter of Fundamental Rights. The Court has now stated all the grounds required for its ruling in this section.

Nevertheless, the Court continues its considerations in a second section of the reasoning. This second part has no connection with the ruling; instead, it may almost be seen as an *obiter dictum* (i.e. an incidental expression of opinion outside the scope of the case). Here, the reasoning is about targeted data retention as an example of a retention compatible with the EU-law. In this part, the Court presents arguments on the possible nature of such data retention. Among the requirements for a targeted retention, the fact that the circle of individuals concerned must be limited is especially notable.

The Commission's assessment is that scope for a limited retention obligation remains, but that the obligation must be made less extensive than today and adapted to what is strictly necessary.

Various retention models

A limited and differentiated retention should be prescribed. The other possible retention models (targeted data retention, data preservation, retention of the latest activity and continued data retention with encryption or anonymization) entail such weaknesses that it is not reasonable to prescribe any of them instead.

Limited retention obligation

The Commission's proposal involves a radical reform of the current model for the retention obligation for telephony, messaging and, to a certain extent, Internet access. Owing to the proposed changes, the obligation will no longer be general; much of the traffic data, as well as all location data that are not traffic data, will not be subject to the obligation. Retention will thus become the exception, not the rule (Tele2 judgment p. 104). In addition, the obligation to retain data will be differentiated by being adapted to cover only data that are strictly necessary to retain for fighting serious crime, taking usefulness, needs, data privacy and proportionality into account (Tele2 judgment p. 105). At the same time, retention periods will be differentiated on the basis of divergent needs and differing sensitivity in terms of privacy.

The proposal means that the infringement on subscribers' privacy would be reduced, but that scope for obstructing, preventing and investigating crime may also, in some cases, be impaired.

Editorial changes and technology neutrality

The Commission recommends dividing the retention obligation into two parts: (1) telephony and messaging and (2) Internet access. The rules should be made technology-neutral. One implication of that is that operators' use of NAT technology (which allows subscribers to share the same public IP address) would not affect the scope for identifying subscriber.

Telephony and messaging

For telephony and messaging, the proposal is that only data on communications via a mobile network access point should be retained. This means that no data would be retained on telephony or messaging that takes place in the fixed-line (landline) telephone network or through fixed Internet access. On the other hand, information will be retained if one of the parties communicates via a mobile network access point, but only at that party's service provider.

Traffic data will still be retained; but the obligation to retain will be limited to data on who contacted whom (number and subscriber, and for telephony also subscription and equipment numbers) and at what time. Data on IP addresses should not be retained for telephony and messaging. The same applies to data on which service has been used, time of logging into and out of the service and data identifying the equipment where the communication with IP telephony is finally separated to the subscriber (see below on Internet access, however). Location data at the beginning and end of a call will still be retained but, as before, no other location data will be retained. For prepaid anonymous services (i.e. unregistered prepaid phone cards), information about communication equipment and initial activation will still be retained. The retention obligation should still include missed (such as unanswered) calls, but not those that fail to get connected.

Internet access

For Internet access, the Commission proposes that the retention obligation should include data that make it possible to identify the subscriber or registered user. Accordingly, the following data should be retained: IP address and other technical data necessary to identify the subscriber or registered user, time data for logging in and out of the service providing Internet access, subscriber information, and data identifying the equipment where the communication is finally separated to the subscriber. However, the Commission suggests that there should no longer be any obligation to retain connection capacity data.

No exception for people bound by professional secrecy

No exceptions to retention should be introduced for people obliged to follow professional secrecy rules. The Data Retention Commission's proposal to impose an obligation to destroy data subject to professional secrecy rules should be considered.

Limits of retention obligation to be clarified by law

The outer limits of the retention obligation should be made clear by law and the more detailed regulations in an ordinance by the Government. To some extent, the Government should be able to delegate the power to issue the necessary ordinance.

Differentiated retention periods

It should be specified in law that the data subject to the retention obligation should be stored for the period prescribed by the Government, but not exceeding ten months from the date when the communication ended. The Government shall prescribe the following. Location data for calls should be stored for two months. Data on Internet access, except for data identifying the equipment where the communication is finally separated to the subscriber, should be retained for ten months. Other data should be retained for six months.

Access to traffic and location data

Only for prevention of serious crime

Access to retained traffic and location data should be given only for prevention of serious crime. 'Serious crime' refers to the same categories of crime for which secret surveillance of electronic communications is currently permitted and also for retrieval of data on electronic communications in the law enforcement agencies' intelligence activities. Swedish law is thus compatible with EU law in this respect.

Access only to data on people involved in some way in crime – as a main rule

Access to retained data may in principle, according to the Court, be granted only for data on people suspected of planning, committing or having committed a serious crime or being implicated in one way or another in such a crime. In some cases, access may also be granted

for data on other people. The Swedish rules on access to data comply with EU legal requirements in this respect.

Prior review by a court or by an independent administrative body

EU law requires that access by law enforcement agencies to retained data, except in justified urgent cases, be preceded by a prior review by a court or by an independent administrative body. The Swedish regulations meet this requirement except for access to retained data in intelligence activities. The Commission therefore proposes that prosecutors shall be appointed as an independent administrative body to decide on such access following an application by the Police Authority, Security Service or Customs.

Information for those concerned

The CJEU states that EU law requires the public agencies that have been granted access to retained data, according to applicable national regulations, to inform the people affected about this as soon as there is no longer a risk of such information being detrimental to the agencies' investigations. The Swedish rules on information for those concerned meet the requirements of EU law in this respect.

Access to include data stored for operators' own purposes

Law enforcement agencies' access to data on electronic communications should continue to include not only the data retained under data retention rules, but also information stored for the operators' own purposes, such as information needed for billing.

Access to subscription data

As mentioned above, the Tele2 judgment does not cover processing of subscription data. With the broad scope of privacy protection, access to subscription data may nonetheless be thought to involve an interference with the protection under the European Convention on Human Rights and the Charter of Fundamental Rights. It is there-

fore essential for access to be limited to what is strictly necessary and proportionate in a democratic society. Overall, the Commission's view is that neither the CJEU's judgment nor Sweden's international commitments provide any reason to change the requirements for the law enforcement agencies' access to subscription data.

Protection and security levels, retention in Sweden and destruction

The data subject to the retention obligation should not be allowed to be stored outside Sweden. The CJEU states only that national legislation must prescribe that electronic data storage may not take place outside the EU. However, confining the retention to Sweden would enable more effective supervision while improving protection of both individuals' confidentiality and national security. Since the matter now in question concerns crucial state interests, there are no EU legal barriers to prescribing that storage takes place only in Sweden.

The rules on protection and security levels, and also those on data destruction, comply with the requirements of EU law.

Impact and implementation

The proposals for a reformed retention obligation, prohibition of retention outside Sweden and advance review of decisions pursuant to the Act (2012:278) on Acquiring Information about Electronic Communication in the Law Enforcement Agencies' Intelligence Activities will strengthen protection for privacy and personal data. The recommended reform of the retention obligation may possibly mean that the law enforcement agencies' capacity for crime fighting is impaired to some extent, but should not mean that crime will increase. The environment will not be affected by the proposals. The proposal on prior review of decisions pursuant to the Act (2012:278) on Acquiring Information about Electronic Communication in the Law Enforcement Agencies' Intelligence Activities means that the Swedish Prosecution Authority will need a larger annual appropriation (SEK 1 million) and a lump sum (SEK 3 million) that should be financed by reducing appropriations for the Police Authority

(SEK 500,000 for the current framework increase and SEK 1.5 million for the lump sum), the Security Service (SEK 200,000 for the current framework increase and SEK 600,000 for the lump sum) and Customs (SEK 300,000 for the current framework increase and SEK 900,000 for the lump sum). Those who are obliged to retain data should bear the cost increases they incur – for retention, security and adaptation – themselves.

The proposals in the Commission's report should enter into force on 1 December 2018.

1 Författningsförslag

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

Härigenom föreskrivs att 6 kap. 16 d § lagen (2003:389) om elektronisk kommunikation ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	16 d §[1]
Uppgifter som avses i 16 a § ska lagras *i sex* månader räknat från den dag kommunikationen avslutades. Vid utgången av denna tid ska den lagringsskyldige genast utplåna dem, om annat inte följer av andra stycket.	Uppgifter som avses i 16 a § ska lagras *den tid regeringen föreskriver dock som längst i tio* månader räknat från den dag kommunikationen avslutades. Vid utgången av denna tid ska den lagringsskyldige genast utplåna dem, om annat inte följer av andra stycket.

Om uppgifter som avses i första stycket begärts utlämnade före utgången av den föreskrivna lagringstiden men uppgifterna inte har hunnit lämnas ut, ska den lagringsskyldige lagra uppgifterna till dess så har skett och därefter genast utplåna de lagrade uppgifterna.

Denna lag träder i kraft den 1 december 2018.

---

[1] Senaste lydelse 2012:127.

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

Härigenom föreskrivs att 4–6 §§ lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
4 §	
Beslut om inhämtning av uppgifter fattas av *myndigheten. Myndighetschefen får delegera rätten att fatta beslut om inhämtning till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs.*	Beslut om inhämtning av uppgifter fattas av *åklagare efter ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket*.
Den som rätten att fatta beslut har delegerats till, får inte fatta beslut om inhämtning i sådan operativ verksamhet som han eller hon deltar i.	
5 §	
I ett beslut om inhämtning av uppgifter ska det anges vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet avser. Tiden får inte bestämmas längre än nödvändigt och får, när det gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.	
Om det inte längre finns skäl för ett beslut om inhämtning av uppgifter, ska beslutet omedelbart hävas.	Om det inte längre finns skäl för ett beslut om inhämtning av uppgifter, ska beslutet omedelbart hävas *av den ansökande myndigheten*.

6 §

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.

Underrättelse enligt första stycket ska fullgöras av den ansökande myndigheten.

Denna lag träder i kraft den 1 december 2018.

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

Härigenom föreskrivs i fråga om förordningen (2003:396) om elektronisk kommunikation[2]

dels att 42 och 43 §§ ska upphöra att gälla,

dels att 37–41 och 44 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
37 §[3]	
Den som är skyldig att lagra uppgifter enligt 6 kap. 16 a § lagen (2003:389) om elektronisk kommunikation ska vidta de åtgärder som krävs 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.	
Den lagringsskyldige ska vidta de åtgärder som krävs för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring. Sådana åtgärder ska även vidtas för att förhindra otillåten lagring, behandling av eller tillgång till och otillåtet avslöjande av uppgifterna. Uppgifterna får göras tillgängliga endast för personal med särskild behörighet.	
	Uppgifterna får inte lagras utanför Sverige.
Post- och telestyrelsen får, efter att ha hört Polismyndigheten, Säkerhetspolisen och Datainspektionen, meddela närmare föreskrifter om de åtgärder som ska vidtas enligt första och andra styckena.	
38 §[4]	
För att fullgöra lagringsskyldigheten i 6 kap. 16 a § lagen (2003:389) om elektronisk kom-	För att fullgöra lagringsskyldigheten i 6 kap. 16 a § lagen (2003:389) om elektronisk kom-

[2] Senaste lydelse av
42 § 2012:128
43 § 2012:128.
[3] Senaste lydelse 2014:1270.
[4] Senaste lydelse 2012:128.

munikation ska den lagringsskyldige lagra de uppgifter som anges i 39–*43* §§.	munikation ska den lagringsskyldige lagra de uppgifter som anges i 39 *och 40* §§.
	39 §[5]
När det gäller *telefonitjänst* ska följande lagras:	När det gäller *internetåtkomst* ska följande lagras:
1. uppringande nummer,	*1. användares ip-adress och annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare,*
2. uppringt nummer och nummer som samtalet styrts till,	*2. uppgifter om abonnent och registrerad användare,*
3. uppgifter om uppringande och uppringd abonnent och, i förekommande fall, registrerad användare,	*3. datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomst, och*
4. datum och spårbar tid då kommunikationen påbörjades och avslutades, och	*4. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.*
5. uppgifter om den eller de tjänster som har använts.	*Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten är någon som inte omfattas av 6 kap. 16 a § lagen (2003:389) om elektronisk kommunikation, ska första stycket 4 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.*

[5] Senaste lydelse 2012:128.

40 §[6]

När det gäller telefonitjänst via en mobil nätanslutningspunkt ska, *utöver det som anges i 39 §*, följande lagras:	När det gäller telefonitjänst *och meddelandehantering* via en mobil nätanslutningspunkt ska följande lagras:
1. uppringandes och uppringds abonnemangsidentitet och utrustningsidentitet,	*1. uppringande och uppringt nummer eller motsvarande adress,*
2. lokaliseringsuppgifter för kommunikationens början och slut, och	*2. såvitt avser telefonitjänst uppringandes och uppringds abonnemangsidentitet och utrustningsidentitet,*
3. datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst.	*3. uppgifter om abonnent och registrerad användare som uppgifterna i 1 och 2 kan hänföras till,*
	4. datum och spårbar tid då kommunikationen påbörjades och avslutades eller ett meddelande skickades och mottogs,
	5. såvitt avser telefonitjänst lokaliseringsuppgifter då kommunikationen påbörjades och avslutades, och
	6. datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst.

41 §[7]

När det gäller telefonitjänst som använder ip-paket för överföring ska, utöver det som anges i 39 och 40 §§, följande lagras:	*Med stöd av 6 kap. 16 d § lagen (2003:389) om elektronisk kommunikation förordnas att:*
1. uppringandes och uppringds ip-adresser,	*1. uppgifter som avses i 39 § första stycket 1–3 ska lagras i tio månader,*

[6] Senaste lydelse 2012:128.
[7] Senaste lydelse 2012:128.

2. datum och spårbar tid för på- och avloggning i den eller de tjänster som använts, och	*2. uppgifter som avses 39 § första stycket 4 och andra stycket samt 40 § 1–4 och 6 ska lagras i sex månader, och*
3. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.	*3. uppgifter som avses i 40 § 5 ska lagras i två månader.*
Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten är någon som inte omfattas av 6 kap. 16 a § lagen (2003:389) om elektronisk kommunikation, ska första stycket 3 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.	
44 §[8]	
Post- och telestyrelsen får meddela närmare föreskrifter *om* de uppgifter som ska lagras enligt 39*–43* §§.	Post- och telestyrelsen får meddela närmare föreskrifter *som rör* de uppgifter som ska lagras enligt 39 *och 40* §§. *Post- och telestyrelsen får också meddela föreskrifter om vilka närmare uppgifter som ska lagras enligt 39 och 40 §§.*

1. Denna förordning träder i kraft den 1 december 2018.

2. Lagringsskyldigheten enligt 39 § första stycket 1 om annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare behöver inte tillämpas förrän den 1 april 2019.

[8] Senaste lydelse 2012:128.

2 Utredningens uppdrag och arbete

2.1 Utredningens uppdrag

Regeringen beslutade den 16 februari 2017 att ge en särskild utredare i uppdrag att se över bestämmelserna om skyldighet att lagra uppgifter om elektronisk kommunikation som gäller leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster[1], samt bestämmelserna om de brottsbekämpande myndigheternas tillgång till sådana uppgifter. Översynen ska ske i syfte att anpassa det svenska regelverket till EU-rätten såsom den uttolkats av EU-domstolen i Tele2-domen. Utredaren fick även i uppdrag att se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när hemliga tvångsmedel för särskilt allvarlig brottslighet används, vilket kommer att redovisas i ett senare betänkande.

Enligt utredningens direktiv bör det även fortsättningsvis finnas ett utrymme för tvingande regler för leverantörernas lagring av uppgifter om elektronisk kommunikation men måste det utredas hur stort det utrymmet är och vilket behov som finns av en sådan lagring. En särskild fråga enligt direktiven är vilken effekt EU-domstolens dom har på verksamheten som avser Sveriges säkerhet, dvs. sådan verksamhet som ligger inom Säkerhetspolisens ansvarsområde.

Även regelverket om tillgång till lagrade uppgifter behöver enligt direktiven ses över, bl.a. vad gäller vilka krav som bör ställas på brottets allvar för att uppgifterna ska få hämtas in, krav på underrättelse till enskilda, beslutsordningen för inhämtning och om ett

[1] I betänkandet används termerna operatör och leverantör synonymt med lagringsskyldig och inte med den distinktion som följer av LEK, i den mån inte annat framgår av sammanhanget. Därtill används ibland termen lagringsskyldig.

särskilt skydd behövs för uppgifter som omfattas av yrkesmässig tystnadsplikt.

I direktiven uppmärksammar regeringen vidare att EU-domstolen i Tele2-domen uttalat sig om skyddet och säkerheten för de lagrade uppgifterna, däribland att leverantörerna av elektroniska tjänster måste garantera en särskilt hög skydds- och säkerhetsnivå, att den nationella lagstiftningen måste föreskriva att lagringen sker inom unionen, att uppgifterna oåterkalleligen förstörs när lagringstiden gått ut samt att det utförs kontroll av en oberoende myndighet.

Mot denna bakgrund ska utredningen enligt direktiven analysera hur reglerna om lagring av uppgifter enligt 6 kap. 16 a § LEK och 39–43 §§ FEK, reglerna om tillgång till de lagrade uppgifterna samt reglerna om skydd av och säkerhet för dessa uppgifter förhåller sig till EU-domstolens dom. Därutöver ska utredningen överväga olika alternativ till förändringar i de delar reglerna inte är förenliga med domen, belysa fördelar och nackdelar med alternativen samt föreslå författningsändringar och andra åtgärder som behövs.

I uppdraget ingår även en internationell utblick. Utredaren ska redovisa gällande rätt och pågående arbete i Finland och Danmark och de övriga länder som bedöms vara relevanta. Vidare ska utredaren följa arbetet på EU-nivå.

Utredaren får enligt direktiven ta upp sådana närliggande frågor som har samband med de frågeställningar som ska utredas. Exempel på en sådan fråga är vilken efterhandskontroll som bör finnas samt om någon myndighet bör ha tillsyn över att uppgifter om elektronisk kommunikation lämnas ut på ett korrekt sätt.

2.2 Utredningsarbetet

Uppdraget har inrymt överväganden inom ett mycket komplext område, både juridiskt och tekniskt. Det har dessutom utförts under stor skyndsamhet eftersom det har varit angeläget att snabbt få en reglering på plats som är förenlig med de uttalanden som EU-domstolen gjort i Tele2-domen. Utredningen har haft flera sammanträden med de förordnade experterna. Därutöver har utredningen haft ett separat möte med experter från Polismyndigheten, Säkerhetspolisen och Tullverket, för att närmre utreda myndigheternas behov av lagrade uppgifter om elektronisk kommunikation. I samma

syfte har studiebesök genomförts hos Åklagarmyndigheten, Polismyndigheten och Säkerhetspolisen. Utredningen har även haft sammanträden med en grupp företrädare från it- och telekomföretagen. Gruppen har utformats av branchorganisationen IT&Telekomföretagen och bestått av företrädare från branchorganisationen samt från Bahnhof, Comhem, Hi3G, Tele2, Telenor och Telia. Utredningen har även haft kontakt med personer som arbetar med motsvarande frågor i andra unionsländer och på EU-nivå. Därtill har utredningen samrått med bl.a. Beslagsutredningen (Ju 2016:08), Utredningen om hemlig dataavläsning (Ju 2016:12) och Utredningen om självkörande fordon (N 2015:07). Slutligen har utredningen tagit del av synpunkter från enskilda personer och organisationer.

Den näraliggande fråga om efterhandskontroll som nämns i direktiven har inte varit möjliga att behandla.

2.3 Betänkandets disposition

Den efterföljande delen av betänkandet inleds med avsnitt 3, om enskildas grundläggande rättigheter, i synnerhet avseende personlig integritet, skyddet för personuppgifter och yttrandefrihet. Därefter beskrivs i avsnitt 4 relevant gällande rätt kring elektronisk kommunikation. Avsnitt 5 utgör en översiktlig beskrivning av de brottsbekämpande myndigheternas utredande verksamhet och underrättelseverksamhet. Regleringen kring datalagring i brottsbekämpande syfte redogörs för i avsnitt 6. Därefter, i avsnitt 7, beskrivs nyttan och behovet av uppgifter om elektronisk kommunikation. Avsnitt 8–10 handlar om EU-rättens påverkan på utformingen och tillämpningen av reglerna om datalagring. En internationell utblick finns i avsnitt 11. Utredningens överväganden och förslag finns mot slutet av betänkandet, i avsnitt 12, medan författningsförslagen finns i avsnitt 1. Den sista delen av betänkandet utgörs av en konsekvensanalys, avsnitt 13, och en författningskommentar, avsnitt 14.

3 Grundläggande rättigheter

3.1 Rätten till personlig integritet

3.1.1 Integritetsbegreppet

Som anförs i Datalagringsutredningens betänkande finns det i svensk rätt inte någon allmängiltig definition av begreppet personlig integritet, SOU 2015:31 s. 51. Någon definition finns inte heller i internationell rätt, SOU 2016:65 s. 34. Olika utredningar har med utgångspunkt i bl.a. de grundläggande fri- och rättigheterna i RF:s 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), se t.ex. Tvångsmedelskommitténs betänkande Tvångsmedel – Anonymitet – Integritet, SOU 1984:54 s. 42. 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 och 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, SOU 2015:31 s. 51. I förarbetena till RF och personuppgiftslagen (1998:204) har lagstiftaren dock försökt att beskriva kärnan i vad som avses skyddas av lag-

stiftningen genom att slå fast att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den 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).

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 t.ex. 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 rätt att göra anspråk på att staten vidtar effektiva åtgärder för att skydda hans eller hennes säkerhet. I detta ligger bl.a. att staten måste anstränga sig för att se till att brott förebyggs och utreds samt att gärningsmän ställs till 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. Detta följer bl.a. av artikel 8 i Europakonventionen (se t.ex. Europadomstolens mål Söderman mot Sverige, 12 november 2013, § 78 och von Hannover mot Tyskland, 24 juni 2004, § 57). Motsvarande skydd följer av rättighetsstadgan. Även utan att det har 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 övergreppet 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. En förutsättning för att staten ska kunna leva upp till kraven på att upprätthålla rättstryggheten för enskilda är att staten har en välfungerande och effektiv brottsbekämpning (SOU 2015:31 s. 51–52 jfr även p. 149 i EU-domstolens yttrande 1/15 den 26 juli 2017). Att ha en välfungerande brottsbekämpning innebär t.ex. att

myndigheterna ska ha tillgång till effektiva utredningsverktyg – även i den elektroniska miljön. När så inte har varit fallet har staten ansetts kränka de rättigheter som följer av Europakonventionen. Ett exempel på detta var när en person som gjort sig skyldig till förtal eller möjligen sexuellt ofredande av ett 12-årigt barn i Finland inte kunde identifieras på grund av att den nationella lagstiftningen inte möjliggjorde att uppgift om vem som använt en ip-adress inte kunde inhämtas från operatören. I det aktuella fallet uttalade domstolen särskilt att konfidentialitet för kommunikation och yttrandefrihet ibland måste få vika för brottsbekämpande ändamål. (Europadomstolens dom den 2 december 2008, K.U. mot Finland, särskilt § 49).

Statens skyldighet att upprätthålla ett straffrättsligt skydd och göra skyndsamma ingripanden mot allvarliga brott följer även av andra artiklar i Europakonventionen och rättighetsstadgan, exempelvis avseende frihetsberövanden, artikel 5 i Europakonventionen samt artiklarna 6 och 52.3 i rättighetsstadgan, se även Hans Danelius, Mänskliga rättigheter i Europeisk praxis, 5:e uppl., s. 112 och p. 42 i Digital Rights-domen.

3.1.3 Regleringen av skyddet för privatlivet

Grundläggande bestämmelser

Grundläggande bestämmelser som har betydelse för det allmännas ansvar att skydda enskildas privatliv och integritet finns i bl.a. 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.

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, 4 december 2008, § 66 och Gillberg mot Sverige, 2 november 2010, § 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. Vidare omfattar skyddet enligt artikeln bl.a. kommunikation genom telefon och e-post (Liberty m.fl. mot Förenade kungariket, 1 juli 2008, § 56 och däri hänvisade rättsfall). Registrering av vilka telefonnummer en person ringer kan utgöra ett ingrepp i rätten till privatliv, beroende på i vilket syfte den görs (P.G. och J.H. mot Förenade kungariket, 25 september 2001, § 42). Europadomstolen har emellertid påpekat att det är en väsentlig skillnad mellan det och att avlyssna vederbörandes kommunikation. Detsamma gäller exempelvis gps-positionering av en person, som bedömts som mindre allvarligt än t.ex. avlyssning (Uzun mot Tyskland, 2 september 2010, §§ 52 och 66). 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 (t.ex. K.U. mot Finland, 2 december 2008, §§ 42 och 43, och von Hannover mot Tyskland, 24 juni 2004, § 50).

Rätten till respekt för privatlivet innefattar även skyddet av personuppgifter (Hans Danelius, Mänskliga rättigheter i europeisk praxis, 5:e uppl., s. 386). Om staten exempelvis lagrar information hänförligt till folks privatliv, kan både det och tillgången till informationen utgöra ett intrång i rätten till privatliv (exempelvis Leander mot Sverige, 26 mars 1987, § 48). Det gäller även om informationen består av enbart offentliga och okänsliga uppgifter samt sker utan hjälp av något hemligt tvångsmedel (Segerstedt-Wiberg m.fl. mot Sverige, 6 juni 2006, § 72; Uzun mot Tyskland, 2 september 2010, § 46, samt Amann mot Schweiz, 16 februari 2000, §§ 65–67). Trots att Europakonventionen inte uttryckligen reglerar skydd av personuppgifter (jfr artikel 8 EU:s rättighetsstadga, se nedan avsnitt 3.2.1) så omfattar konventionen således ett sådant skydd. 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 (t.ex. Rotaru mot Rumänien, 4 maj 2000, § 43).

Som nämnts ovan, innebär rätten till privatliv inte bara ett skydd mot myndigheters ingrepp, utan även en skyldighet för stater att kriminalisera brott och tillämpa straffrättsliga bestämmelser genom effektiv utredning och lagföring. När brott har begåtts mot en persons fysiska eller psykiska hälsa krävs det att det, i rimlig mån, finns redskap som gör det möjligt att identifiera och lagföra förövaren. Det måste samtidigt beaktas att redskapen används på ett sätt som är förenligt med de mänskliga rättigheterna i övrigt. Det är lagstiftarens skyldighet att upprätta ett ramverk som är förenligt med samtliga dessa konkurrerande principer. (K.U. mot Finland, 2 december 2008, §§ 46–49 och p. 149 i EU-domstolens yttrande 1/15 den 26 juli 2017)

En bestämmelse om rätt till respekt för bl.a. privatlivet finns också i artikel 7 i rättighetsstadgan. Av samma artikel följer att var och en har rätt till respekt för sina kommunikationer. 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 eller ett mer långtgående skydd. 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, mål C-617/10, § 21). Av Tele2-domen följer att rättighetsstadgan är av vikt vid utformningen av bestämmelser om datalagring även för brottsbekämpande ändamål.

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.[1] 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

[1] Principerna finns att läsa på necessaryandproportionate.org

legitimt ändamål. Vidare ska åtgärderna beslutas av en behörig rättslig myndighet. Den som utsätts för åtgärderna ska underrättas om dem. Staterna ska också inrätta kontrollmekanismer som ska säkerställa transparens och ansvar för åtgärderna.

Av intresse är även de principer som upprättats av Artikel 29-gruppen. Gruppen har bl.a. satt upp garantier som gruppen menar måste följas för att en inskränkning i skyddet för personuppgifter ska vara godtagbar.[2]

Ett skydd mot godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens finns även i andra internationella instrument, se t.ex. artikel 12 i Förenta Nationernas allmänna förklaring om de mänskliga rättigheterna och artikel 17 i Förenta Nationernas internationella konvention om medborgerliga och politiska rättigheter.[3]

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 från andra individer eller ostörd av samhällets organ. I syfte att tillförsäkra medborgarna trygghet och säkerhet mot yttre och inre hot kan det ibland vara nödvändigt med vissa inskränkningar av integritetsskyddet. Som anges ovan har staten till och med en skyldighet att införa sådana regler (avsnitt 3.1.2–3.1.3).

Det är en svår uppgift att avväga å ena sidan skyddet för enskilda mot ingrepp från staten mot å andra sidan statens plikt att skydda individen, dvs. att se till att myndigheterna har effektiva verktyg till sin hjälp för att bekämpa brott. En självklar utgångspunkt i sådana avvägningar är Europakonventionen och rättighetsstadgan. En annan 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

[2] Article 29 data protection working party, WP 237, 13 april 2016.
[3] Om rätten till privatliv i den digitala eran, läs t.ex. Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, A/HRC/27/37, 30 juni 2014 samt Europarådets resolution 1970 (2014) och rekommendationer 2033 (2014).

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 om 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 RF 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. Vad avser lagringsskyldighet för elektroniska kommunikationsuppgifter, som medför en inskränkning i integritetsskyddet, uttalade regeringen, i samband med att bestämmelserna om lagring av trafikuppgifter för brottsbekämpande ändamål infördes, att principerna kring lagringsskyldigheten och begränsningar till teknikområden borde vara reglerade i lag medan den mer tekniska specifikationen av lagringskravet kunde regleras i förordning (prop. 2010/11:46 s. 28).

På liknande sätt får rättigheter enligt artikel 8 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 utformad med tillräcklig precision, så att inskränkningarna i den grundläggande konventionsrättigheten i rimlig utsträckning kan 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 (Hans Danelius, Mänskliga rättigheter i Europeisk praxis, 5:e uppl., 2015, s. 370 samt Kopp mot Schweiz, 25 mars 1998, § 55).

När det gäller dolda spaningsåtgärder innebär kravet på förutsebarhet 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. Det gäller oavsett om övervakningen riktar sig mot en individ eller är av mer övergripande karaktär. (Weber och Saravia mot Tyskland, 29 juni 2006, § 93, samt Liberty m.fl. mot Förenade Kungariket, 1 juli 2008, § 63)

Europadomstolen har utarbetat en minimistandard som ställer följande krav på lagstiftning om hemliga övervakningsåtgärder (t.ex. Uzun mot Tyskland, 2 september 2010, § 61 med hänvisningar):

- Arten av de brott som skulle kunna leda till en begäran om åtgärden måste framgå.
- Det ska finnas en definition av de personkategorier som skulle kunna riskera att bli föremål för åtgärden, t.ex. få sin telefon avlyssnad.
- Åtgärdens 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.
- De omständigheter under vilka inhämtade uppgifter (t.ex. inspelningar) kan eller måste raderas ska anges.

De viktigaste punkterna har bedömts vara de två förstnämnda. Vad avser karaktären på de förseelser som kan föranleda övervakning krävs inte att det finns en lista med namngivna brott; det är tillräckligt med exempelvis information om minimistraff för brottet. När det gäller avgränsning av personkategori har Europadomstolen ansett det kunna vara berättigat att även personer som inte är misstänkta för brott men som kan ha upplysningar om brottet berörs av åtgärden, bl.a. har domstolen bedömt det vara befogat att avlyssna en telefon tillhörande partnern till en dödad person. (Greuter mot

Nederländerna, 19 mars 2002 samt Roman Zakharov mot Ryssland, 4 december 2015, §§ 231, 243–245)

Det kan 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 (Uzun mot Tyskland, 2 september 2010, §§ 65 och 66; jfr även P.G. och J.H. mot Förenade kungariket, 25 september 2001, § 42). 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 (SOU 2015:31 s. 57).

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 (t.ex. Szabó och Vissy mot Ungern, 12 januari 2016). 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 (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, se Cameron, Expertrapport åt Polismetodutredningen, SOU 2010:103 s. 547–548.

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 (Hans Danelius, Mänskliga rättigheter i Europeisk praxis, 5:e uppl., s. 370–371).

Vid bedömningen av om åtgärden är nödvändig i ett demokratiskt samhälle måste en helhetsbedömning göras av alla omständigheter, exempelvis omfattningen och varaktigheten av åtgärden, skälen för åtgärden, vem som är behörig att besluta om, genomföra och övervaka åtgärden samt vilka rättsmedel som finns. Exempelvis skulle en vid formulering av villkoren för en hemlig övervakningsåtgärd delvis kunna uppvägas av en förhandskontroll i domstol. (Roman Zakharov mot Ryssland, 4 december 2015, §§ 232, 248, 249 samt Uzun mot Tyskland, 2 september 2010, § 63).

Vad avser just förhandskontroll av domstol har Europadomstolen uttalat att ett system där sådan prövning saknas och de brottsbekämpande myndigheterna i stället har direktåtkomst till exempelvis upp-

gifter om mobiltelefonkommunikation är särskilt känsligt för missbruk och att andra garantier mot godtycke och missbruk blir synnerligen stort med ett sådant system (Roman Zakharov mot Ryssland, 4 december 2015, §§ 268–270). Vid positionsövervakning har det ansetts tillräckligt med en prövning av domstol efter att åtgärden redan skett, exempelvis genom att uppgifter som framkommit genom övervakningen inte får användas som bevis i rättegång, om övervakningsåtgärden inte varit lagenlig (Uzun mot Tyskland, 2 september 2010, §§ 71 och 72).

Europadomstolen har vidare ställt vissa krav på att lagstiftningar om hemliga tvångsmedel och övervakningsåtgärder även innehåller andra rättssäkerhetsgarantier. Domstolen har uttryckt att, eftersom det vid hemliga tvångsmedel finns en risk för missbruk i enskilda fall, det är lämpligt att en domare bör ha ansvaret för övervakningen. Samtidigt har domstolen godtagit att ett oberoende utomrättsligt organ med tillräckliga befogenheter ansvarar för tillsynen. (Roman Zakharov mot Ryssland, 4 december 2015, §§ 233 och 275)

Som huvudregel ska den som varit föremål för den hemliga tvångsåtgärden underrättas om det, för att han eller hon inte ska berövas möjligheten att söka gottgörelse för eventuell olaglig användning av tvångsmedlet. Europadomstolen har emellertid inte uppställt något absolut krav, med hänvisning till att en underrättelse både kan äventyra syftet med åtgärden och också avslöja hemliga arbetsmetoder eller agenter inom den brottsbekämpande myndigheten. Domstolen har, som exempel, godtagit att en oberoende myndighet avgör om underrättelse ska skickas eller inte eller att underrättelse underlåts om det finns möjlighet för en enskild som misstänker att han eller hon är föremål för hemlig övervakning att vända sig till en oberoende domstol med utredningsbefogenheter. (Klass m.fl. mot Tyskland, 6 september 1978, § 58 samt Roman Zakharov mot Ryssland, 4 december 2015, §§ 286–288 och däri hänvisade rättsfall, särskilt Kennedy mot Förenade kungariket, 18 maj 2010, § 167).

När det gäller unionsrätten följer det 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 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 samhälls-

intresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter. Enligt EU-domstolens fasta praxis kräver proportionalitetsprincipen att unionsinstitutionernas 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 allvarligt ingreppet är, vilket syfte ingreppet har etc. Ju mer långtgående ett ingrepp är, desto mer strikt blir EU-domstolens kontroll av att proportionalitetsprincipens krav följs (SOU 2015:31 s. 59).

Med kravet att rättighetsinskränkningarna ska vara föreskrivna i lag avses inte nödvändigtvis att föreskriften måste finnas i en författning som benämns just lag (i jämförelse med andra föreskrifter, t.ex. förordning). I sitt förslag till avgörande i Tele2-målet diskuterade generaladvokaten vad som avses med uttrycket i såväl stadgan som i direktiv 2002/58. Efter en jämförelse av olika språkversioner, en genomgång av praxis från EU-domstolen och Europadomstolen samt efter beaktande av det rättighetsintrång som en generell lagringsskyldighet medför, ansåg generaladvokaten det önskvärt att det väsentliga innehållet i skyldigheten anges i bestämmelser som antas av den lagstiftande makten och att den verkställande makten närmare fastställer tillämpningsföreskrifterna till dessa (punkterna 134–153).

3.2 Skyddet för personuppgifter

3.2.1 Grundläggande EU-rätt

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.

Rätten till skydd för enskilda personer avseende behandlingen av personuppgifter kommer till uttryck även i artikel 16 i 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 artikel 39 FEUF. Även där slås fast att oberoende myndigheter ska kontrollera att bestämmelserna följs.

3.2.2 EU:s dataskyddsdirektiv och dataskyddsreform

En allmän reglering om skydd av personuppgifter inom EU finns i direktiv 95/46/EG (dataskyddsdirektivet). Direktivet har antagits med stöd av fördragens bestämmelser om den 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. Direktivet gäller inte på områden som faller utanför unionsrätten, såsom försvar, allmän säkerhet och statens verksamhet på straffrättens område. Det finns också andra rättsakter som kompletterar dataskyddsdirektivet, bl.a. rådets rambeslut 2008/977/RIF av den 27 november 2009 om skydd för personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete, det s.k. dataskyddsrambeslutet.

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. I direktivet regleras ett antal allmänna principer om uppgifternas kvalitet och godtagbara grunder för behandling av personuppgifter. Vidare finns det bestämmelser om enskildas rätt till information och tillgång till behandlade uppgifter. Begränsningar i principerna 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.

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.

Dataskyddsdirektivet har genomförts i medlemsstaterna genom nationell lagstiftning – i Sverige främst genom personuppgiftslagen – och medlemsstaterna får inom direktivets ram precisera villkoren för personuppgiftsbehandling. De nationella preciseringarna får dock inte hindra det fria flödet av personuppgifter inom EU.

Både dataskyddsdirektivet och dataskyddsrambeslutet har varit föremål för ett omfattande reformarbete inom EU, i syfte att ytterligare harmonisera och effektivisera skyddet av personuppgifter. EU-förhandlingarna har pågått sedan 2012 och i april 2016 antog rådet och parlamentet dels en dataskyddsförordning med en generell reglering som ska ersätta dataskyddsdirektivet, dels ett nytt direktiv med särskilda regler om dataskydd för den brottsbekämpande verksamheten.[4] Förordningen ska börja tillämpas i medlemsstaterna den 25 maj 2018 och direktivet ska vara implementerat senast den 6 maj 2018.

Från den generella dataskyddsförordningens tillämpningsområde undantas behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten (artikel 2). För sådan behandling gäller i stället det nya dataskyddsdirektivet. Förordningen ska, liksom det nya dataskyddsdirektivet, inte heller tillämpas på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten.

[4] Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) respektive Europaparlamentets och rådets direktiv (EU) 2016/680 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

Såväl förordningen som det nya direktivet innehåller regler som begränsar möjligheterna att överföra personuppgifter till tredje land.

3.2.3 Dataskyddskonventionen

Sverige har ratificerat Europarådets konvention från 1981 om skydd för enskilda vid automatisk behandling av personuppgifter (ETS 108), som trädde i kraft den 1 oktober 1985. Konventionen, som brukar ses som en precisering av artikel 8 i Europakonventionen, syftar till att säkerställa den enskildes grundläggande fri- och rättigheter i samband med automatisk behandling av personuppgifter hänförliga till den enskilde (artikel 1).

Dataskyddskonventionen innehåller principer för dataskydd som 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. (artikel 5) Varje person ska ha rätt att få bekräftat om personlig information om honom eller henne har lagrats (artikel 8).

Av artikel 12.2 konventionen följer som huvudregel att en konventionsstat inte endast av integritetsskyddsskäl får hindra att personuppgifter förs över till en annan konventionsstat för att behandlas 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). 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 (ETS 181). 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. Av protokollet framgår bl.a. att varje konventionsstat ska 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. 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.

Dataskyddskonventionen är för närvarande föremål för översyn.[5]

3.2.4 Nationell lagstiftning

Dataskyddsdirektivet har genomförts i svensk rätt genom framför allt personuppgiftslagen (1998:204). Lagen är i första hand tillämplig på personuppgiftsansvariga 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 (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. Sådana särregler finns i t.ex. åklagardatalagen (2015:433) och polisdatalagen (2010:361).

3.3 Yttrandefrihet

EU:s rättighetsstadga skyddar yttrandefriheten, artikel 11. I artikeln föreskrivs att var och en har rätt till yttrandefrihet. Denna rätt innefattar åsiktsfrihet samt frihet att ta emot och sprida uppgifter och tankar utan någon offentlig myndighets inblandning och oberoende av territoriella gränser. Motsvarande skydd finns i artikel 10 i Europakonventionen.

[5] www.coe.int/en/web/portal/28-january-data-protection-day-factsheet; förslag till ny konventionstext samt en Draft Explanatory Report lämnades i juni 2016.

Även enligt RF tillförsäkras yttrandefrihet. Var och en är gentemot det allmänna tillförsäkrad yttrandefrihet, dvs. frihet att i tal, skrift eller bild eller på annat sätt meddela upplysningar samt uttrycka tankar, åsikter och känslor (2 kap. 1 §).

4 Elektronisk kommunikation

4.1 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 (SOU 2015:31). Denna utveckling har framför allt möjliggjorts genom 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.

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

4.2 Integritetsskydd och tystnadsplikt vid elektronisk kommunikation

Som anförs ovan (avsnitt 3.1.3) skyddas mellanmänsklig kommunikation av rättighetsstadgan, som föreskriver att var och en har rätt till respekt för sitt privatliv och familjeliv, sin bostad och sina kommunikationer (artikel 7). Som också nämns ovan (avsnitt 3.2.1) föreskriver rättighetsstadgan även ett skydd för personuppgifter (artikel 8).

I syfte att säkerställa full respekt för de rättigheter som följer av artikel 7 och 8 har EU antagit direktiv 2002/58 som rör just integritet och elektronisk kommunikation. Direktivet 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 att skydda berättigade intressen för de abonnenter som är juridiska personer, artikel 1.

Direktivet definierar trafikuppgifter och lokaliseringsuppgifter men inte abonnemangsuppgifter, artikel 2.

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.

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 innebär att kommunikationen och de därmed förbundna trafikuppgifterna kan fångas upp eller övervakas av andra personer än användarna, utan de berörda användarnas samtycke och förutom när de har laglig rätt att göra så i enlighet med direktivet.

I artikel 6 finns bestämmelser om för vilka 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.

I artikel 9 finns bestämmelser om andra lokaliseringsuppgifter än trafikuppgifter. Om sådana uppgifter kan behandlas, får dessa upp-

gifter endast behandlas sedan de har avidentifierats eller om användarna eller abonnenterna gett sitt samtycke.

Vidare finns i artikel 15 ett stöd för medlemsstaterna att – för vissa närmare specificerade ändamål – föreskriva undantag från de skyddsregler som finns i artiklarna 5, 6 och 9. Undantag får bl.a. 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.

Direktiv 2002/58 har genomförts i svensk rätt främst genom bestämmelser som tagits in i LEK, se nedan.

EU-kommissionen har lagt fram ett förslag till en ny förordning om respekt för privatlivet och skydd för personuppgifter i samband med elektronisk kommunikation som ska ersätta direktiv 2002/58. Förordningen kommer enligt de utkast som hittills har presenterats inte att förändra det nationella utrymmet att anta bestämmelser om datalagring för brottsbekämpande ändamål. Förslaget bereds för närvarande inom EU.

4.3 LEK

LEK trädde i kraft i juli 2003 och syftade bl.a. till att genomföra flera EG-direktiv om elektronisk kommunikation. Lagen är i huvudsak en 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.

LEK 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 tillgängliga 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 IHL (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 6 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 RB:s 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. En liknande bestämmelse finns i 16 f § samma kapitel. Enligt den ska verksamheten bedrivas så att uppgifterna som omfattas av lagrings-

skyldigheten utan dröjsmål kan lämnas ut och så att verkställandet av utlämnandet inte röjs. Uppgifterna ska göras tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand.

För försvarsunderrättelseändamål finns en annan sorts anpassningsskyldighet. För att inhämtning av signaler i elektronisk form enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet ska kunna ske, är operatörer som äger tråd i vilka signaler förs över Sveriges gräns skyldiga att överföra dessa till vissa samverkanspunkter.

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. Sådana uppgifter har ibland kallats för kataloguppgifter eftersom informationen som kan erhållas närmast motsvarar vad som finns i telefonkataloger (prop. 2011/12:55 s. 100). Begreppet är emellertid missvisande eftersom abonnemangsuppgifter omfattar även andra uppgifter, t.ex. vilken användare som vid varje given tidpunkt hade en viss ip-adress eller ett IMSI-nummer (prop. 2011/12:55 s. 100 och SOU 2007:76 s. 64).[1]

Enligt 2 § förordningen (2003:396) om elektronisk kommunikation är Post- och telestyrelsen tillsynsmyndighet enligt LEK.

[1] Mer om begreppet abonnemangsuppgifter finns att läsa i avsnitt 6.2.1.

5 Brottsbekämpande verksamhet

5.1 Brottutredande 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 brottsutredande uppgifter.

Förfarandet vid den utredning som föregår ett beslut om åtal, förundersökningen, regleras främst i RB och i förundersökningskungörelsen (1947:948). En förundersökning ska, enligt 23 kap. 1 § RB, 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 av Polismyndigheten, Säkerhetspolisen eller av åklagare. För vissa särskilda brott får även beslut om att inleda förundersökning fattas vid andra myndigheter som Tullverket, Kustbevakningen och JK. Om förundersökning har inletts av Polismyndigheten eller Säkerhetspolisen 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 § RB huvudsakligen två syften. Det ena syftet är att utreda om brott har begåtts och vem som i så fall skäligen kan misstänkas för brottet samt 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.

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 beroende av vad som har kommit fram under förundersökningen. Därför blir resultatet av förundersökningen i praktiken helt avgörande för utgången av målet.

5.2 Underrättelseverksamhet

Vissa av de brottsbekämpande myndigheterna bedriver 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 brottsbekämpande myndigheterna med kunskap som kan omsättas i operativ verksamhet.

I underrättelseverksamheten samlar myndigheterna in, bearbetar och analyserar uppgifter som senare kan ha betydelse för att förebygga, förhindra och upptäcka brottslig verksamhet.

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.

Inhämtningen kan ske från olika källor. Det kan t.ex. ske genom rutinmässig spaning, internationell samverkan eller genom information från tipsare och informatörer. En annan källa för inhämtning är allmänt tillgänglig information i tidningar eller på internet.

När informationen har inhämtats bearbetas den genom att informationen struktureras, systematiseras och värderas, t.ex. genom jämförelser med sedan tidigare kända uppgifter. Därefter vidtar den avgörande fasen i underrättelseprocessen – analysen. Det kan handla om hot- och riskanalys, analys av brottsmönster och kartläggning av kriminella nätverk och grupperingar.

Efter inhämtning, bearbetning och analys är ambitionen att kunna använda materialet i operativt arbete. Det framtagna underrättelsematerialet kan t.ex. läggas till grund för beslut om att inleda förundersökning eller beslut om att vidta särskilda åtgärder för att förebygga, förhindra eller upptäcka brott. Det kan också användas för att gå ut i media för att förebygga ett visst brottsligt tillvägagångssätt. En annan form av förebyggande verksamhet är att de berörda perso-

nerna kontaktas och därigenom blir medvetna om den brottsbekämpande myndighetens intresse, vilket många gånger leder till att den planerade brottsliga verksamhet aldrig kommer till stånd.

5.2.1 Polismyndighetens underrättelseverksamhet

Till skillnad från Polismyndighetens utredande verksamhet fokuserar underrättelseverksamheten inte på enskilda brott, utan på brottslig verksamhet. Utredande verksamhet i form av en förundersökning eller primärutredning är att betrakta som bakåtblickande, då utredningen avser ett specifikt brott som har begåtts. Underrättelseverksamheten är typiskt sett framåtblickande, då den ofta försöker upptäcka, förutse och beskriva viss brottslighet, brottsutveckling eller ett visst fenomen i syfte att förebygga och förhindra.

I enlighet med underrättelseprocessen bearbetar och registrerar Polismyndighetens underrättelsetjänst inkommen eller inhämtad information. Informationen kommer bl.a. direkt från allmänheten i form av tips, från särskilda informatörer, från enskilda poliser, från tekniska system, från andra myndigheter i Sverige, från polisens sambandsmän i andra länder samt från Europol och Interpol.

Inhämtad information bedöms och värderas för registrering och vidare bearbetning. Genom analys länkas uppgifter samman och sammanhang, nätverk och skeenden värderas. Resultatet blir ett underlag för strategiska och operativa beslut i polisverksamheten och ett direkt stöd till medarbetare i kärnverksamheten. 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 samtliga nivåer i organisationen.

På nationell nivå finns en underrättelseenhet vid Nationella operativa avdelningen, NOA. Underrättelseenheten vid NOA har det övergripande ansvaret för polisens underrättelseverksamhet. I detta ansvar ligger bl.a. att ta fram en nationell underrättelsebild och en underrättelsemodell samt processmässigt styra verksamheten. Underrättelseverksamheten vid den nationella underrättelseenheten

är huvudsakligen inriktad mot organiserad brottslighet på nationell och internationell nivå.

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

På regional nivå finns en underrättelseenhet per region som bedriver underrättelseverksamhet med såväl strategiskt som operativt fokus. Dessa enheter stöder samtliga delar inom regionen, från lokalpolisområde till regional nivå. Förutom bearbetning av information och delgivning av underrättelser tillhandahåller enheterna också strategiska och operativa underrättelseanalyser. De regionala enheterna upprätthåller en regional underrättelsebild. De regionala enheterna innefattar även myndighetsgemensamma regionala underrättelsecenter, RUC. I likhet med NUC samordnar RUC myndigheters underrättelsearbete men på regional nivå.

Inom den regionala enheten finns delar som stöder polisområdesnivån med underrättelser. Som stöd till lokalpolisområdesnivån finns underrättelsesamordnare. Dessa arbetar direkt mot varje lokalpolisområde med stort fokus på den operativa kärnverksamheten.

5.2.2 Säkerhetspolisens underrättelseverksamhet

Säkerhetspolisens underrättelseverksamhet syftar till att förebygga, förhindra och upptäcka brottslig verksamhet som bl.a. avser rikets säkerhet och bekämpning av terrorism samt fullgöra uppgifter enligt säkerhetsskyddslagen (1996:627) och säkerhetsskyddsförordningen (1996:633). Med säkerhetsskydd avses skydd mot bl.a. spionerilikasom 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, förhindra och upptäcka 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 utgör en begränsad del av verksamheten. Detta avspeglar sig också 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. Det är fråga om dels 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.

Säkerhetspolisen tillämpar i princip samma modell som den öppna polisen för att styra underrättelsearbetet. Modellen innebär i korthet att ett 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. Underrättelseverksamheten är tydligt avgränsad och det finns ett väl definierat mål för arbetet.

Liksom beträffande den öppna polisen sätter de allmänna principerna för polisingripande som anges i 8 § polislagen (1984:387) den yttre ramen för verksamheten. Säkerhetspolisens inhämtningsmetoder skiljer sig härigenom inte från de metoder som används inom Polismyndigheten. Det kan exempelvis vara fråga om inhämtning genom fysisk spaning, liksom genom öppna eller egna källor. Även nationell och internationell samverkan har stor betydelse för underrättelseverksamheten.

I sammanhanget bör nämnas att EU har verkat för en mer effektiv samverkan inom unionen när det gäller utbyte av information mellan medlemsstaterna för att bekämpa bl.a. terrorbrott.[1]

5.2.3 Tullverkets underrättelseverksamhet

I Tullverkets uppdrag ingår bl.a. att övervaka och kontrollera trafiken till och från utlandet så att bestämmelser om in- och utförsel av varor följs och brottslighet vid in- och utförseln av varor förebyggs och motverkas.

Tullverkets underrättelseverksamhet är framåtblickande och består i att inhämta, bearbeta och analysera information om externa aktörer och fenomen i syfte att skapa underrättelser med framtidsperspektiv. Underrättelseverksamheten inriktar sig på att förebygga, förhindra och upptäcka brottslig verksamhet och skiljer sig därmed från Tullverkets utredande verksamhet, som har till syfte att utreda ett specifikt brott som har begåtts.

Syftet med underrättelseverksamheten är att producera underrättelser som ger rekommendationer om inriktning och prioritering av myndighetens verksamhet. Underrättelseverksamheten är en kunskapsuppbyggande verksamhet om sådana förhållanden som bl.a. kan vara av intresse för att upptäcka och identifiera brottslig verksamhet. Att underrättelseverksamheten är kunskapsuppbyggande innebär att verksamheten är kumulativ och varje dokument, ärende och produkt utgör en pusselbit som adderas till Tullverkets förståelse för de

[1] Europeiska unionens råds slutsatser om vägen till ett förbättrat informationsutbyte och säkerställande av interoperabiliteten mellan EU:s informationssystem, 10151/17, 8 juni 2017.

aktörer och fenomen som verksamheten har i uppdrag att följa. Målet med underrättelseverksamheten är att reducera osäkerheter som är kopplade till beslutsfattande genom kunskaper och insikter om omvärlden.

Underrättelseverksamheten vid Tullverket beskrivs genom en uppdelning i strategisk och operativ underrättelseverksamhet. Målet med den strategiska underrättelseverksamheten är att producera underrättelser i syfte att identifiera, formulera och stödja Tullverkets övergripande mål, policy, inriktningar och prioriteringar. Den strategiska verksamheten berör i huvudsak frågor om hur Tullverket ska lösa sitt uppdrag. Målet är att arbetet ska generera rekommendationer om operativa åtgärder. Operativ underrättelseverksamhet producerar underrättelser i syfte att stödja prioritering och genomförande av operativa insatser riktade mot identifierade aktörer och fenomen. Den strategiska underrättelseverksamheten skiljer sig därmed från den operativa genom att den har ett mer långsiktigt och övergripande fokus på myndighetens samlade verksamhet.

5.3 Allmänt om straffprocessuella tvångsmedel

RB 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 (Gunnel Lindberg, Straffprocessuella tvångsmedel, 3:e uppl., 2013, s. 5–6). Exempel på tvångsmedel är 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. Till dessa kommer de osjälvständiga tvångsmedlen, dvs. tvångsmedlen enligt LSU och 2007 års preventivlag, som har sin tillämpning utanför en förundersökning. Dessa lagar utökar möjligheterna att under särskilda omständigheter ge Polismyndigheten och Säkerhetspolisen tillstånd att använda vissa hemliga tvångsmedel enligt 27 kap. RB. Även inhämt-

ning av uppgifter enligt 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. Inhämtning av abonnemangsuppgifter enligt LEK har inte ansetts som ett hemligt tvångsmedel, prop. 2011/12:55 s. 110–111. Utredningen delar denna bedömning.

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 editionsföreläggande eller husrannsakan i förening med beslag i fall där annars andra regler för utfående av sådana uppgifter gäller (prop. 2002/03:74 s. 45–46). Följande exempel kan belysa detta. Polisen har inte rätt att utverka ett beslag av en server hos en operatör för att därigenom få tillgång till trafikuppgifter. Polisen måste i sådant fall i stället genom åklagare ansöka om tillstånd till hemlig övervakning av elektronisk kommunikation hos domstol.

Principerna om ändamål, behov och proportionalitet

Villkoren för att använda de olika tvångsmedlen skiljer sig åt beroende på vilket 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 gäller både vid lagstiftningsarbetet samt vid beslut om, och tillämpning av, de hemliga tvångsmedlen. Principerna finns beskrivna

på flera ställen, se t.ex. SOU 1984:54, avsnitt 3.2.2, SOU 2012:44 s. 118, prop. 1988/89:124 s. 26 och Gunnel Lindberg, Straffprocessuella tvångsmedel, 3:e uppl., 2013, kapitel 3. Principerna gäller inte enbart för tvångsmedel, bl.a. återfinns behovs- och proportionalitetsprincipen i 8 § polislagen, som avser alla tjänsteuppgifter en polisman utför.

Enligt ändamålsprincipen får ett tvångsmedel användas endast för det ändamål som framgår av lagstiftningen. Det är därför av stor vikt att det för varje enskilt tvångsmedel anges i lagstiftningen för vilket eller vilka ändamål det får användas. Som påpekats av bl.a. Gunnel Lindberg har lagstiftaren inte gjort detta för t.ex. hemlig övervakning av elektronisk kommunikation, Gunnel Lindberg, Straffprocessuella tvångsmedel, 3:e uppl., 2013, kapitel 3.2, not 10, och kapitel 36.2. En ändamålsprövning bör ske före behovs- och proportionalitetsprövningen. Om tvångsmedlet inte ska användas för det ändamål det är till för, spelar det ingen roll om det finns ett påtagligt behov och åtgärden framstår som proportionerlig. Enligt ändamålsprincipen kan man inte heller använda ett tvångsmedel med syfte att få fram överskottsinformation.

Behovsprincipen innebär att ett tvångsmedel får användas endast om det finns ett påtagligt behov och en mindre ingripande åtgärd inte är tillräcklig. När det inte längre föreligger skäl för åtgärden ska den upphävas. Åtgärder som huvudsakligen har till syfte att underlätta för myndigheten anses strida mot principen.

Enligt proportionalitetsprincipen ska en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet stå i rimlig proportion till vad som står att vinna med åtgärden. Proportionalitetsprincipen finns lagstadgad i t.ex. 27 kap. 1 § RB och 2 § IHL, men anses gälla vid all tvångsanvändning även utan lagstöd. Vid bedömningen om åtgärden är proportionerlig ska det intrång eller annat men som tvångsmedlet innebär för den misstänkte eller för något annat motstående intresse beaktas. Härmed inbegrips, förutom direkta följder för den som utsätts för tvångsmedlet, även indirekta verkningar av tvångsmedelsanvändningen. Det kan t.ex. röra sig om intrång i tredje mans rättsligt skyddade intressen. Proportionalitetsavvägningar kan därför få till följd exempelvis att en myndighet underlåter en tvångsåtgärd mot en advokatbyrå, ett sjukhus eller någon annan inrättning där särskilt känsliga uppgifter bevaras eller yppas.

Det ska alltid ske en prövning huruvida tvångsmedlet över huvud taget är påkallat med hänsyn till förhållandena i det särskilda fallet

och om syftet kan tillgodoses genom någon mindre ingripande åtgärd. Utgångspunkten bör vara att pröva om alternativa spaningsåtgärder kan användas och om det kan räcka med att exempelvis tillgripa hemlig övervakning av elektronisk kommunikation i stället för hemlig avlyssning. Proportionalitetsprincipen innebär alltså att utredningen i princip ska ha nått ett stadium där det förefaller omöjligt att komma längre med mindre ingripande metoder. Ibland kan det emellertid redan från början stå klart att det är meningslöst att försöka med andra metoder. Det kan t.ex. bero på att den misstänkte går mycket försiktigt till väga och kan förutsättas på alla sätt skydda sig mot normala utredningsmetoder. Ett annat fall kan vara att efterforskningar med vanliga metoder skulle kräva en orimligt stor insats av personal, kunna i förtid avslöja den pågående utredningen eller vara farliga för polispersonalen. (prop. 1988/89:124 s. 27, 28 och 66)

Personlig frihet och integritet ska också beaktas. Ingrepp i dessa intressen är till sin art allvarligare än ingrepp mot egendom eller andra ekonomiska intressen (SOU 1979:6 s. 294 och SOU 1984:54 s. 78). Det är särskilt viktigt att proportionalitet iakttas vid långtgående intrång i den privata sfären.

Som framgår ovan (avsnitt 3.1.3), följer ett krav på proportionalitetsavvägningar även av Sveriges internationella åtaganden. När begränsningar görs i rättigheter som följer av Europakonventionen eller EU-stadgan ska alltid proportionalitetsprincipen beaktas. Endast om det finns ett rimligt förhållande mellan behovet av det som ska tillgodoses och ingreppet i den enskildes rätt kan ingreppet vara proportionerligt och därmed nödvändigt i ett demokratiskt samhälle (Hans Danelius, Mänskliga rättigheter i Europeisk praxis, 5:e uppl., 2015, s. 57–58 samt artikel 52.1 i stadgan).

Sammanfattningsvis ger proportionalitetsprincipen i sig stöd för att rätten att använda tvångsmedel ska begränsas till vad som är strängt nödvändigt. Samtidigt möjliggör den ett generöst tillämpningsområde, eftersom myndigheterna i varje enskilt fall måste göra övervägningar som leder till begränsningar som annars hade behövt vara lagstadgade.

Utöver de principer som nyss redogjorts för, påverkar andra principer användandet av tvångsmedel. Till dem hör exempelvis objektivitets- och hänsynsprinciperna i 23 kap. 4 § RB (objektivitetsprincipen finns även uttryckt i 1 kap. 9 § RF).

6 Uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

6.1 Regleringen av lagring av uppgifter

Som utvecklas nedan är uppgifter om elektronisk kommunikation och abonnemangsuppgifter mycket viktiga för brottsbekämpningen (avsnitt 7). Det finns därför regler som har till syfte att säkerställa att de brottsbekämpande myndigheterna har tillgång till dessa uppgifter.

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 införskaffa uppgifter som denne annars inte genererar eller behandlar. Däremot ska en uppgift lagras så fort den funnits hos leverantören, även om det bara rör sig om en ytterst kort tid (prop. 2010/11:46 s. 77). Omfattningen av lagringen är begränsad till uppgifter som genereras eller behandlas vid telefonitjänst, meddelandehantering,

internetåtkomst och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform).

Telefonitjänst omfattar situationer då E.164-nummer (vanliga telefonnummer) används av någon av samtalsparterna. Det inkluderar fast och mobil telefoni och de flesta internettelefonitjänster. Internettelefoni som bara använder andra adresser än E.164-nummer (exempelvis ip-adresser) omfattas inte. Med telefoni avses inte heller kommunikation som omfattas av begreppet meddelandehantering.[1] (prop. 2010/11:46 s. 29–30)

Meddelandehantering definieras i 6 kap. 1 § LEK som utbyte eller överföring av elektroniskt meddelande som inte är samtal och inte heller är information som överförs som del av sändningar av ljudradio- och tv-program. Begreppet innefattar elektroniska meddelanden som t.ex. e-post, sms och mms. Lagringsskyldigheten är inte begränsad till något speciellt kommunikationsprotokoll. (prop. 2010/11:46 s. 30)

Internetåtkomst finns också definierat i 6 kap. 1 § LEK. Med internetåtkomst avses enligt bestämmelsen möjlighet till överföring av ip-paket som ger användaren tillgång till internet. Med ip-paket menas ett telekommunikationspaket med data som ska överföras, inklusive en titelrad med bl.a. sändarens namn och mottagarens ip-adress. I praktiken innebär internetåtkomst att användaren tilldelas en eller flera ip-adresser för kommunikation. Med ip-adress (Internet Protocol Adress) avses en unik adress som används för identifiering och kommunikation mellan två datorer på internet med hjälp av Internet Protocol-standarden (ip). Ip-adresserna kan vara fasta adresser, dvs. samma användare har alltid samma adress, eller dynamiska adresser, dvs. de tilldelas användaren under en begränsad tid. När dynamiska ip-adresser används kan alltså samma användare ha olika adresser vid olika tillfällen och samma ip-adress kan användas av olika användare vid olika tillfällen. (prop. 2010/11:46 s. 30)

Med anslutningsform avses själva tekniken eller kapaciteten som ger möjlighet till överföring av ip-paket för att få internetåtkomst, t.ex. DSL (Digital Subscriber Line), fiberoptiska anslutningar, 3G (UMTS), GSM (GPRS), traditionella telefonmodem och WLAN (trådlöst nät), prop. 2010/11:46 s. 30–31 och 77.

[1] Observera att definitionen av telefonitjänst i datalagringsdirektivet även innefattade meddelandetjänster, såsom sms och mms, artikel 2 c.

Besök på webbsidor och chattsidor samt användning av File Transfer Protocol (FTP, dvs. upp- och nedladdning av filer) är exempel på tjänster som faller utanför lagringsskyldighetens räckvidd (prop. 2010/11:46 s. 77, se även avsnitt 12.4.2).

I 39–43 §§ FEK anges på en mer detaljerad nivå vilka uppgifter som ska lagras inom respektive teknikslag. PTS får också meddela närmare föreskrifter om de uppgifter som ska lagras (44 §).

Av bestämmelserna i FEK framgår följande.

För telefonitjänst ska det lagras uppringande nummer, uppringt nummer och nummer som samtalet styrts till, uppgifter om uppringande och uppringd abonnent och, i förekommande fall, registrerad användare, datum och spårbar tid då kommunikationen påbörjades och avslutades samt uppgifter om den eller de tjänster som har använts. För mobiltelefoni ska det därutöver lagras uppringandes och uppringds abonnemangsidentitet och utrustningsidentitet, lokaliseringsuppgifter för kommunikationens början och slut samt datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst (t.ex. oregistrerade kontantkort).

För ip-telefoni ska det därutöver lagras uppringandes och uppringds ip-adresser, datum och spårbar tid för på- och avloggning i den eller de tjänster som använts samt uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.

Vid meddelandehantering ska det lagras avsändares och mottagares nummer, ip-adress eller annan meddelandeadress, uppgifter om avsändande och mottagande abonnent och, i förekommande fall, registrerad användare, datum och spårbar tid för på- och avloggning i den eller de tjänster som använts, datum och spårbar tid för avsändande och mottagande av meddelande samt uppgifter om den eller de tjänster som har använts.[2]

När det gäller internetåtkomst och anslutningsform ska det lagras användares ip-adress, uppgifter om abonnent och, i förekommande

[2] Det kan särskilt noteras att lokaliseringsuppgifter inte ska lagras vid (mobil) meddelandehantering. Varför denna skillnad, i förhållande till telefonitjänst, har gjorts finns inte närmare utvecklat i förarbetena, se SOU 2007:76, särskilt avsnitt 6.10, samt prop. 2010/11:46, särskilt s. 27–28 och 33–37. Någon sådan skillnad finns inte i 6 kap. 16 a § LEK och det kan diskuteras om det möjligen inte var så att datalagringsdirektivet ålade medlemsstaterna att införa en sådan lagringsskyldighet, se artikel 5.1 f) 1 i datalagringsdirektivet samt artikel 2 d) i direktiv 2002/58, jfr dock artikel 2.2 e) i datalagringsdirektivet.

fall, registrerad användare, datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomst, den typ av kapacitet för överföring som har använts samt uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.

En fråga som varit föremål för diskussion är hur långt lagringsskyldigheten sträcker sig avseende ip-adresser. Det är inte ovanligt att privatpersoner, företag eller operatörer använder sig av NAT-teknik, som enkelt uttryckt innebär att en publik ip-adress används och delas upp i flera privata ip-adresser, exempelvis genom en router. NAT-tekniken används även i stor skala, av t.ex. internetleverantörer, och en publik ip-adress kan i teorin delas av omkring 65 000 abonnenter eller användare. PTS har gjort bedömningen att lagringsskyldigheten i dessa fall inte sträcker sig längre än till den privata ip-adressen, se PTS skrivelse den 26 februari 2015 till Ekobrottsmyndigheten, dnr 15-1185. (se även SOU 2015:31 s. 320)

Som framgår ovan, ska det i flera fall lagras de tjänster som använts. Med tjänst avses exempelvis rösttelefoni, konferenssamtal, typ av meddelandetjänst (sms, mms, etc.) eller extratjänster som vidaresändning och omstyrning av samtal (SOU 2007:76 s. 154).

Av 6 kap. 16 a § LEK följer vidare att den svenska regleringen på två punkter går längre än vad datalagringsdirektivet krävde (avsnitt 8.1). 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.

6.2 Regleringen av tillgång till uppgifter

Enligt 6 kap. 16 c § LEK får uppgifter som lagrats enligt 16 a § behandlas endast för att lämnas ut enligt 22 § första stycket 2, 27 kap. 19 § RB eller IHL. Härtill kommer de osjälvständiga hemliga tvångmedlen, dvs. de hemliga tvångsmedlen enligt 27 kap. RB som får användas enligt förutsättningarna i 2007 års preventivlag och LSU. De två sistnämnda hänvisar till RB:s regler om hemlig övervakning av elektronisk kommunikation.

6.2.1 Begreppen 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 får behandlas – vid sidan av själva lagringen och den efterföljande raderingen – endast för att lämnas ut enligt 6 kap. 22 § första stycket 2 LEK, 27 kap. 19 § RB och enligt IHL. Villkoren för denna inhämtning av uppgifter, som alltså är uppdelad på tre olika regelverk, berörs mer ingående i det följande.

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.

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 (avsnitt 4.3). Reglerna om lagring är på så sätt frikopplade från reglerna om inhämtning. Lagringsskyldigheten är alltså till för att underlätta inhämtningen och säkerställa att alla operatörerna lagrar de uppgifter som omfattas, men reglerna om inhämtning är inte beroende av lagringsskyldigheten.

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, efter-

forskning 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 uppgift om abonnemang i 6 kap. 20 § LEK avses t.ex. uppgifter om abonnentens nummer, namn, titel och adress (prop. 1992/93:200 s. 310). Till abonnemangsuppgifter brukar även räknas uppgifter om exempelvis avtal och fakturering. Vidare innefattas såväl fasta som dynamiska ip-adresser och IMSI-nummer (ett nummer som är kopplat till abonnentens sim-kort och därmed telefonnummer). Däremot har det påstått att varken IMEI-nummer (ett id-nummer för kommunikationsutrustningen) eller PUK-kod omfattas av begreppet, prop. 2011/12:55 s. 62, 69 och 101 (se dock det i propositionen redovisade remissyttrandet av Säkerhetspolisens ang. IMEI-nummer), SOU 2007:76 s. 64–66, SOU 2009:1 s. 70–73 och 95 samt Gunnel Lindberg, Straffprocessuella tvångsmedel, 3:e uppl., 2013, s. 485 (annan uppfattning ang. IMEI-nummer).

Det kan ifrågasättas om det är lämpligt eller ens möjligt att definiera abonnemangsuppgifter endast utifrån vilken uppgift det är fråga om. Enligt utredningen är det mer relevant att som utgångspunkt definiera abonnemangsuppgifter som uppgifter som identifierar abonnenten eller den registrerade användaren bakom ett visst nummer eller en viss adress, i motsats till uppgifter som redogör för hur numret eller adressen har använts. Utifrån en sådan definition utgör uppgift om vilken abonnent som är kopplad till ett visst IMSI-nummer en abonnemangsuppgift medan information om vilka andra nummer eller adresser som ett visst IMSI-nummer har kommunicerat med inte gör det. En sådan definition stämmer väl överens med hur de olika uppgiftskategorierna exemplifierades i förarbetena till telelagen, varifrån begreppet ursprungligen härstammar, prop. 1992/93:200 s. 310 och prop. 2002/03:110 s. 271. Definitionen får också visst stöd av ett uttalande från Kammarrätten i Stockholm i rättsfallet RK 2010:1. Kammarrätten ansåg att en begäran om uppgifter som syftar till att identifiera ett abonnemang eller en abonnent i princip avser uppgifter om abonnemang. Kammarrätten gick emellertid ett steg längre och menade att om en sådan begäran även inne-

fattade en annan uppgift, i det fallet vilka IMSI-nummer som använts i kombination med ett visst känt IMEI-nummer, utgjorde det alltjämt en fråga som syftade till att identifiera ett abonnemang och därmed en uppgift som skulle lämnas ut av operatören i enlighet med 6 kap. 22 § första stycket 2 LEK.

För att ytterligare illustrera skillnaden mellan abonnemangsuppgifter och andra uppgifter kan en jämförelse göras med uppgifter om ett fordon. Uppgift om vem som äger fordonet vid en viss tidpunkt skulle motsvara en abonnemangsuppgift medan frågor om var fordonet befunnit sig vid samma tidpunkt inte skulle göra det.

Abonnemangsuppgifter finns tillgängliga för leverantören i elektronisk form. 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 uppgifter som normalt inte offentliggörs, t.ex. ip-adresser.

Som framgår i avsnitt 6.1 är en ip-adress en unik adress som en dator eller ett lokalt nätverk tilldelas för att datapaket ska kunna skickas och tas emot över internet genom den tekniska kommunikationsstandarden Internet Protocol. Ip-adressen kan därför, något förenklat, liknas med ett postnummer för vanliga brevförsändelser. Ip-adressen är en teknisk uppgift som ingår i varje datapaket och som behövs för att datapaketet ska nå sin destination på internet.

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). Utredningen delar denna bedömning. Även de flesta medlemsstater i den informella rådsarbetsgrupp i EU som behandlar datalagringsfrågan efter Tele2-domen har preliminärt kommit till slutsatsen att ip-adresser är abonnemangsuppgifter (som inte omfattas av domen, se även avsnitt 12.2). Det existerar emellertid även andra uppfattningar, enligt vilka de uppgifter som krävs för att identifiera abonnenten bakom en ip-adress inte ska anses vara uppgifter om abonnemang, bl.a. eftersom det kan röra sig om tidsloggar för internetåtkomst (avsnitt 12.2).

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 (telefoni, sms, etc.), vilken utrustning som använts, vilka nummer eller adresser som kommunicerat med varandra samt när och hur länge kommunikationen pågått. Utanför begreppet trafikuppgifter faller information som avslöjar meddelandets innehåll.

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 t.ex. fakturera för utnyttjade tjänster eller erbjuda andra mervärdestjänster.

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. Det kan t.ex. vara fråga om vilken cell (antenn på basstation) som utrustningen kopplat upp sig mot eller en gps-position. (prop. 2002/03:110 s. 261–262 och SOU 2009:1 s. 71–72)

6.2.2 Abonnemangsuppgifter

Som framgår ovan, har en leverantör tystnadsplikt för uppgifter om abonnemang, innehållet i ett elektroniskt meddelande och andra uppgifter som angår ett särskilt elektroniskt meddelande – med vissa undantag i förhållande till innehavaren av ett abonnemang och den som tagit del i utväxlingen av meddelandet (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 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, Kustbevakningen 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 som åtalas enbart av målsäganden. Inhämtning av sådana uppgifter får även göras i underrättelseverksamhet (SOU 2015:31 s. 198–199, med förslag till förtydligande i denna del). En begränsning av tillgången följer dock av behovs- och proportionalitetsprincipens krav. Det är emellertid svårt att se att en inhämtning av abonnemangsuppgifter i praktiken skulle utmana någon av de nämnda principerna. Som nämnts ovan anses inte inhämtning av uppgifter om abonnemang enligt LEK nå upp till den nivå av integritetsintrång att det har bedömts vara ett hemligt tvångsmedel (prop. 2013/14:237 s. 134). Uppgifterna är typiskt sett inte heller särskilt integritetskänsliga (SOU 2015:31 s. 186 och Ds 2014:23 s. 66 och 69). Däremot är uppgifterna ändå skyddsvärda, eftersom de utgör en länk mellan förhållandevis anonyma uppgifter och en fysisk person.

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 LEK 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. Regeringen framhöll 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 ansåg regeringen 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 motstående 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 och rskr. 2011/12:212).

6.2.3 Hemlig övervakning av elektronisk kommunikation

Hemlig övervakning av elektronisk kommunikation innebär att uppgifter i hemlighet hämtas in om meddelanden (dvs. både samtal och skriftliga 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 RB). De uppgifter som kan hämtas in genom tvångsmedlet är alltså 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 RB 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 nu 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. Tillstånd till tvångsmedlet kan 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 avse

uppgifter i förfluten tid (27 kap. 20 § andra stycket RB). En basstationstömning får avse kommunikationsutrustning, telefonnummer eller annan adress och göras även när utrustningens identifikationsnummer är okänt (27 kap. 20 § första stycket 1 samt prop. 2011/12:55 s. 128).

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 RB).

Tvångsmedlet får enligt huvudregeln användas endast efter förhandsprövning och beslut av domstol. Tingsrätten prövar frågan efter ansökan av en åklagare (27 kap. 21 § RB). 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 § RB).

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 § RB).

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 (överskottsinformation) är begränsade. Förundersökning får nämligen normalt endast inledas om det är föreskrivet fängelse ett år eller mer för brottet (27 kap. 23 a § RB). Uppgifterna får dock alltid användas för att förhindra förestående brott eller i pågående förundersökningar.

6.2.4 IHL

IHL 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

- historiska uppgifter om meddelanden
- uppgifter om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område (basstationstömning)
- uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

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 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 med lägre straffminimum, t.ex. sabotage och spioneri. Denna bestämmelse är tidsbegränsad och gäller till utgången av 2019.

Genom rekvisitet ”brottslig verksamhet” framgår att det inte ställs krav på att det ska finnas en misstanke om ett specifikt brott (prop. 2011/12:55 s. 123). Det föreligger därmed en principiell skillnad i förhållande till tillämpningsområdet för straffprocessuella tvångsmedel enligt RB.

Beslut om inhämtning fattas av myndigheten själv utan förhandskontroll av någon utomstående oberoende myndighet.

6.2.5 2007 års preventivlag

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 2007 års preventivlag 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, spionerioch terroristbrottslighet, men även vissa våldsbrott och brott mot frihet och frid som begås i syfte att påverka offentliga organ eller journalister (systemhotande brottslighet). Även om lagen främst rör brottslig verksamhet inom Säkerhetspolisens område kan också Polismyndigheten använda lagen. Det sker dock mycket sällan. Tillstånd får meddelas endast om åtgärden är proportionerlig och av synnerlig vikt för att förhindra sådan brottslig verksamhet (1 och 5 §§).

Hemlig övervakning enligt 2007 års preventivlag får avse endast ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som under den tid tillståndet omfattar innehas eller har innehafts av den som kan antas komma att utöva den brottsliga verksamheten eller som annars kan antas ha använts eller komma att användas av honom eller henne. Hemlig övervakning får också avse ett telefonnummer, en annan adress eller en viss kommunikationsutrustning som det finns synnerlig anledning att anta att han eller hon under den tid tillståndet avser har kontaktat eller kommer att kontakta.

Frågan om tillstånd till tvångsmedel enligt lagen prövas av domstol (Stockholms tingsrätt) efter ansökan av åklagare (6 §). Tillståndet får – som beträffande övriga hemliga tvångsmedel – inte ges för längre tid än nödvändigt och får, i fråga om tid efter beslutet, inte överstiga en månad från dagen för beslutet (7 §). Om tiden inte räcker, får tillstånd sökas på nytt. Om det inte längre finns skäl för ett tillstånd till tvångsmedelsanvändning, ska åklagaren eller rätten omedelbart häva beslutet. Polisen ska omedelbart underrätta åklagaren om omständigheter som har betydelse för om beslutet ska hävas (10 §). Reglerna i RB om handläggning vid domstol av frågor om tvångsmedel i brottmål och om överklagande av beslut i sådana frågor

tillämpas på förfarandet, om inte annat sägs i lagen. Handläggningen ska ske skyndsamt (15 §).

6.2.6 LSU

Enligt LSU får en utlänning utvisas ur landet bl.a. om det med hänsyn till vad som är känt om utlänningens tidigare verksamhet och övriga omständigheter kan befaras att han eller hon kommer att begå eller medverka till terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller försök, förberedelse eller stämpling till sådant brott (1 §). Om ett beslut om sådan utvisning tills vidare inte ska verkställas på grund av inhibition eller ett tidsbegränsat uppehållstillstånd, får Migrationsverket eller regeringen besluta att vissa tvångsmedelsregler som finns i lagens 19–22 §§ ska tillämpas på utlänningen. Detsamma gäller om det utvisningsbeslut som inte ska verkställas har fattats enligt 8 kap. utlänningslagen (2005:716) och det finns sådana omständigheter avseende utlänningen som nämnts ovan (11 och 11 a §§).

Av 19 och 20 §§ framgår att tvångsmedelsreglerna när de är tillämpliga medför att rätten under vissa förutsättningar kan meddela tillstånd enligt 27 kap. RB till hemlig avlyssning av elektronisk kommunikation eller, om det är tillräckligt, hemlig övervakning av elektronisk kommunikation. Sådant tillstånd får meddelas om det är av betydelse för att utröna om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott och det finns synnerliga skäl.

Yrkande om tillstånd hos domstol görs av Säkerhetspolisen eller Polismyndigheten. En särskild regel gäller beträffande forum (21 §). Tillståndet ska, som beträffande övriga hemliga tvångsmedel, meddelas att gälla för en viss tid som inte får överstiga en månad. Om tiden inte räcker får en ny ansökan göras. I fråga om förfarandet i övrigt tillämpas 27 kap. RB (21 §).

6.3 Säkerheten för lagrade uppgifter

Vid genomförandet av datalagringsdirektivet i Sverige (avsnitt 8.1.4) konstaterades att det i LEK redan fanns regler om såväl driftsäkerhet (5 kap. 6 a §) som integritetsskydd (6 kap. 3 §). Sist nämnda bestäm-

melse, som genomför artikel 4.1 i direktiv 2002/58, 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 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 § FEK. 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 bemyndigandet i 37 § FEK 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 har även fått i uppdrag att utöva tillsyn över leverantörernas lagring av trafikuppgifter. Det ansågs att myndighetens tillsynsbefogenheter var ändamålsenliga och tillräckliga (prop. 2010/11:46 s. 58). 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 förelägganden 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.

6.4 Kontrollmekanismer och rättssäkerhetsgarantier

För att skydda personers integritet och upprätthålla en hög grad av rättssäkerhet innehåller regelverket kring myndigheternas tillgång till uppgifter om elektronisk kommunikation ett antal kontrollmekanismer och rättssäkerhetsgarantier. Dessa beskrivs nedan.

Det ska i sammanhanget framhållas att andelen människor i Sverige som oroar sig för att myndigheterna ska kränka deras personliga integritet har minskat. Däremot har oron för att stora internetföretag ska kränka den ökat.[3]

6.4.1 Förhandskontroll

Hemlig övervakning av elektronisk kommunikation

De brottsbekämpande myndigheternas tillgång till trafik- och lokaliseringsuppgifter i en förundersökning om brott förutsätter som regel att tingsrätten, efter prövning av en ansökan från åklagaren, har

[3] Internetstiftelsen i Sveriges rapport Svenskarna och internet 2016, avsnitt 11.

meddelat tillstånd till inhämtningen (27 kap. 21 § RB). 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.

2007 års preventivlag

Innan övervakning av elektronisk kommunikation får utföras enligt 2007 års preventivlag måste domstolsbeslut inhämtas från Stockholms tingsrätt (6 §). Om det kan befaras att inhämtande av rättens tillstånd skulle medföra en fördröjning av väsentlig betydelse för möjligheterna att förhindra den brottsliga verksamheten, får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut (6 a §).

LSU

Frågan om tillstånd till hemlig övervakning av elektronisk kommunikation inom ramen för särskild utlänningskontroll prövas av Stockholms tingsrätt på yrkande av Säkerhetspolisen eller Polismyndigheten (21 §).

IHL

Beslut enligt IHL 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 delega-

tion har fått rätt att hämta in uppgifter får inte fatta beslut om inhämtning i sådan operativ verksamhet som han eller hon själv deltar i. Beslutet ska vara preciserat och tiden för beslutet får, när det gäller tid som infaller efter beslutet, inte överstiga en månad (5 §).

6.4.2 Efterhandskontroll

Tillsyn

Tillsynen över de brottsbekämpande myndigheternas tillämpning av lagar och andra författningar i den brottsbekämpande verksamheten delas mellan flera myndigheter.

Säkerhets- och integritetsskyddsnämnden (SIN) har i uppdrag att utöva tillsyn över bl.a. 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 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 Polismyndighetens, Säkerhetspolisens och Ekobrottsmyndighetens behandling av personuppgifter enligt polisdatalagen (2010:361) och lagen (2010:362) om polisens allmänna spaningsregister. Exakt hur tillsynen av personuppgiftsbehandlingen för Polismyndigheten ska regleras är nu föremål för överväganden (se betänkandena Ett samlat ansvar för tillsyn över den personliga integriteten, SOU 2016:65, och Brottsdatalag, SOU 2017:29, samt Utredningen om 2016 års dataskyddsdirektiv, dir. 2016:21).

SIN bedriver sin verksamhet genom inspektioner och andra undersökningar som sker på eget initiativ (2 § lagen om tillsyn över viss brottsbekämpande verksamhet). När nämnden beslutar att inleda tillsyn på eget initiativ görs detta främst utifrån bedömningen av var risken för en felaktig rättstillämpning hos de granskade myndigheterna är som störst (se för detta och det följande SIN:s årsredovisning 2016 s. 7–8). Bedömningen baseras på nämndens egna erfarenheter men även andra myndigheters (t.ex. Datainspektionens) iakttagelser kan beaktas. Nämnden kan även inleda tillsyn på eget initiativ, t.ex. efter att någon företeelse inom nämndens tillsyns-

område har uppmärksammats i medierna. Nämnden har rätt att få de uppgifter och det biträde som nämnden begär av den myndighet som omfattas av tillsynen samt begärda uppgifter av andra myndigheter och domstolar (4 § lagen om tillsyn över viss brottsbekämpande verksamhet). Inriktningen på nämndens tillsyn på eget initiativ sker även med beaktande av de uppdrag som myndigheten får från regeringen. Med utgångspunkt från ovanstående beslutar nämnden om fokusområden för sin tillsyn.

Nämndens ambition är att sprida sina tillsynsinsatser såväl geografiskt som verksamhetsmässigt. Tillsynsärendena kan utmynna i uttalanden om konstaterade förhållanden eller behov av förändringar i verksamheten (2 § lagen om tillsyn över viss brottsbekämpande verksamhet). Dessa avgöranden är varken bindande eller överklagbara utan nämnden ska i stället anmäla sina iakttagelser och överlämna relevanta delar av det som har framkommit i tillsynsärendet till den myndighet som ansvarar för frågan (6 § lagen om tillsyn över viss brottsbekämpande verksamhet och prop. 2006/07:133 s. 70 och 83).

Till grund för tillsynsverksamheten ligger även de anmälningar som de brottsbekämpande myndigheterna gör om inhämtning enligt IHL (6 §) och 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.

Datainspektionen är tillsynsmyndighet enligt personuppgiftslagen, 2 § personuppgiftsförordningen (1998:1191). Myndigheten har rätt att få tillgång till de personuppgifter som behandlas samt upplysningar och dokumentation om behandlingen, 43 § personuppgiftslagen (1998:204). Om Datainspektionen konstaterar att personuppgifter behandlas på ett olagligt sätt ska myndigheten genom påpekanden eller liknande förfaranden försöka att åstadkomma rättelse (45 §). Datainspektionen kan begära hos domstol att olagligt behandlade personuppgifter ska förstöras (47 §). 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 Polismyndighetens, Säkerhetspolisens och Ekobrottsmyndighetens behandling av personuppgifter. Övriga brottsbekäm-

pande myndigheters behandling av personuppgifter står under tillsyn enbart av Datainspektionen.

Förutom den specifika tillsyn som nu redogjorts för utövar Riksdagens ombudsmän (JO) och Justitiekanslern (JK) tillsyn över att myndigheterna följer lagar och andra författningar.

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 från allmänheten och 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 görs emellertid inte särskilt ofta på det brottsbekämpande området eftersom det där i stor utsträckning saknas ämnesspecifika 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. 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 honom eller henne 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

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 ha 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.

Den som har varit utsatt för hemliga tvångsmedel enligt RB 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 §). 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 underrättelseskyldigheten (27 kap. 33 § tredje stycket RB).

Om övervakning har avsett ett telefonnummer eller annan adress eller en viss elektronisk kommunikationsutrustning som innehas av någon annan än den misstänkte, ska även innehavaren underrättas. Om inhämtningen har skett i syfte att utreda vem som är skäligen

misstänkt och integritetsintrånget för den enskilde kan antas vara ringa behöver inte underrättelse lämnas.

Vid tvångsmedelsanvändning enligt 2007 års preventivlag gäller ingen underrättelseskyldighet, förutom avseende de brott som avses i lagens 1 § första stycke 7, dvs. mord, dråp, grov misshandel, människorov eller olaga frihetsberövande i avsikt att påverka ett offentligt organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik, att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd (16 §). Om åtgärden har avsett ett telefonnummer eller annan adress, en viss elektronisk kommunikationsutrustning eller en plats som innehas av någon annan, ska även den personen underrättas. Underrättelse ska lämnas så snart det kan ske efter det att det ärende som åtgärden vidtogs i har avlutats. En underrättelse behöver inte lämnas till den som redan har fått del av eller tillgång till uppgifterna. En underrättelse behöver inte heller lämnas om den med hänsyn till omständigheterna uppenbart är utan betydelse.

Underrättelse får skjutas upp om sekretess gäller (17 §). Om sekretess hindrar underrättelse i ett år behöver någon underrättelse inte lämnas.

Underrättelseskyldigheten ska fullgöras av åklagare och om sekretess hindrar underrättelse ska i stället Säkerhets- och integritetsskyddsnämnden underrättas, förordningen (2007:1144) om fullgörande av underrättelseskyldighet enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

Den ovan beskrivna underrättelseskyldigheten har inte någon motsvarighet när det gäller den inhämtning som utförs med stöd av IHL. För IHL gäller i stället att SIN ska underrättas om myndigheternas beslut om inhämtning. En sådan underrättelse ska lämnas senast en månad efter det att ärendet om inhämtning avslutades (6 § IHL).

Det saknas bestämmelser om underrättelse till enskild vid övervakning som ytterst har sitt stöd i LSU (prop. 2006/07:133 s. 52).

Kontroll på begäran av enskild

Som ett komplement till bestämmelserna om underrättelse till enskilda som utsatts för användning av hemliga tvångsmedel finns en reglering som ålägger SIN 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 ska det anmälas 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.

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, hemlig rumsavlyssning och inhämtning av uppgifter enligt IHL. Även tillämpningen av hemliga tvångsmedel som utförs för att förhindra vissa särskilt allvarliga brott redovisas. Numera redovisas även tillstånd som avser Säkerhetspolisen. Den senaste skrivelsen till riksdagen lämnades i december 2016 (skr. 2016/17:69).

Även tillämpningen av LSU redovisas årligen till riksdagen. I samband med att LSU infördes ansågs det nämligen att den parlamentariska kontrollen av hur regeringen tillämpar bestämmelserna och reglerna om tvångsåtgärder bör göras genom att regeringen årligen lämnar en skrivelse till riksdagen (prop. 1990/91:118 s. 72). Den senaste skrivelsen till riksdagen lämnades i december 2016 (skr. 2016/17:72).

6.4.3 Begränsningar i rätten att använda överskottsinformation

När tvångsmedel används kan det komma fram uppgifter som inte rör det brott som har legat till grund för tvångsmedelsbeslutet. Uppgifterna kan i stället ha betydelse för att utreda ett annat brott eller för att förhindra nya brott. Användningen av sådan information för att inleda en förundersökning är kringgärdad av vissa begränsningar (27 kap. 23 a § RB, 7 och 8 §§ IHL och 12 § 2007 års preventivlag).

7 Nyttan och behovet av 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 är det av vikt att klargöra vilken betydelse en åtgärd som innebär intrång i en skyddad rättighet kan ha för att uppnå målet. En proportionalitetsavvägning måste därefter göras mellan åtgärdens betydelse för det eftersträvade ändamålet å ena sidan och den grad av intrång i enskildas skyddade rättigheter som åtgärden innebär å andra sidan. Vid utformningen av regler kring straffprocessuella verktyg är det därför viktigt att undersöka hur verktygen används i den brottsbekämpande verksamheten och vilka behov av reglerna som finns (jfr SOU 2007:22 s. 175).

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 också ett behov av uppgifter om elektronisk kommunikation.

I analyser av nu aktuellt slag brukar uttrycken nytta och behov användas. Med nytta avses helt enkelt att uppgifterna har något värde för brottsutredningen. Uttrycket behov går tillbaks på den straffprocessuella behovsprincipen som anger att en myndighet får använda ett tvångsmedel bara när det föreligger ett påtagligt behov och en mindre ingripande åtgärd inte är tillräcklig för att tillgodose behovet. Eftersom de brottsbekämpande myndigheternas behov av tvångs-

medlen till stor del är beroende av vilken nytta dessa kan förväntas leda till är det oundvikligt att behovs- och nyttoanalyserna i flera avseenden blir lika varandra. Begreppen är dock inte helt synonyma. Det kan t.ex. finnas situationer där tvångsmedlen visserligen kan förväntas leda till nytta, men där behovet av att använda dem inte är särskilt stort. Så kan t.ex. vara fallet om de brottsbekämpande myndigheterna effektivt kan komma åt den eftersökta informationen med hjälp av andra metoder (prop. 2013/14:237 s. 61).

På ett generellt plan har nyttan av en bred tillgång till elektroniska kommunikationsuppgifter bekräftats av utländska studier. Europeiska kommissionen och Högsta förvaltningsdomstolen i Frankrike har i rapporter konstaterat att en riktad lagring ger de brottsbekämpande myndigheterna uppenbara begränsningar gentemot en generell lagring av data över längre tid (Commission Staff Working Document, som lades fram som bilaga till det förslag till direktiv som ledde fram till antagandet av direktiv 2006/24, SEK(2005) 1131, den 21 september 2005, ”Data Preservation versus Data Retention” samt Generaladvokatens förslag till avgörande i Tele2-målet not 54).

Sammanfattningsvis är nyttan av historisk kommunikationsdata i sig väl dokumenterad. Däremot finns de olika typerna av kommunikationsuppgifter sällan särredovisade, i synnerhet inte i förhållande till uppgifternas ålder.[1]

7.1 Utredningsverksamhet

Uppgifter om elektronisk kommunikation har stor betydelse i nästan all verksamhet som rör utredning av allvarlig brottslighet. Beredningen för rättsväsendets utveckling (BRU) konstaterade redan 2005 att trafikuppgifter ofta utgjorde den information som var viktigast för att föra utredningar om grövre brott framåt. Sådana uppgifter 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 (SOU 2005:38 s. 323–324).

[1] Se exempelvis Ds 2014:23 s. 85–86 och Europeiska kommissionens utvärderingsrapport av direktiv 2006/24 (Celexnummer: 52011DC0225) s. 23–24.

Uppgifterna är ofta av stor betydelse redan i utredningsarbetets inledningsskede. En kontroll av de trafikuppgifter som kan knytas till en brottsplats, ett brottsoffer eller en misstänkt kan användas tillsammans med annan information för att föra utredningen framåt (SOU 2015:31 s. 84).

Uppgifter om elektronisk kommunikation kan svara på frågor om vilka nummer som haft kontakt med varandra, hur intensiv kommunikationen har varit och var användarna av t.ex. mobiltelefoner har befunnit sig. Även uppgifter från anonyma kontantkort kan ha betydelse för att kunna kartlägga en misstänkt och på så sätt försöka få fram en identitet, ett skeende eller andra misstänkta. BRU konstaterade att inhämtade uppgifter i många fall kan få till följd att personer avförs från utredningen genom att misstankarna mot dem visar sig sakna substans. Att misstänkta avförs från utredningen genom användning av hemliga tvångsmedel framgår även av regeringens årliga skrivelse till riksdagen med redovisning av användningen av hemliga tvångsmedel (t.ex. skr. 2012/13:47 s. 14).

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. Cirka två tredjedelar av all hemlig övervakning av elektronisk kommunikation avser vålds- och narkotikabrottslighet (Säkerhetspolisen omfattas inte av statistiken), skr. 2016/17:69 s. 20–21.

Vid utredningen av internetrelaterad brottslighet är uppgifter om elektronisk kommunikation ofta helt avgörande 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

uppgifter om elektronisk kommunikation 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 (SOU 2015:31 s. 85). Av direktiven till Utredningen om hemlig dataavläsning framgår i enlighet med detta att anonymiseringstjänster har försvårat användningen av hemlig avlyssning av elektronisk kommunikation (dir. 2016:36 s. 2–3).

Av den ovan gjorda beskrivningen följer att det i princip inte går att ersätta inhämtning av nu aktuella uppgifter med t.ex. fysisk spaning just eftersom inhämtningen ofta avser historiska uppgifter.

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.

För att komplettera den generella beskrivningen ovan följer nedan exempel på utredningar där hemlig övervakning av elektronisk kommunikation har varit till nytta. Exemplen kommer från regeringens senaste redovisning till riksdagen av tvångsmedelsanvändningen (skr. 2016/17:69 s. 22) och från anonymiserade exempel från de brottsbekämpande myndigheterna. En mer detaljerad beskrivning av de brottsbekämpande myndigheternas nytta och behov av uppgifter om elektronisk kommunikation finns i avsnitt 12.6.

- Vid en utredning av en grov misshandel utförd efter intrång i målsägandens bostad beviljades hemlig övervakning av elektronisk kommunikation mot de misstänkta. Misshandeln misstänktes vara utförd av sex personer genom slag med bl.a. batong. Tack vare uppgifterna från övervakningen kunde åklagaren styrka att samtliga gärningsmän varit på plats vid tiden för den grova misshandeln. Genom bevisningen kunde det även visas att gärningsmännen träffats tidigare under dagen, att ingen kommunikation pågick under brottstiden men att telefonerna efter händelsen återigen var i kontakt med varandra. Vid jämförelse mellan innehållet i de beslagtagna telefonerna och telefonlistorna kunde det även visas att flera av de tilltalade hade raderat innehållet i telefontrafiken i tiden nära gärningen. De sex gärningsmännen dömdes för grov misshandel.

- Tre gärningsmän greps på flyende fot efter ett inbrott i en villa. En hundförare hittade gärningsmännens mobiltelefoner längs flyktvägen. De var sönderslagna för att försvåra spårning. Trots det kunde sim-korten identifieras. Genom lokaliseringsuppgifter kunde ytterligare ett tiotal bostadsinbrott klaras upp.
- En kvinna blev knivmördad i ett parkeringshus. Genom lokaliseringsuppgifter avseende kvinnans man kunde konstateras att han hade varit på platsen vid tidpunkten för mordet, som på så vis kunde klaras upp.
- Två okända gärningsmän rånade en guldbutik med skarpladdade vapen. Lyckade initiala åtgärder ledde till att två personer blev skäligen misstänkta för brottet. Den efterföljande hemliga övervakningen av elektronisk kommunikation ledde till att de båda männen kunde knytas till de platser där man förberett rånet, tillgripit en motorcykel och gömt denna under rånet.
- Säkerhetspolisen fick information om att en gruppering inom vit makt-miljön planerade att bränna ner en flyktingförläggning på en mindre ort. En förundersökning om förberedelse till grov mordbrand inleddes. Genom uppgifter från hemlig övervakning av elektronisk kommunikation gick det att fastställa att personer från grupperingen funnits i närheten av flyktingförläggningen under flera nätter i rad.
- Vid förundersökning rörande försök till mordbrand riktat mot ett kommunalråd misstänktes det att brottet utförts av personer inom den autonoma miljön. Genom uppgifter från hemlig övervakning av elektronisk kommunikation, bl.a. masttömning, kunde gärningsmännen identifieras.
- Ett flertal polisanmälningar gjordes runt om i landet avseende sexuella övergrepp mot barn som förövades genom sociala forum på internet. Ip-spårningar ledde till en man som sedermera kom att dömas för flera hundra sexualbrott brott mot över hundra målsägande.

7.2 Underrättelseverksamhet

Uppgifter om elektronisk kommunikation används inte bara i förundersökningar utan också i underrättelseverksamhet. Det är till största delen (cirka 80 procent) vid narkotikabrottslighet som uppgifter inhämtas i underrättelseverksamhet (Säkerhetspolisen omfattas inte av statistiken), skr. 2016/17:69 s. 28. För att illustrera nyttan av uppgifter i underrättelseverksamheten följer nedan några exempel på hur informationen kan användas. Exemplen är hämtade från regeringens senaste redovisning till riksdagen av tvångsmedelsanvändningen (skr. 2016/17:69 s. 29 och 31) och från anonymiserade exempel från de brottsbekämpande myndigheterna. En mer detaljerad beskrivning av de brottsbekämpande myndigheternas nytta och behov av uppgifterna finns i avsnitt 12.6.

- Underrättelser angav att ett antal personer, vilka inte hade några kända kopplingar till varandra sedan tidigare, var involverade i storskalig vapen- och narkotikahantering i Stockholmsområdet. Inhämtning av uppgifter om elektronisk kommunikation och spaning mot de utpekade personerna ledde till att ett nätverk identifierades samt att en lagerplats för narkotika och vapen kunde lokaliseras. En förundersökning om grovt narkotikabrott inleddes och narkotika togs i beslag.
- Inhämtning av uppgifter om elektronisk kommunikation tillsammans med fysisk spaning ledde till att misstankar om tillverkning av narkotikaklassade tabletter stärktes och att en förundersökning kunde inledas. Under pågående förundersökning kunde ett flertal personer gripas och en stor mängd narkotika tas i beslag.
- Säkerhetspolisen fick information från ett annat lands säkerhetstjänst om att en person med diplomatisk immunitet misstänktes ägna sig åt flyktingspionage och att han hade kontakter med en kvinna i Sverige. Genom användning av IHL klarlades att det fanns kontakter mellan dem och att de samtidigt hade befunnit sig i samma geografiska område. På grund av de uppgifterna och andra omständigheter inleddes en förundersökning om olovlig underrättelseverksamhet.

- I ett ärende rörande amfetaminsmuggling i Halland inkom underrättelser om att en mobilabonnent i Stockholmsområdet föreföll ha kopplingar till ärendets huvudman. Efter inhämtning och analys av information om elektronisk kommunikation kunde det i kombination med fysisk spaning konstateras att den egentlige brukaren av det mobilabonnemanget inte var abonnenten själv utan en annan person, som tidigare varit dömd för grova narkotikabrott. Efter inledd förundersökning beslagtogs en större mängd narkotika.
- I ett ärende erhölls information från ett annat land om att mottagare av en större mängd kokain var bosatta i Sverige. Genom inhämtning enligt IHL kunde dessa mottagare identifieras. Med hjälp av historiska uppgifter kunde polisen också påvisa att narkotika hade mottagits vid flera tillfällen. Till slut kunde en förundersökning inledas och narkotikasmugglingen klaras upp.
- Genom en internationell polisinsats kunde flera marknadsplatser för narkotika på internet (Darknet) stängas ner. Polismyndigheten fick underrättelseinformation om vilka ip-adresser som använts på en svensk sådan marknadsplats. Flera av adresserna var emellertid oanvändbara, dels eftersom en längre tid hade passerat sedan de användes (och adresserna därför inte längre var lagrade), dels eftersom flera användare inte gick att identifiera på grund av NAT-teknik (en teknik för att tillåta att flera abonnenter delar på en och samma publika ip-adress, se avsnitt 6.1). I vissa fall kunde dock förundersökning avseende narkotikabrott inledas.

Polismyndigheten och Tullverket har konstaterat att information om elektronisk kommunikation är väsentlig för myndigheternas underrättelseverksamhet och att de möjligheter till inhämtning som IHL medger har varit avgörande för att inleda förundersökning för en lång rad grova brott. Tillgången till uppgifter om elektronisk kommunikation i underrättelsestadiet kan vara avgörande för att aktörer, platser och tidpunkter ska kunna kopplas samman och ge ett tillräckligt underlag för att inleda en förundersökning. Uppgifterna är enligt myndigheterna också väsentliga för en effektiv planering av yttre fysisk spaning, som är resurskrävande och därför viktig att använda på rätt plats vid rätt tillfälle (skr. 2016/17:69 s. 33).

Av den ovan gjorda redogörelsen följer att det i princip inte går att ersätta inhämtning av nu aktuella uppgifter med t.ex. fysisk spaning, särskilt eftersom inhämtningen ofta avser historiska uppgifter.

För Säkerhetspolisen är analys av elektronisk kommunikation, enligt myndigheten, av ovärderlig vikt för arbetet på underrättelsesidan. Regeringen har uttryckt att Säkerhetspolisen har ett uppenbart behov av uppgifterna för att bedriva kontraspionageverksamhet och arbete mot terrorism, prop. 2016/17:186 s. 9. Sådana uppgifter kan inte heller inhämtas på annat sätt, genom t.ex. fysisk spaning, eftersom inhämtning enligt IHL innebär att historiska uppgifter kan analyseras. Därutöver kan Säkerhetspolisens spaningsresurser användas mer effektivt efter en analys av användarens dygnsmönster och geografiskt återkommande platser. I underrättelsesyfte bidrar uppgifter om elektronisk kommunikation också med mycket värdefull information bl.a. för att kartlägga aktörer och nätverk som har avsikt och förmåga att begå brott som är allvarliga för rikets säkerhet. Inhämtningen av uppgifterna möjliggör således att man på ett tidigt stadium kan fånga upp eventuella grupperingar och skeenden (SOU 2015:31 s. 87). Ett exempel på sådan verksamhet som bedrivs av Säkerhetspolisen inom ramen för kontraspionaget är att på ett tidigt stadium kartlägga kontakter som utländska underrättelseofficerare tar med personer i Sverige. Även om denna del av Säkerhetspolisens verksamhet har lett till fällande dom, så är den absolut största nyttan med verksamheten att den person som den utländska underrättelseofficeraren bearbetar kan uppmärksammas på sin nya bekantskaps bakgrund och uppdrag i Sverige. Därmed kan en kontakt avbrytas i ett tidigt skede. Säkerhetspolisens huvudsakliga verksamhet är av praktiska skäl inte heller inriktad på att nå fällande domar och bedriva förundersökning mot misstänkta personer. Det är nämligen betydligt mer resurseffektivt och skadebegränsande att med ett tidigt ingripande genom t.ex. ett samtal reducera risken för hot och sårbarhet snarare än att fullfölja en lång underrättelseprocess med eventuell efterföljande förundersökning. Denna arbetsmetod innebär även att de personer som är intressanta i underrättelseverksamheten inte behöver utsättas för onödigt integritetskränkande övervakning eftersom syftet i stället kan uppnås genom betydligt mindre ingripande metoder.

Det ska i sammanhanget även lyftas fram att många av de personer som är intressanta för Säkerhetspolisen när det gäller kontra-

spionage skyddas av diplomatisk immunitet. Det är ytterligare en anledning till att resultatet av Säkerhetspolisens arbete i dessa fall inte syns i form av fällande domar och inledda förundersökningar. I dessa fall kan i stället Regeringskansliet eller regeringen överväga om det ska fattas ett beslut om *persona non grata* avseende den aktuella personen, 21 § förordningen (1996:1515) med instruktion för Regeringskansliet.

På motsvarande sätt som inom ramen för kontraspionaget är det inom författningsskyddet och kontraterrorismverksamheten avgörande för Säkerhetspolisen att kunna kartlägga personers kontakter och uppehållsorter.

Säkerhetspolisens användning av hemliga tvångsmedel regleras även av 2007 års preventivlag. Ett anonymiserat exempel på när Säkerhetspolisen haft nytta av uppgifter som inhämtats enligt den lagen är följande.

- Säkerhetspolisen hade information om att fem personer kunde vara i färd med att planera terrorattentat i Sverige. De fem männen bodde på visst avstånd från varandra och Säkerhetspolisen misstänkte att de använde elektronisk kommunikation i kontakten mellan sig. Genom hemlig övervakning av elektronisk kommunikation enligt 2007 års preventivlag kunde det bekräftas att männen hade kontakt med varandra samt att de ibland hade vistats i samma geografiska område. Genom informationen kunde en förundersökning om stämpling till terroristbrott inledas.

7.3 Användandet av kommunikationstjänster

För att kunna bedöma de brottsbekämpande myndigheternas nytta och behov samt vilket integritetsintrång lagring av och tillgång till uppgifter om elektronisk kommunikation innebär är det av intresse att veta hur elektroniska kommunikationstjänster används i Sverige.

En allt större krets har bytt ut sin traditionella mobiltelefon mot en smart telefon, som ger möjlighet till kommunikation på flertalet sätt och genom tjänster tillhandahållna av andra aktörer än teleoperatörerna. Flera mobiltelefoner, datorer och annan kommunikationsutrustning levereras med exempelvis mobiltelefontillverkarens egna kommunikationstjänster installerade och förvalda. Det kan antas att

en följd av det är att kommunikationsmönstret nu ser annorlunda ut i jämförelse med hur det såg ut för bara några år sedan och hur det kommer att se ut framöver. Användandet av elektroniska kommunikationstjänster skiljer sig också mellan yngre och äldre generationer, vilket även det kan antas ge upphov till ett förändrat och föränderligt behov av uppgifter för de brottsbekämpande myndigheterna.

PTS företar återkommande undersökningar om svenskarnas användning av telefoni och internet. Den senaste är från år 2015[2]. PTS för statistik över bl.a. trafiken i mobil-, tele- och fibernäten samt antalet och typen av telekomabonnemang. Statistiken presenteras i rapporter varje halvår.

Informationen i följande avsnitt kommer från användarrapporten 2015 och rapporten Svensk Telekommarknad 2016[3]. Internetstiftelsen i Sverige, IIS, har också gjort en undersökning om svenskarnas internetvanor med liknande resultat, rapporten Svenskarna och internet 2016.

7.3.1 Mobiltelefoner och mobilt internet

År 2016 fanns det totalt 14,6 miljoner abonnemang på mobila samtals- och datatjänster (inklusive mobilt bredband som fristående tjänst) i Sverige, varav mer än hälften var abonnemang i vilka 1 gigabyte datatrafik eller mer ingår. Abonnemang på tjänster för s.k. machine-to-machine (M2M) uppgick till 8,7 miljoner, vilket innebär en ökning med 28 procent från föregående år. Mobiltelefonin stod för 79 procent av all utgående samtalstrafik, vilket är en ökning från tidigare år. Knappt 11 miljoner var kontraktsabonnemang och resterande del, drygt 3,5 miljoner abonnemang, var kontantkort. Kontantkorten utgjorde således ungefär en fjärdedel av abonnemangen. För tio år sedan var hälften av abonnemangen kontantkort. Det ringdes ungefär 10,2 miljarder samtal från mobilabonnemang 2016. Det genomsnittliga antalet samtal per månad från privata abonnemang var 67. Ett privatsamtal pågick i snitt i drygt tre minuter.

Under 2016 överfördes 639 000 terabyte data i mobilnäten, vilket var en ökning med 35 procent jämfört med föregående år. De fyra

[2] PTS rapport Svenskarnas användning av telefoni och internet 2015 (PTS-ER-2015:29), 10 december 2015.
[3] PTS rapport Svensk Telekommarknad 2016 (PTS-ER-2017:10), 22 maj 2017.

största operatörerna, Telenor, Tele2, Hi3G och Telia, stod tillsammans för 98 procent av trafiken. Av datatrafiken härrörde knappt hälften från abonnemang för mobilt internet och den andra dryga hälften från mobiltelefonabonnemang.

Skickade sms har minskat kraftigt sedan 2011, då det skickades omkring 9 miljarder sms i halvåret, till omkring 6,5 miljarder för motsvarande tid år 2014. Under 2016 (helåret) skickades det 9 miljarder sms. Minskningen, som pågått sedan 2011, kan enligt PTS bero på att andra meddelandetjänster, så som Imessage, Whatsapp och Kik, har ökat i popularitet. Den klart största mängden sms (knappt 8 miljarder) skickades från privata abonnemang. Det skickades i genomsnitt 60 sms och drygt 3 mms per privat abonnemang och månad.

Omkring 97 procent av Sveriges befolkning använde mobiltelefon för privat bruk och närmare 90 procent hade en smart telefon år 2015. I stort sett samtliga av mobilanvändarna använde telefonen för samtal och 85 procent använde den till internetsurfning (vilket kan jämföras med 46 procent år 2011 och 74 procent år 2013). Ungefär tre fjärdedelar hade kopplat upp sig mot ett trådlöst nätverk (wifi) och lika många hade använt mobiltelefonen för e-post. 65–70 procent använde mobiltelefonen för att titta på film, lyssna på musik och för sociala medier. En dryg fjärdedel använde mobiltelefonen för att ringa med internettelefoni. I samtliga fall hade användandet ökat i jämförelse med år 2013. Även användandet av mobiltelefonen utomlands hade ökat.

Nästan alla mobiltelefonanvändare skickade meddelanden med sin telefon. Omkring 90 procent skickade meddelande varje vecka och omkring hälften av alla användare skickade meddelande varje dag. Omkring hälften av deltagarna i undersökningen svarade att de skickar meddelanden via internet (exempelvis Messenger eller Whatsapp).[4]

[4] Eftersom meddelandeprogram (exempelvis den förvalda meddelandeappen för Iphone) kan hantera flera meddelandetjänster, t.ex. både Imessage och sms, och dessutom använder sig av telefonnummer för att identifiera andra användare, kan det spekuleras i om många använder meddelandetjänster över internet i tron att de skickar sms via sin operatör. Det är därför möjligt att många använder sådana tjänster utan att veta om det. Enligt Business insider uppgav Eddy Cue, senior vice president för Apple, år 2016 att det skickades 200 000 meddelanden med Imessage per sekund (Kif Leswing, Apple says people send as many as 200,000 Imessages per second, Business insider, 12 feb. 2016). Som framgår i detta avsnitt har även sms-trafiken minskat kraftigt sedan år 2011, vilket inte kan förklaras av hur folk uppger att de använder sina mobiltelefoner.

7.3.2 Fast telefoni

Användandet av fast telefoni minskar. År 2015 var det nära hälften av dem som deltog i PTS användarundersökning som uppgav att de inte hade fast telefoni. Det var framför allt personer under 40 år som inte hade det men även bland äldre minskade andelen. Allt fler kunde tänka sig att avstå från sin fasta telefon till förmån för att enbart använda mobiltelefon. Antalet abonnemang för fast telefoni minskade med 300 000, från 3,6 miljoner år 2015 till 3,3 miljoner år 2016. Det innebär en minskning med 7 procent på bara ett år. Drygt hälften av alla abonnemang för fast telefoni utgjordes av ip-telefoniabonnemang.

Totalt ringdes det 1,3 miljarder samtal från det fasta nätet under första halvåret 2016. Det genomsnittliga antalet samtal per privat fastnätsabonnemang och månad var 22. Samtalen var längre än vid mobiltelefoni; ett genomsnittligt privat samtal var drygt fem minuter långt.

Drygt hälften av svenskarna hade år 2015 använt internettelefoni via dator eller surfplatta (exempelvis genom tjänster som Skype och Viber). Sedan 2013 har den grupp som använder internettelefoni för att ringa till fasta och mobila telefoner ökat.

7.3.3 Internet i hemmet

Nära 95 procent av befolkningen använde internet i hemmet år 2015. En fjärdedel uppgav sig ha en gruppanslutning genom exempelvis sin hyresvärd. Den vanligaste anslutningen som användes var fiber. Mobilt bredband användes av 27 procent av internetanvändarna.

Av dem som använde internet hemma var det 90 procent som använde det för e-post. Andra stora användningsområden var film, handel och sociala medier.

7.3.4 Andra användningsområden

Utöver mobiltelefoner, surfplattor och datorer finns det en mängd andra apparater som använder sig av elektronisk kommunikation. Allt från glödlampor, kläder och hushållsapparater till värmesystem, fordon och byggnader kan numera vara anslutna till internet eller på

andra sätt uppkopplade mot omvärlden. Sverige är bland de länder i världen som har mest enheter uppkopplade per person (OECD:s rapport OECD Digital Economy Outlook 2015 s. 259).

Av störst intresse är kanske den allt vanligare uppkopplingen i fordon. Fordon kan vara uppkopplade för flera syften, såsom trafiksäkerhet, bränsleeffektivitet, karttjänster och underhållning. Fordonet genererar information om exempelvis position och hastighet, som av olika anledningar kan behöva kommuniceras elektroniskt via mobilnätet. Även äldre fordon kan bli uppkopplade med tjänster som exempelvis Telia Sense, som låter fordonet kommunicera med en mobilapp och med internet, genom ett sim-kort. Från och med april 2018 måste dessutom alla nya bilar vara utrustade med det automatiska nödsamtalssystemet Ecall[5], som vid en olycka automatiskt kan sända information om exempelvis fordonets position till en larmcentral via gsm-nätet.

7.4 Nyttan och behovet av de olika uppgifterna

Polismyndigheten och Säkerhetspolisen har anfört att det inte är möjligt att identifiera någon av de uppgifter som omfattas av lagringsskyldigheten som viktigare än någon annan då de varierar från verksamhet till verksamhet och från ärende till ärende. Polismyndigheten och Säkerhetspolisen har ändock rangordnat uppgifterna i en prioritetsordning. Ekobrottsmyndigheten har i princip anslutit sig till denna bedömning. Åklagarmyndigheten har instämt i att det är svårt att rangordna betydelsen av de olika uppgifterna men anfört att de viktigaste uppgifterna som används rör tid och plats för kontakt mellan två adresser och uppgift om vilka dessa adresser är. Tullverket har uppgett att alla uppgifter innebär nytta men att den absolut viktigaste informationen är tids-, datum- och lokaliseringsuppgifter.

Gemensamt för myndigheterna är att de skattar nyttan av uppgift om vilken tjänst som har använts vid mobiltelefoni och ip-telefoni lägre i förhållande till andra uppgifter, både i förundersöknings- och i underrättelseverksamhet. På samma sätt råder det tämligen stor enighet om att nyttan av att veta spårbar tid för på- och avloggning i

[5] Europaparlamentets och rådets förordning (EU) 2015/758 av den 29 april 2015 om typgodkännandekrav för montering av Ecall-system som bygger på 112-tjänsten i fordon och om ändring av direktiv 2007/46/EG.

de tjänster som har använts prioriteras lägre. När det gäller internetåtkomst har uppgift om typ av kapacitet för överföring värderats lågt.

Det ska dock betonas att de brottsbekämpande myndigheterna har uppgett att alla uppgifter är strängt nödvändiga att lagra för den brottsbekämpande verksamheten.

För en mer detaljerad redovisning av nyttan och behovet, se avsnitt 12.6.3–12.6.4.

7.5 Lagringstiden

När analysen av Digital Rights-domen gjordes (avsnitt 8.3) erhölls information från Polismyndigheten om åldern på de uppgifter om elektronisk kommunikation som inhämtats. I underrättelseverksamheten var de flesta inhämtade uppgifter yngre än en månad men det fanns ärenden där historik upp till sex månader var av stor vikt. I utredningsverksamheten var den största andelen uppgifter yngre än tre månader. Uppskattningsvis 20–25 procent var 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. (Ds 2014:23 s. 86)

Myndigheterna har uppgett att den lagringstid om sex månader som anges i LEK i många fall är för kort. Som exempel har Polismyndigheten anfört att ett mord av normal komplexitet tar ungefär sex månader att utreda. De mer komplicerade ärendena tar ännu längre tid. Polismyndigheten har även uppgett att behovet av långa lagringstider för användare av ip-adresser är särskilt påtagligt i barnpornografiärenden. Även med en lagringstid på sex månader måste man lägga ner hälften av alla barnpornografiärenden som upparbetas utomlands. Skälet till det är att dessa ärenden tar lång tid att bearbeta på grund av de många stegen i utredningen. Normalt följer ett sådant ärende dessa steg: Gärningsmannens nedladdning av barnpornografi följs av ett polisiärt tillslag. Materialet som beslagtas bearbetas i ursprungslandet. Därefter översänds materialet till rätt mottagar-

länder, t.ex. Sverige, för identifikation av gärningsmannen samt fortsatt utredning och lagföring.

Myndigheterna kan sammanfattningsvis sägas ha uppgett att de har behov av längst lagringstider för uppgifter hänförliga till mobil telefoni och ip-telefoni samt för abonnemangsuppgifter hänförliga till internetåtkomst. De har inte redovisat några avgörande skillnader mellan underrättelseverksamhet och förundersökningsverksamhet.

8 EU-rättens påverkan på reglerna om datalagring

8.1 Datalagringsdirektivet

8.1.1 Direktivets syfte och tillämpningsområde

Det numera upphävda direktivet 2006/24 antogs den 15 mars 2006 och 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). Datalagringsdirektivet reglerade således – till skillnad från de relevanta artiklarna i direktiv 2002/58 – även abonnemangsuppgifter, se avsnitt 4.2.

Direktivet gällde, enligt artikel 1.2, trafik- och lokaliseringsuppgifter om såväl fysiska som juridiska personer samt uppgifter som var nödvändiga för att kunna identifiera abonnenten eller den registrerade användaren, alltså, som strax ovan har nämnts, även abonnemangsuppgifter.

8.1.2 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 genererades eller behandlades av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät vid leverans av kommunikationstjänster.

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 var 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 var 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.

8.1.3 Tillgången till 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 uppgifterna skulle få 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 skulle säkerställa att de lagrade uppgifter var 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 kunde överföras till behöriga myndigheter utan dröjsmål (artikel 8).

Frågan om uppgiftsskydd och datasäkerhet reglerades i artikel 7 i direktivet, där det angavs att varje medlemsstat skulle säkerställa att leverantörerna som lagrade uppgifter enligt direktivet skulle respek-

tera 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 skulle säkerställa att de skyddades mot förstöring, förlust, ändring eller olaglig lagring, behandling av, tillgång till eller avslöjande av uppgifterna samt som skulle säkerställa att tillgång gavs endast till bemyndigad personal. Vidare angavs att uppgifterna skulle förstöras vid slutet av lagringstiden, utom de uppgifter för vilka tillgång hade medgetts och som hade 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 skulle genomföra bestämmelserna om rättslig prövning, ansvar och sanktioner i dataskyddsdirektivet skulle bli 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 (ETS 185) liksom dataskyddskonventionen skulle också omfatta uppgifter som lagras i enlighet med direktivet om lagring av trafikuppgifter (skäl 20).

8.1.4 Den svenska genomförandeprocessen

Datalagringsdirektivet genomfördes i svensk rätt genom författningsändringar 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 §§ FEK.

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 på eget initiativ att de föreskrifter om skyddsåtgärder som regeringen bemyndigades att meddela snarast skulle underställas riksdagen för prövning (8 kap. 6 § RF). Detta gjordes 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.

8.2 EU-domstolens första dom – Digital Rights-domen

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

EU-domstolen konstaterade att de uppgifter som skulle lagras enligt direktivet sammantaget gjorde 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 i domen). Domstolen slog fast att redan lagringsskyldigheten i fråga om de aktuella uppgifterna avseende personers privatliv och kommunikationer utgjorde ett ingrepp i de rättigheter som skyddas enligt artikel 7 i rättighetsstadgan (dvs. rätten till respekt för privatlivet och familjelivet; se punkt 34 i domen). Ett ytterligare ingrepp i denna rättighet gjordes enligt domstolen när nationella myndigheter

medgavs tillgång till de lagrade uppgifterna (punkt 35). Det kunde alltså enligt domstolen konstateras att det 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 (dvs. rätten till skydd av personuppgifter; se punkt 36 i domen).

Domstolen slog i avgörandet 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 kunde ge berörda personer en känsla av att deras privatliv stod under ständig övervakning (punkt 37). Domstolen konstaterade trots det att skyldigheten 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 prövning av om direktivet levde upp till den unionsrättsliga proportionalitetsprincipen. Domstolen konstaterade inledningsvis att lagringen var ägnad att nå det eftersträvade målet eftersom de nationella myndigheternas tillgång till lagrade trafikuppgifter innebar 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 strängt nödvändigt (punkt 52). Det innebär 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 uppgifterna 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 att se till att tillgången begränsas till vad som är strängt 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 strängt 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 skulle ta ekonomiska hänsyn när de skulle bestämma säkerhetsnivån eller för att uppgifterna skulle förstöras när lagringstiden hade 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 hade 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. Innebörden av att domen får tillbakaverkande effekt är dock inte att nationella genomförandeåtgärder också omedelbart blir ogiltiga (SOU 2015:31 s. 116).

8.3 Analysen efter Digital Rights-domen (Ds 2014:23)

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 §§ LEK samt övriga bestämmelser om tillgång till och behandling av sådana uppgifter och deras förhållande till unionsrätten. Analysen redovisades i juni 2014 i promemorian Datalagring, EU-rätten och svensk rätt (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 särskilt pekade på i domen. I analysen betonades att domstolens slutsats – att direktivet står i strid med rättigheter som garanteras av stadgan – byggde 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 skulle anses oproportionerlig, utan det var först vid den sammantagna bedömningen som svensk rätts förenlighet med EU-rätten fullt ut kunde avgöras. På samma sätt som EU-domstolens dom, avslutades analysen därför med en samlad bedömning av om den svenska regleringen var proportionerlig och förenlig med Europarätten och EU-rätten. Det konstaterades därvid att det kunde 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, var förenlig med unionsrätten och europarätten.

Slutsatserna i denna första analys redovisas närmare i det följande.

8.3.1 Lagringsskyldighetens omfattning

Generellt om lagringsskyldigheten

EU-domstolen konstaterade i sin dom (punkterna 56–59) att omfattningen av den lagringsskyldighet som följde av artiklarna 3 och 5 i direktivet innebar att trafikuppgifter skulle lagras för alla personer och alla elektroniska kommunikationssätt, utan att någon urskillning skulle göras av de uppgifter som kunde tänkas vara relevanta för att uppnå målet att bekämpa allvarlig brottslighet. Man kunde därmed säga att den inskränkning i de grundläggande rättigheter som följde av artiklarna 7 och 8 omfattade hela Europas befolkning. Domstolen angav att lagringsskyldigheten som följde av direktivet således omfattade även personer som inte misstänktes 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 eller begränsningar till en viss grupp av människor som gjorde att lagringsskyldigheten bara omfattade sådana uppgifter som av något skäl kunde antas ha relevans för att förhindra, utreda eller åtala allvarliga brott.

Direktiv 2002/58 innehåller regler om i vilka situationer och för vilka syften trafikuppgifter får behandlas. Tidigare följde av artikel 11 i det numera upphävda datalagringsdirektivet att artikel 15.1 i direktiv 2002/58 inte skulle tillämpas på de uppgifter som specifikt måste lagras enligt datalagringsdirektivets bestämmelser.

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

I denna del hade utredaren inhämtat information från polisen om behovet av de uppgifter som omfattas av lagringskravet enligt de

svenska reglerna (se för detta och det följande Ds 2014:23 s. 52). Det framkom då att ingen lagrad information som i dag kan hämtas in kunde anses som oviktig. Som extremt viktiga angavs uppgifter om lokaliseringen av var en telefon eller internetsession kopplat upp och riktningen till basstationen. 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 § 1 FEK), uppgifter om den första aktiveringen av en förbetald anonym tjänst (del av 40 § 3 FEK) och uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten (41 § 3 FEK). När det gällde 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 § 4 och 5 FEK) 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 var 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 kunde 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 var 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 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 (Ds 2014:23 s. 53).

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 kombinerad 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 kunde anses proportionerlig. Även skyddet för den merpart av alla uppgifter som lagras men aldrig begärs utlämnade konstaterades också vara tillräckligt högt (Ds 2014:23 s. 54–55).

Särskilt om uppgifter som omfattas av yrkesmässig tystnadsplikt

Domstolen lyfte i Digital Rights-domen 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 då nyligen föreslagit att reglerna om avlyssningsförbud vid hemlig avlyssning av elektronisk kommunikation i 27 kap. 22 § RB skulle 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 RB (prop. 2013/14:237 s. 131–133). Det konstaterades samtidigt att det aldrig hade 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 bedömdes att det ur ett EU-rättsligt perspektiv inte fanns något som tydde på en konflikt mellan reglerna om yrkesmässig tystnadsplikt och ett generellt lagringskrav avseende trafikuppgifter (Ds 2014:23 s. 55–56).

8.3.2 Tillgången till uppgifterna

Direktivet och EU-domstolens första dom

I artikel 4 i datalagringsdirektivet föreskrevs att medlemsstaterna skulle vidta åtgärder för att säkerställa att uppgifter som lagrades i enlighet med direktivet skulle göras 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 skulle finnas tillgängliga för utredning, 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 (prop. 2010/11:46 s. 47–49). 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 brotten i den lista som finns i artikel 2 i rådets rambeslut den 13 juni 2002 om en europeisk arresteringsorder och överlämnande mellan medlems-

staterna (2002/548/RIF) och till brott där telekommunikation ingår (prop. 2010/11:46 s. 21). 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 förfalskning och hjälp till olovlig inresa, finns på listan.

I Digital Rights-domen kritiserade EU-domstolen på ett antal punkter att datalagringsdirektivet inte närmare reglerade hur tillgång skulle ges till de lagrade uppgifterna, 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 kunde få tillgång till uppgifterna. Vidare innehöll direktivet inga bestämmelser som begränsade antalet personer som kunde få tillgång till uppgifterna till vad som kunde anses absolut nödvändigt. Domstolen lyfte också fram att de nationella myndigheternas tillgång till lagrade trafikuppgifter inte var beroende av en föregående kontroll av en domstol eller av ett annat organ.

Analysen som gjordes i promemorian såvitt avser tillgången till lagrade uppgifter redogörs för i det följande.

Tillgången till uppgifter enligt RB

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.

I analysen konstaterades inledningsvis att det stora flertalet brott som omfattas av tillämpningsområdet för hemlig övervakning av elektronisk kommunikation har ett minimistraff på fängelse i minst sex månader. 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 (s. 75 i promemorian).

Det noterades vidare att hemlig övervakning av elektronisk kommunikation därutöver får användas i förundersökning om narkotikabrott och narkotikasmuggling (som inte är ringa) och för att

utreda dataintrång och barnpornografibrott, 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 (s. 75).

När det gäller barnpornografibrott och dataintrång framhölls i analysen att straffskalorna för dessa brottstyper gav stöd för 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 konstaterades samtidigt 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 skulle innebära att barnpornografibrott inte skulle kunna utredas knappast godtagbar. 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 (s. 75–76).

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 spioneri. 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 (s. 76).

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 (s. 77).

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 prövar 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 (s. 78).

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

Tillgången till uppgifter enligt IHL

De brottsbekämpande myndigheternas tillgång enligt IHL är 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. 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 så som sabotage, spionerі och andra brott som bekämpas av Säkerhetspolisen.

I analysen i departementspromemorian framhölls inledningsvis att brott vars minimistraff är fängelse i minst två år tveklöst tillhör kategorin allvarliga brott (s. 81). 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 (s. 81–82).

Ett frågetecken som lyftes i analysen är det förhållandet att uppgifter hämtas in av myndigheterna själva utan föregående prövning

av en oberoende instans (s. 83). Samtidigt framhölls att frågor om rättssäkerhet och integritetsskydd hade varit föremål för ingående överväganden när IHL 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 dittills hade presenterats av SIN och de brottsbekämpande myndigheterna visade att inhämtning utfördes 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 inhämtningsbesluten, 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 IHL kan hämtas in bara för mycket allvarlig brottslighet för vilken samhällsintresset är betydande (s. 81–82).

8.3.3 Lagringstiden

EU-domstolen konstaterade i Digital Rights-domen 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 hade tillåtits ett tidsspann på sex månader upp till två år, några objektiva kriterier som tillgodoser att lagringstiden begränsas till vad som kan anses strängt 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 fanns några EU-rättsliga krav som hindrar att en kortare lagringstid än sex månader väljs (s. 85). Det konstaterades dock att för att de lagrade uppgifterna skulle tjäna sitt syfte, nämligen att kunna användas för att upptäcka, utreda och lag-

föra 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 (s. 86).

Mot bakgrund av detta riskerade, enligt bedömningen i promemorian, en kortare lagringstid än sex månader att leda till att syftet med lagringen inte kunde 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 (s. 86).

Sammanfattningsvis bedömdes därför en lagringstid om sex månader uppfylla EU-domstolens krav på att tiden ska begränsas till vad som kan anses strikt nödvändigt (s. 86–87).

8.3.4 Säkerheten för de lagrade uppgifterna

Skyddsregler och utplåning av uppgifter

EU-domstolen fann i Digital Rights-domen att direktivets regler om skydd för lagrade uppgifter var otillräckliga på flera punkter (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 i promemorian 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 (s. 90 i promemorian).

Vidare konstaterades i analysen att 37 § FEK 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 § FEK 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 uppgifter, 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 (s. 90). Det påpekas 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 noteras 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 § RB och 9 § IHL. 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 (Europadomstolens domar i målen Natunen mot Finland, 31 mars 2009, och Janatuinen mot Finland, 8 december 2009, 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 (s. 91–92).

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 (s. 92–93).

Krav på lagring inom EU

EU-domstolen pekade i Digital Rights-domen på att datalagringsdirektivet inte krävde att uppgifterna skulle lagras inom unionen. Detta innebar enligt domstolen att den oberoende myndighetskontrollen av att skydds- och säkerhetskraven för de lagrade uppgifterna 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 promemorian framhölls att det mot bakgrund av domstolens uttalanden om intresset av effektiv tillsyn fanns mycket som talade för att det bör införas ett krav på att lagringen av uppgifter ska göras inom EU eller EES (s. 97). I anslutning till denna bedömning redogjordes också för risken för 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 (s. 96–97).

8.3.5 Samlad bedömning

Sammanfattningsvis framhölls i analysen att det svenska regelverket avseende lagring enligt 6 kap. 16 a–f §§ LEK samt bestämmelserna om tillgång och behandling av sådana uppgifter med beaktande av EU-domstolens uttalanden, inte strider mot unionsrätten eller europarätten. Utredaren fann dock att det fanns skäl att ändå närmare överväga några frågor. Det gällde dels lagringsskyldigheten avseende ett par uppgiftskategorier, dels reglerna om tillsyn såvitt avser inhämtning av abonnemangsuppgifter samt reglerna om en oberoende kontroll såvitt gäller inhämtning av uppgifter i underrättelseskedet. Vidare ansågs att det kunde övervägas om ett uttryckligt förbud mot lagring utanför EU/EES borde införas (s. 101).

8.4 Datalagringsutredningens överväganden (SOU 2015:31)

Som en uppföljning av analysen i departementspromemorian Datalagring, EU-rätten och svensk rätt (Ds 2014:23) gav regeringen en utredare i uppdrag att överväga ytterligare rättssäkerhets- och inte-

gritetsstärkande åtgärder för IHL och för reglerna om lagring enligt 6 kap. 16 a–f §§ LEK (dir. 2014:101).

Utredningen, som antog namnet Datalagringsutredningen, redovisade sina slutsatser i betänkandet Datalagring och integritet (SOU 2015:31) i mars 2015.

Datalagringsutredningens slutsatser redovisas i det följande.

8.4.1 Inget förslag om förändring i fråga om vilka uppgiftskategorier som ska lagras

I departementspromemorian gjordes bedömningen att inga av de uppgifter som omfattas av datalagringsskyldigheten var att anse som oviktiga. Vissa bedömdes dock vara mindre viktiga (avsnitt 8.3.1).

Enligt de uppgifter Datalagringsutredningen inhämtade framgick dock att samtliga uppgiftskategorier som ska lagras enligt LEK bedömdes vara av stor vikt för brottsbekämpningen (SOU 2015:31 s. 167). Mot bakgrund härav föreslog inte utredningen någon förändring i fråga om vilka uppgiftskategorier som skulle lagras enligt datalagringsreglerna.

8.4.2 Inget förslag om krav på lagring inom EU

Som antecknades i departementspromemorian, fanns inte något krav i datalagringsdirektivet på var uppgifterna skulle lagras. I den mån de lagrade uppgifterna var personuppgifter kunde dock den allmänna dataskyddaregleringen påverka i vilken utsträckning det var möjligt att överföra uppgifterna till andra länder (s. 93 i Ds 2014:23).

Datalagringsutredningen konstaterade att 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 (SOU 2015:31 s. 178 med hänvisning till prop. 2010/11:46 s. 60). Detta skulle enligt Datalagringsutredningen särskilt beaktas av leverantörerna vid överväganden 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. Det ansvaret gäller oberoende av var leverantörerna väljer att lagra uppgifter. Som framgår nedan har PTS vissa befogenheter för

att kontrollera att leverantörerna följer skydds- och säkerhetsreglerna. Regeringen bedömde när datalagringsdirektivet genomfördes att de befogenheterna fick anses vara tillräckliga för att myndigheten skulle kunna utöva en aktiv och ändamålsenlig tillsynsverksamhet (prop. 2010/11:46 s. 58).

PTS befogenhet att få tillträde till områden, lokaler och andra utrymmen där verksamhet som omfattas av LEK bedrivs kunde enligt Datalagringsutredningen 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 kom Datalagringsutredningen till slutsatsen att PTS har vissa möjligheter att bedriva en aktiv och ändamålsenlig tillsynsverksamhet även gentemot leverantörer som väljer att lagra uppgifter utanför unionen (SOU 2015:31 s. 179).

I sammanhanget framhöll Datalagringsutredningen 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 skulle det enligt Datalagringsutredningen 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 (SOU 2015:31 s. 179).

Mot den bakgrunden kom Datalagringsutredningen till slutsatsen att den oberoende myndighetskontrollen var 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 innebar således, enligt Datalagringsutredningen, inte att regleringen i svensk lag stred mot bestämmelserna om grundläggande rättigheter i EU-stadgan. Enligt utredningen skulle dessutom ett förbud mot lagring utanför EU strida mot Sveriges åtaganden enligt dataskyddskonventionen. (SOU 2015:31 s. 179–182)

8.4.3 Uppgifter som omfattas av tystnadsplikt

Inget förbud mot övervakning av personer som omfattas av tystnadsplikt

I fråga om förbud mot övervakning av personer med tystnadsplikt konstaterade Datalagringsutredningen inledningsvis att svensk rätt intar ståndpunkten att det normalt är en uppgifts innehåll som avgör om den omfattas av skydd mot avlyssning och undantag från vittnesplikt. Trots det kunde det enligt utredningen i vissa situationer finnas ett intresse av att begränsa myndigheternas insyn i att kommunikation över huvud taget har förekommit, t.ex. vid 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 (SOU 2015:31 s. 208).

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 lämnas för publicering. Vid inhämtning av uppgifter om elektronisk kommunikation känner de brottsbekämpande myndigheterna normalt sett inte till innehållet i kommunikationen. Det innebär att det oftast inte går att avgöra vilka uppgifter som omfattas av tystnadsplikt. Ett förbud mot att hämta in sådana uppgifter skulle därför enligt Datalagringsutredningen vara mycket svårt att tillämpa. Om myndigheten i något fall skulle känna till att de aktuella uppgifterna omfattas av yrkesmässig tystnadsplikt redan innan inhämtning utförs, 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, enligt Datalagringsutredningen, vara av begränsat praktiskt värde. Något förslag på sådant förbud lämnades därför inte (SOU 2015:31 s. 209).

Förslag på förstörandeskyldighet

Ett annat tänkbart alternativ för att stärka skyddet för uppgifter som omfattas av yrkesmässig tystnadsplikt var enligt Datalagringsutredningen att införa regler om att sådana uppgifter ska förstöras i efterhand. Även tillämpningen av en sådan regel skulle visserligen nor-

malt förutsätta att den brottsbekämpande myndigheten känner till innehållet i kommunikationen. Det skulle dock enligt utredningen inte vara otänkbart att det i undantagsfall skulle kunna inträffa att myndigheten får sådan kännedom, 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 uppteckningsarna 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 Datalagringsutredningens uppfattning var detta en brist i skyddet för den yrkesmässiga tystnadsplikten. Utredningen kunde inte heller se några tungt vägande skäl mot att den brottsbekämpande myndigheten i en sådan situation skulle vara skyldig att radera även uppgifter som anger att kommunikationen har ägt rum (SOU 2015:31 s. 209–210).

Mot bakgrund av det ovan anförda föreslog Datalagringsutredningen en skyldighet för de brottsbekämpande myndigheterna att förstöra uppteckningsar från hemlig övervakning av elektronisk kommunikation och inhämtning av uppgifter enligt IHL i de delar uppteckningsarna innehåller uppgifter som, på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena RB, 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. Det var emellertid enligt Datalagringsutredningen inte något starkt skäl för att avstå från att införa reglerna (SOU 2015:31 s. 210).

8.4.4 IHL

Datalagringsutredningen gjorde en genomgång av tillämpningen av IHL hos Säkerhetspolisen, Polismyndigheten och Tullverket. För denna genomgång hänvisas till Datalagringsutredningens betänkande Datalagring och integritet (SOU 2015:31 s. 213–283).

I anslutning till denna genomgång övervägdes ett antal förslag som skulle kunna stärka rättssäkerheten och integritetsskyddet. Dessa förslag redogörs för i det följande.

Inget förslag med krav på förhandskontroll av domstol

Datalagringsutredningen inledde sina överväganden i fråga om ändrad beslutsordning med att erinra om att alternativet med domstolsprövning övervägdes redan i samband med att IHL infördes. Regeringen uttalade då följande (prop. 2011/12:55 s. 88–89).

> 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 […] 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.

Enligt Datalagringsutredningens uppfattning saknades det skäl att göra någon annan bedömning än den regeringen gjorde när IHL infördes. De argument som då fördes fram mot en domstolsprövning hade fortfarande bärkraft. Vidare noterade utredningen att underrättelseverksamheten, till skillnad från en förundersökning, inte primärt är inriktad på någon viss gärning eller någon viss person. Till detta kom den omständigheten att det är tveksamt om domstolarna, inom ramen för den nuvarande jourorganisationen, skulle kunna tillgodose de brottsbekämpande myndigheternas behov av snabba beslut. 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 var dock inte heller helt oproblematisk enligt Datalagringsutredningen. Dels kvarstår övriga argument mot en domstolsprövning. Dels gäller i princip samtliga beslut enligt IHL 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 dem som gäller i fråga om interimistiska beslut om hemliga tvångsmedel under en förundersökning (27 kap. 21 a § RB). Att föreskriva att inhämtade uppgifter i en liknande situation inte får användas i en förundersökning är enligt Datalagringsutredningen 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 framstod enligt Datalagringsutredningen inte som förtroendeingivande. (SOU 2015:31 s. 288–289)

Ett annat skäl som enligt Datalagringsutredningen talade mot att beslutskompetensen skulle anförtros domstol, eller någon annan myndighet som är fristående från de brottsbekämpande myndigheterna, var intresset av att kunna hålla den information som finns i underrättelseärendena inom en så snäv personkrets som möjligt. Även om domstolarna naturligtvis har stor vana av att hantera sekre-

tesskyddat material på ett säkert sätt, går det enligt utredningen inte att bortse från att risken för spridning av informationen ökar ju större personkrets som får tillgång till den. (SOU 2015:31 s. 289)

Datalagringsutredningen lämnade därför inte något förslag på förhandsprövning av domstol.

Inget förslag om möjlighet att överklaga

Ett annat alternativ som Datalagringsutredningen övervägde var att konstruera ett system med en möjlighet att överklaga de brottsbekämpande myndigheternas beslut enligt IHL till domstol. En sådan ordning inrymde dock enligt utredningen en hel del praktiska problem. 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 skulle enligt utredningen förutsätta att ett offentligt ombud eller motsvarande involveras i beslutsprocessen hos myndigheterna. Dessutom var det enligt utredningen sannolikt att relativt få beslut skulle överklagas. Svårigheten för tingsrätterna att arbeta upp en vana av att handlägga ärenden enligt inhämtningslagen var 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. Utredningen lämnade därför inte något förslag om överklagande av beslut enligt IHL (SOU 2015:31 s. 290).

Inget förslag om åklagarbeslut

Datalagringsutredningen övervägde om åklagare skulle få en roll vid beslut enligt IHL (SOU 2015:31 s. 290–292). Utredningen inledde med att notera att regeringen i förarbetena till IHL konstaterade att åklagare som regel inte deltar i polisens eller Tullverkets underrättelseverksamhet och att åklagare inträder först i samband med att förundersökning har 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 myndigheternas

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.

Datalagringsutredningen noterade i och för sig att åklagare har en roll i beslutsprocessen när det gäller preventiva tvångsmedel men konstaterade samtidigt att lagen om preventiva tvångsmedel används 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 var därför enligt Datalagringsutredningen betydligt mindre.

Mot den angivna bakgrunden borde det enligt Datalagringsutredningen 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. Några sådana indikationer fanns inte enligt Datalagringsutredningen. Det saknades därför sådana starka skäl som borde krävas för att föreslå att beslutsbefogenheten skulle anförtros åklagare (SOU 2015:31 s. 292).

Inget förslag på nytt beslutsorgan

Datalagringsutredningen övervägde även om förslag skulle lämnas på en ny nämnd som skulle pröva frågor enligt IHL. Utredningen pekade på att frågan om det är lämpligt att inrätta särskilda nämnder för beslut enligt lagen om preventiva tvångsmedel övervägdes när den infördes. Regeringen bedömde då att ett system med en särskild nämnd hade 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. 64–65).

Frågan övervägdes på nytt i samband med att IHL 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 var enligt Datalagringsutredningen 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 kunde 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.

Datalagringsutredningen instämde vidare i regeringens tidigare bedömning att ett nämndsystem skulle innebära vissa praktiska nackdelar. Prövningens i många fall brådskande natur i kombination med en spridd geografisk förekomst gjorde att det inte framstod 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 framstod ur ett verksamhets- och effektivitetsperspektiv inte heller som särskilt lämpligt (SOU 2015:31 s. 293).

En annan fråga var hur ett nämndsystem skulle behöva organiseras för att de brottsbekämpande myndigheternas behov av snabba beslut skulle kunna tillgodoses. Det var för utredningen knappast rimligt att tänka sig att ett antal nämnder av det aktuella slaget skulle vara tillgängliga dygnet runt för att snabbt kunna fatta beslut i frågor om inhämtning av uppgifter enligt IHL. Visserligen skulle det kunna 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. Något förslag på inrättande av en särskild nämnd lämnades därför inte av Datalagringsutredningen (SOU 2015:31 s. 293).

Inget förslag på förändrad beslutsnivå inom myndigheterna

Myndighetschefen får enligt 4 § IHL 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).

Av dessa skäl och eftersom bestämmelsen om delegation har en så strikt utformning som man rimligen kan begära föreslog Datalagringsutredningen i den här delen inga författningsändringar.

Förslag om underrättelseskyldighet till SIN

Datalagringsutredningen undersökte om det fanns några åtgärder som enligt SIN:s uppfattning skulle kunna vidtas för att göra tillsynen än mer effektiv. Nämnden framförde att bestämmelsen i 6 § IHL om underrättelseskyldighet till nämnden skulle kunna förtydligas på så sätt att det skulle framgå att underrättelseskyldigheten tar sikte på själva beslutet (SOU 2015:31 s. 298).

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 annat sätt, t.ex. genom en särskild skrivelse, och i vissa fall uppkommer frågan om SIN verkligen fått del av beslutet. Enligt nämnden skulle emellertid följderna av otydligheten i detta avseende inte överdrivas.

Det var enligt Datalagringsutredningen rimligt att underrättelseskyldigheten skulle fullgöras på det sätt som SIN hade förordat, dvs. genom att den brottsbekämpande myndigheten ger in själva beslutshandlingen till nämnden. Ett förslag till sådant förtydligande lämnades därför av utredningen (SOU 2015:31 s. 298).

Inget förslag på krav på beslutens innehåll

Enligt 5 § IHL 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 innefattas 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 framförde till Datalagringsutredningen 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 angav de beslutande myndigheterna 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 IHL (2 och 3 §§) och att överskottsinformation samt förstöring av materialet hanteras rättsenligt (7 och 9 §§) kunde det enligt nämnden 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 enligt Datalagringsutredningen 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 mot vissa brottstyper eller brottsliga företeelser (prop. 2009/10:85 s. 362–363).

Utredningen uppmärksammade även vid kartläggningen att det varierade en del hur den brottsliga verksamheten beskrevs i beslut enligt IHL. I vissa fall angavs endast det eller de brott som verksamheten bedömdes innefatta, medan besluten i andra fall innehöll mer konkreta beskrivningar. Ett exempel på det senare var att det i ett beslut angavs att den brottsliga verksamheten utgörs av grovt narkotikabrott genom hantering av en viss mängd av ett angivet preparat. I vilken mån den brottsliga verksamheten kunde konkretiseras på ett sådant sätt var enligt Datalagringsutredningen beroende av vilken information som fanns i ärendet vid tidpunkten för beslutet.

Datalagringsutredningen uttryckte förståelse för att det kunde 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 enligt utredningen 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 hade föreslagit skulle innebära att detta inte längre skulle vara tillräckligt. Frågan inställde sig då om det i sådana fall inte längre skulle vara tillåtet att hämta in uppgifter enligt IHL. En sådan ändring skulle få effekter i fråga om vilket krav på konkretion som skulle ställas, för att det ska anses vara fråga om brottslig verksamhet. Detta kunde få konsekvenser som var svåra att överblicka. Krav på beskrivningar av mer konkret angiven brottslighet hörde enligt utredningen hemma på förundersökningsstadiet. Det var därför enligt Datalagringsutredningen inte lämpligt att föreslå någon ändring i fråga om kraven på hur den brottsliga verksamheten ska anges (SOU 2015:31 s. 300).

Inget förslag på förändrat 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)[1]. 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).

Bestämmelsen i 5 § IHL 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. Datalagringsutredningen frågade sig mot denna bakgrund om det finns anledning att ändra bestämmelsen så att det blir tydligare att så ska göras.

Det väsentliga var enligt Datalagringsutredningen 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 IHL 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 vad SIN uppgav för Datalagringsutredningen visar erfarenheterna från den tid som IHL har varit i kraft att denna ordning fungerar förhållandevis väl och att skälen för besluten i regel finns där de bör finnas. Mot den bakgrunden fanns det enligt Datalagringsutredningen inte skäl att föreslå några förändringar som skulle ta sikte på dokumentationsskyldigheten (SOU 2015:31 s. 301–302).

Inget förslag om förändrad tystnadsplikt

Enligt 6 kap. 20 § LEK har operatörerna tystnadsplikt för vissa uppgifter. Tystnadsplikten omfattar även uppgifter som hänför sig till användningen av hemliga tvångsmedel (6 kap. 21 §). Operatörernas tystnadsplikt gäller även i förhållande till SIN. Det innebär alltså att det inte är tillåtet för operatörerna att vidarebefordra information

[1] En ny förvaltningslag träder i kraft den 1 juli 2018, prop. 2016/17:180, bet. 2017/18:KU2, rskr. 2017/18:2.

som de får del av vid verkställighet av beslut om hemliga tvångsmedel till nämnden.

Datalagringsutredningen övervägde mot den nu angivna bakgrunden 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 kunde uppmärksamma vid verkställighet av beslut enligt IHL (SOU 2015:31 s. 302).

Datalagringsutredningen noterade i sammanhanget att någon information om vilket brott eller vilken brottslig verksamhet som ligger till grund för beslutet inte lämnas. Inte heller lämnas någon information om syftet med åtgärden. Möjligen skulle man enligt Datalagringsutredningen kunna tänka sig att en anställd hos en operatör utifrån denna information skulle kunna uppmärksamma om en beställning enligt IHL avser inhämtning av trafikuppgifter i realtid, vilket inte är tillåtet enligt lagen. Denna information skulle således kunna vidarebefordras till SIN. Enligt uppgift från SIN som Datalagringsutredningen inhämtade är detta emellertid ett förhållande som nämnden i sådana fall ändå skulle uppmärksamma genom myndigheternas underrättelser till nämnden.

I övrigt var det enligt Datalagringsutredningens 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 var det enligt Datalagringsutredningen t.ex. inte möjligt att bedöma om inhämtningen är tillåten enligt den lagstiftning som åberopas. Inte heller skulle det vara möjligt att ta ställning till frågor om proportionalitet och liknande, vilket enligt Datalagringsutredningen inte heller är operatörernas uppgift att göra.

SIN ställde sig mot den angivna bakgrunden tveksam till en sådan ordning. Nämnden påtalade också i sammanhanget att uppgifter förmodligen i många fall skulle komma att lämnas rätt formlöst, vilket skulle kunna innebära risker för att känslig information skulle spridas på ett olämpligt sätt. Detta kunde få negativa konsekvenser både för myndigheternas underrättelsearbete och för t.ex. källor.

Av dessa skäl bedömde Datalagringsutredningen att en lättnad av tystnadsplikten enligt LEK i förhållande till SIN inte skulle fylla någon större funktion. Något sådant förslag lämnades därför inte (SOU 2015:31 s. 303).

9 EU-domstolens andra dom – Tele2-domen

EU-domstolen meddelade den 21 december 2016 dom i de förenade målen C-203/15 mellan Tele2 och PTS och C-698/15 mellan Tom Watson, Peter Brice och Geoffrey Lewis, å ena sidan, och Secretary of State for the Home Department (inrikesministern i Förenade konungariket Storbritannien och Nordirland) å andra sidan. Båda målen avsåg förhandsavgöranden. Domen finns som bilaga till detta betänkande.

Respektive begäran om förhandsavgörande avsåg tolkningen av artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8 och 52.1 i rättighetsstadgan.

Till grund för förhandsavgörandet låg två frågor från Kammarrätten i Stockholm med följande innebörd:

1) Är en generell skyldighet att lagra trafikuppgifter som omfattar samtliga personer, samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter utan att det görs några åtskillnader, begränsningar eller undantag utifrån syftet att bekämpa brott förenlig med artikel 15.1 i direktiv 2002/58 med beaktande av artiklarna 7, 8 och 52.1 i stadgan?

2) Om svaret på fråga 1 är nej, kan lagringen ändå vara tillåten

a) om de nationella myndigheternas tillgång till de uppgifter som lagras är fastställd som i Sverige, och

b) om kraven på säkerhet är reglerade som i Sverige, samt då

c) samtliga aktuella uppgifter ska lagras i sex månader räknat från den dag kommunikationen avslutades och därefter utplånas?

I samma avgörande behandlades även två frågorna från Court of Appeal (England & Wales) (Civil Division):

1) Innebär Digital Rights-domen (särskilt punkterna 60–62) att det i unionsrätten uppställs tvingande krav som en medlemsstats

nationella bestämmelser om tillgång till uppgifter som lagrats i enlighet med nationell lagstiftning måste uppfylla för att vara förenliga med artiklarna 7 och 8 i rättighetsstadgan?

2) Innebär Digital Rights-domen att artikel 7 eller artikel 8 i stadgan ges ett mer vidsträckt tillämpningsområde än artikel 8 i Europakonventionen såsom den bestämmelsens tillämpningsområde har fastställts i praxis från Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen)?

Domstolen besvarade frågorna utifrån resonemanget nedan i avsnitten 9.1–9.10.

9.1 Direktiv 2002/58 är tillämpligt på datalagringsreglerna

I målet inför EU-domstolen förekom det olika uppfattningar i fråga om direktiv 2002/58 över huvud taget var tillämpligt. Det som gav upphov till de olika uppfattningarna var att å ena sidan föreskriver direktivet att det inte ska tillämpas på verksamhet på straffrättens område (artikel 1.3) samtidigt som direktivet å andra sidan anger att medlemsstaterna genom lagstiftning får vidta åtgärder för att begränsa omfattningen av vissa rättigheter i direktivet när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för bl.a. förebyggande, undersökning, avslöjande av och åtal för brott (artikel 15.1). Medlemsstaterna får enligt sistnämnda bestämmelse för de angivna ändamålen anta regler som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i punkten. Alla åtgärder ska enligt artikel 15.1 vara i enlighet med de allmänna principerna i gemenskapslagstiftningen.

EU-domstolen menade att om man såg till den allmänna systematiken i direktiv 2002/58 så betyder inte det att statens verksamhet på det straffrättsliga området ska anses utesluten från direktivets tillämpningsområde. Det skulle enligt domstolen helt frånta artikel 15.1 dess ändamålsenliga verkan. Nämnda bestämmelse förutsätter nämligen med nödvändighet att de där avsedda nationella åtgärderna, såsom de om lagring av uppgifter i brottsbekämpande syfte, omfattas av direktivets tillämpningsområde, eftersom direktivet uttryckligen tillåter medlemsstaterna att vidta sådana åtgärder

endast under förutsättning att de däri angivna villkoren är uppfyllda (p. 73 i domen).

EU-domstolen ansåg att direktivet omfattade både lagstiftning som reglerar lagringen av uppgifter och lagstiftning som reglerar tillgången till dessa uppgifter (p. 75–76 i domen).

9.2 Artikel 15.1 ska tolkas strikt

Som framgår av skäl 2 i direktiv 2002/58, eftersträvas i direktivet att säkerställa full respekt för rättigheterna i artikel 7 (respekt för privatliv) och 8 (skydd av personuppgifter) i rättighetsstadgan. Direktivet innehåller specifika bestämmelser för detta ändamål. Dessa bestämmelser syftar till att skydda personuppgifter och integritet hos användarna av elektroniska kommunikationstjänster mot de risker som ny teknik och den ökade kapaciteten för automatisk lagring och behandling av uppgifter medför (skäl 6 och 7).

Enligt artikel 5.1 i direktivet ska medlemsstaterna genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster liksom för därmed förbundna trafikuppgifter. Principen om konfidentialitet vid kommunikation innebär i princip ett förbud för andra personer än användarna att utan samtycke lagra trafikuppgifter avseende elektronisk kommunikation. Undantag gäller endast för personer som har laglig rätt att göra detta i enlighet med artikel 15.1 i direktivet, samt för teknisk lagring som är nödvändig för överföring av kommunikationen (p. 84–85 i domen).

Enligt artikel 6 i direktivet får trafikuppgifter behandlas och lagras i den utsträckning och under den tid som krävs för att kunna fakturera för tjänster, marknadsföra tjänster eller tillhandahålla kringtjänster. Vad specifikt gäller fakturering för tjänster, är sådan behandling endast tillåten fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning. När den perioden har löpt ut ska de behandlade och lagrade uppgifterna utplånas eller avidentifieras. Vad gäller andra lokaliseringsuppgifter än trafikuppgifter föreskriver artikel 9.1 i direktivet att de endast får behandlas på vissa villkor och sedan de har avidentifierats eller om användarna eller abonnenterna gett sitt samtycke (p. 86 i domen).

Räckvidden av bestämmelserna i de nu nämnda artiklarna (5, 6 och 9.1) i direktivet, som syftar till att säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter och att minimera riskerna för missbruk, ska enligt domstolen bedömas mot bakgrund av skäl 30 i direktivet. Där anges att ”[s]ystemen för tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster bör utformas så att mängden nödvändiga personuppgifter begränsas till ett absolut minimum” (p. 87 i domen).

I och med att artikel 15.1 i direktivet ger medlemsstaterna möjlighet att begränsa omfattningen av den principiella skyldigheten att säkerställa konfidentialiteten för kommunikation och därmed förbundna trafikuppgifter, ska denna artikel enligt domstolens fasta praxis tolkas strikt. En sådan bestämmelse kan därför enligt domstolen inte motivera att undantaget från denna principiella skyldighet, i synnerhet förbudet i artikel 5 i direktivet mot att lagra dessa uppgifter, görs till huvudregel. Det skulle enligt domstolen i stor utsträckning förta verkan av sistnämnda bestämmelse (p. 89 i domen).

9.3 Artikel 15.1 ska tolkas mot bakgrund av rättighetsstadgan

I artikel 15.1 i direktiv 2002/58 föreskrivs att alla åtgärder som avses i artikeln ska vara i enlighet med de allmänna principerna i unionslagstiftningen. Bland dessa ingår de allmänna principer och grundläggande rättigheter som numera garanteras i rättighetsstadgan. Nämnda artikel 15.1 ska alltså tolkas mot bakgrund av de grundläggande rättigheter som garanteras i stadgan (p. 91 i domen).

9.4 Inskränkningar i rättighetsskyddet får bara göras om åtgärden är proportionell

Enligt artikel 52.1 i rättighetsstadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara föreskriven i lag och vara förenlig med rättigheternas och friheternas väsentliga innehåll. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt intresse som erkänns av unionen eller mot

behovet av skydd för andra människors rättigheter och friheter (p. 94 i domen).

Artikel 15.1 i direktivet föreskriver att medlemsstaterna får vidta en åtgärd som avviker från principen om konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter om åtgärden ”i ett demokratiskt samhälle är nödvändig, lämplig och proportionell” för de syften som anges i den bestämmelsen. Skäl 11 i direktivet preciserar att en åtgärd av sådant slag måste stå i strikt proportion till det avsedda ändamålet. Vad särskilt gäller lagring av uppgifter kräver artikel 15.1 andra meningen i direktivet att uppgifter endast bevaras under en begränsad period och att lagringen motiveras av de skäl som fastställs i artikel 15.1 första meningen i direktivet. (p. 95 i domen)

Att proportionalitetsprincipen ska iakttas framgår även av domstolens fasta praxis, enligt vilken skyddet av den grundläggande rätten till respekt för privatlivet på unionsnivå kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt (p. 96 i domen).

9.5 De svenska reglerna utgör inskränkningar i artikel 7, 8 och 11 i rättighetsstadgan

När det gäller frågan om den svenska lagstiftningen uppfyller kraven på proportionalitet, påpekar domstolen att den svenska lagstiftningen föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel och ålägger leverantörer av elektroniska kommunikationstjänster att systematiskt och kontinuerligt lagra dessa uppgifter utan undantag (p. 97 i domen).

De uppgifter som leverantörer av elektroniska kommunikationstjänster således är skyldiga att lagra är sådana som gör det möjligt att spåra och identifiera en kommunikationskälla, identifiera slutmålet för en kommunikation, identifiera en kommunikations datum, tidpunkt, varaktighet och typ, identifiera användarnas kommunikationsutrustning och identifiera lokaliseringen av mobil kommunikationsutrustning. Bland dessa uppgifter ingår abonnentens eller den registrerade användarens namn och adress, det uppringande telefonnumret, det uppringda numret och ip-adressen för internettjänster.

Dessa uppgifter gör det möjligt att få kännedom om med vilken person en abonnent eller registrerad användare har kommunicerat och på vilket sätt, hur länge kommunikationen varat och från vilken plats kommunikationen skett. Uppgifterna gör det dessutom möjligt att få kännedom om hur ofta abonnenten eller den registrerade användaren kommunicerat med vissa personer under en viss tidsperiod. (p. 98 i domen)

Dessa uppgifter kan enligt EU-domstolen sammantagna göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i. Dessa uppgifter gör det enligt domstolen möjligt att kartlägga de berörda personerna på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationerna. (p. 99 i domen)

Det ingrepp som en sådan lagstiftning utgör i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan är enligt EU-domstolen långtgående och måste betraktas som synnerligen allvarligt. Den omständigheten att lagringen av uppgifterna och den senare användningen av dem sker utan att abonnenten eller den registrerade användaren är underrättad om detta kan enligt domstolen ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning. (p. 100 i domen)

Även om en sådan lagstiftning inte medger lagring av innehållet i en kommunikation, och därför inte kan kränka det väsentliga innehållet i dessa grundläggande rättigheter, skulle lagringen av trafikuppgifter och lokaliseringsuppgifter emellertid kunna inverka på användningen av de elektroniska kommunikationsmedlen och följaktligen på användarnas utövande av sin i artikel 11 i stadgan garanterade yttrandefrihet (p. 101 i domen).

9.6 Inskränkningarna som de svenska reglerna medför är inte proportionella

EU-domstolen konstaterar att den svenska lagstiftningen omfattar samtliga abonnenter och avser samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter, och att det inte görs några åt-

skillnader, begränsningar eller undantag utifrån det eftersträvade syftet. Domstolen konstaterar vidare att den på ett allomfattande sätt berör samtliga personer som använder elektroniska kommunikationstjänster, utan att dessa personer ens indirekt befinner sig i en situation som kan föranleda lagföring. Den är således även tillämplig på personer beträffande vilka det inte föreligger något indicium som ger anledning att tro att deras beteende ens kan ha ett indirekt eller avlägset samband med grov brottslighet. Den föreskriver inte heller några undantag, vilket innebär att den även är tillämplig på personer vilkas kommunikationer enligt nationell rätt omfattas av tystnadsplikt (p. 105 i domen).

EU-domstolen konstaterar vidare att en sådan lagstiftning inte kräver något samband mellan de uppgifter som ska lagras och ett hot mot den allmänna säkerheten. Den är inte begränsad till lagring av uppgifter avseende en viss tidsperiod eller ett visst geografiskt område eller en viss krets av personer som på något sätt kan vara inblandade i ett allvarligt brott eller till personer beträffande vilka lagringen av uppgifter av andra skäl skulle kunna bidra till bekämpningen av brott (p. 106 i domen).

EU-domstolen konkluderar att den svenska lagstiftningen överskrider gränserna för vad som är strängt nödvändigt och att den inte kan anses motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan (p. 107 i domen).

9.7 Lagringen

9.7.1 Generell och odifferentierad lagring är inte motiverad ens för att bekämpa grov brottslighet

EU-domstolen menar att – med hänsyn till det allvarliga ingrepp i de berörda grundläggande rättigheterna som en nationell lagstiftning som i brottsbekämpande syfte föreskriver lagring av trafikuppgifter och lokaliseringsuppgifter utgör – endast bekämpning av grov brottslighet kan motivera en sådan åtgärd (p. 102 i domen).

EU-domstolen bejakar i och för sig att en effektiv bekämpning av grov brottslighet, särskilt organiserad brottslighet och terrorism, i stor utsträckning kan vara beroende av användningen av moderna utredningstekniker. Fastän det syftet är av allmänt samhällsintresse

kan det enligt domstolen inte i sig ensamt motivera en nationell lagstiftning som föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter (p. 103 i domen).

9.7.2 Riktad lagring

Domstolen menar att inget hindrar att en medlemsstat antar lagstiftning som i förebyggande syfte tillåter en riktad lagring av trafikuppgifter och lokaliseringsuppgifter, i syfte att bekämpa grov brottslighet, förutsatt att lagringen av uppgifterna, vad gäller vilka slags uppgifter som ska lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske, begränsas till vad som är strängt nödvändigt (p. 108 i domen).

För att en riktad lagring ska vara förenlig med EU-rätten måste den nationella lagstiftningen enligt EU-domstolen föreskriva tydliga och precisa bestämmelser som reglerar omfattningen och tillämpligheten av en sådan lagringsåtgärd och som slår fast minimikrav, så att de personer vars uppgifter har lagrats har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk. Den måste särskilt precisera under vilka omständigheter och villkor en sådan lagringsåtgärd får vidtas i förebyggande syfte, vilket säkerställer att lagringen begränsas till vad som är strängt nödvändigt (p. 109 i domen).

Vad för det andra gäller de villkor som en nationell lagstiftning måste uppfylla för att säkerställa att den är begränsad till vad som är strängt nödvändigt, påpekar domstolen att även om villkoren kan variera utifrån vilka åtgärder som vidtas för att förebygga, undersöka, avslöja och väcka åtal för grov brottslighet, måste lagringen av uppgifterna alltid uppfylla objektiva kriterier, som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträvade syftet. I synnerhet måste villkoren vara sådana att de klart avgränsar omfattning och följaktligen den berörda personkretsen (p. 110 i domen).

Vad gäller avgränsningen av den personkrets och de situationer som kan komma att beröras av riktad lagring gör EU-domstolen följande bedömning. Den nationella lagstiftningen ska grunda sig på objektiva omständigheter som gör det möjligt att ta sikte på en personkrets vars uppgifter kan avslöja en, åtminstone indirekt, koppling till grov brottslighet och på ett eller annat sätt kan bidra till att

bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten. En sådan avgränsning kan säkerställas genom ett geografiskt kriterium genom en bedömning att det i ett eller flera geografiska områden finns en förhöjd risk för förberedelse eller genomförande av sådana handlingar (p. 111 i domen).

9.8 Tillgången

9.8.1 Endast för att bekämpa grov brottslighet

När det gäller de syften som kan motivera en nationell lagstiftning som avviker från principen om konfidentialitet vid elektronisk kommunikation anför EU-domstolen följande. Tillgång till lagrade uppgifter måste vara faktiskt och strikt begränsad till de fall då tillgången krävs för något av de syften som anges i artikel 15.1 i direktiv 2002/58. Då syftet med lagstiftningen måste stå i proportion till hur allvarligt ingrepp i de grundläggande rättigheterna det innebär att ge tillgång till de lagrade uppgifterna är det vid förebyggande, undersökning, avslöjande av och åtal för brott endast bekämpning av grov brottslighet som kan motivera en sådan tillgång. (p. 115 i domen)

Vad gäller proportionalitetsprincipen fastslår EU-domstolen att en nationell lagstiftning måste garantera att tillgång inte ges utöver vad som är strängt nödvändigt (p. 116 i domen).

9.8.2 Precisa krav måste föreskrivas

Eftersom de lagstiftningsåtgärder som avses i artikel 15.1 i direktiv 2002/58 enligt skäl 11 i direktivet ska ”omfattas av lämpliga skyddsmekanismer”, måste en sådan åtgärd, enligt EU-domstolen, dessutom föreskriva klara och precisa bestämmelser som anger under vilka omständigheter och på vilka villkor leverantörer av elektroniska kommunikationstjänster måste ge behöriga nationella myndigheter tillgång till uppgifterna (p. 117 i domen).

För att säkerställa att behöriga nationella myndigheters tillgång till lagrade uppgifter begränsas till vad som är strängt nödvändigt, ankommer det förvisso på nationell rätt att fastställa på vilka villkor leverantörer av elektroniska kommunikationstjänster ska ge sådan tillgång. Det räcker dock enligt EU-domstolen inte att den berörda

nationella lagstiftningen stadgar att tillgång enbart ska medges för något av de syften som avses i artikel 15.1 i direktiv 2002/58, även om det gäller bekämpning av grov brottslighet. Den måste även ange de materiella och formella villkoren för de behöriga nationella myndigheternas tillgång till de lagrade uppgifterna (p. 118 i domen).

9.8.3 Tillgång bara till uppgifter om personer som är inblandade i ett allvarligt brott

Eftersom en allmän tillgång till samtliga lagrade uppgifter, oberoende av om det finns någon koppling, ens indirekt, till det eftersträvade syftet, inte enligt EU-domstolen kan anses vara begränsad till vad som är strängt nödvändigt, måste den berörda nationella lagstiftningen vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till uppgifter om abonnenter eller registrerade användare. Tillgång kan enligt domstolen i princip bara beviljas, i samband med bekämpning av brott, till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. I särskilda fall, som när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism, skulle dock enligt domstolen tillgång kunna ges även till uppgifter om andra personer när det finns objektiva omständigheter som ger skäl att anta att de uppgifterna i ett konkret fall effektivt skulle kunna bidra till att bekämpa terrorism. (p. 119 i domen)

9.8.4 Förhandskontroll av domstol eller oberoende myndighet

För att säkerställa att de ovan nämnda preciserade villkoren uppfylls fullt ut, är det enligt EU-domstolen väsentligt att tillgången till de lagrade uppgifterna i princip, utom i motiverade brådskande fall, är underkastad förhandskontroll av en domstol eller en oberoende myndighet och att domstolen meddelar sitt avgörande eller myndigheten fattar sitt beslut efter det att de behöriga nationella myndigheterna framställt en motiverad ansökan (p. 120 i domen).

9.8.5 Information till de berörda

Enligt EU-domstolen krävs att de myndigheter som har beviljats tillgång till lagrade uppgifter informerar de berörda personerna om detta enligt tillämpliga nationella förfaranden så snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar. Den informationen är enligt EU-domstolen nödvändig bl.a. för att dessa personer ska kunna utöva sin rätt till rättslig prövning vid kränkning av deras rättigheter, såsom uttryckligen stadgas i artikel 15.2 i direktiv 2002/58, jämförd med artikel 22 i direktiv 95/46. (p. 121 i domen)

9.9 Skydds- och säkerhetsnivåer, lagring inom EU och utplåning

Vad gäller bestämmelserna om skydd av och säkerhet för de uppgifter som lagras av leverantörer av elektroniska kommunikationstjänster, konstaterar EU-domstolen att artikel 15.1 i direktiv 2002/58 inte medger att medlemsstaterna avviker från artikel 4.1 eller 4.1a i direktivet. De sistnämnda bestämmelserna kräver att leverantörerna vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa ett effektivt skydd av de lagrade uppgifterna mot riskerna för missbruk och otillåten tillgång till uppgifterna. Med hänsyn till att det är fråga om en stor mängd uppgifter och att dessa är av känslig natur samt att det finns en risk för otillåten tillgång till uppgifterna måste leverantörerna av elektroniska kommunikationstjänster enligt EU-domstolen garantera en särskilt hög skydds- och säkerhetsnivå genom lämpliga tekniska och organisatoriska åtgärder. Den nationella lagstiftningen måste i synnerhet föreskriva att lagringen sker inom unionen och att uppgifterna oåterkalleligen förstörs när deras lagringstid gått ut. (p. 122 i domen)

9.10 Tillsyn

Medlemsstaterna måste enligt EU-domstolen garantera att en oberoende myndighet kontrollerar att den skyddsnivå som säkerställs i unionsrätten iakttas vad gäller skyddet för fysiska personer vid behandlingen av personuppgifter. En sådan kontroll krävs uttryckligen enligt artikel 8.3 i stadgan och utgör enligt domstolens

fasta praxis en grundläggande beståndsdel i skyddet för enskilda i samband med behandlingen av personuppgifter. Annars skulle enligt domstolen de personer vars personuppgifter har lagrats berövas sin rätt enligt artikel 8.1 och 8.3 i stadgan att vända sig till de nationella tillsynsmyndigheterna med begäran om skydd för sina personuppgifter. (p. 123 i domen)

9.11 EU-domstolens slutsatser

EU-domstolen kom till följande två slutsatser.

EU-rätten utgör ett hinder för en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.

EU-rätten utgör hinder för en nationell lagstiftning som inte begränsar tillgången till trafik- och lokaliseringsuppgifter till enbart åtgärder som syftar till att bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet och inte kräver att uppgifterna ska lagras inom unionen.

Den andra frågan i det engelska målet tog EU-domstolen inte upp till prövning, eftersom ett besvarande av den frågan enligt domstolen inte skulle bidra till tolkningen av unionsrätten på ett sätt som är nödvändigt för att i unionsrättsligt avseende avgöra tvisten i det nationella målet (p. 132 i domen).

Kommissionen har uttalat att den avser att komma med någon sorts vägledning eller kommentar med anledning av Tele2-domen.

10 Målet i Kammarrätten i Stockholm

10.1 Bakgrund

Kort efter Digital Rights-domen meddelade Tele2 PTS att bolaget skulle upphöra att lagra uppgifter om elektronisk kommunikation och även radera de uppgifter som tidigare lagrats i enlighet med 6 kap. LEK.

PTS beslutade den 27 juni 2014 att förelägga Tele2 enligt 7 kap. 5 § LEK att lagra uppgifter i enlighet med 6 kap. 16 a § LEK jämte 37–43 §§ FEK. Tele2 överklagade föreläggandet till Förvaltningsrätten i Stockholm (mål nr 14891-14).

10.2 Målet i förvaltningsrätten

Tele2 yrkade att förvaltningsrätten skulle upphäva föreläggandet. Till stöd för sin talan anförde bolaget i huvudsak följande. De svenska datalagringsbestämmelserna i 6 kap. LEK står i strid med Europakonventionen och därmed också svensk grundlag. De svenska bestämmelserna lever inte upp till de krav på grundläggande fri- och rättigheter som EU-domstolen angett följer av Europakonventionen. De svenska datalagringskraven är så omfattande och långtgående att de rimligen inte kan vägas upp av regler som begränsar tillgången till de lagrade uppgifterna.

PTS motsatte sig överklagandet och anförde i huvudsak följande. Digital Rights-domen innebär inte per automatik att den svenska lagstiftningen blir ogiltig. EU-domstolen har inte funnit att datalagring i syfte att ge nationella myndigheter tillgång till uppgifterna i sig är otillåten. I likhet med de slutsatser som redovisats i Ds 2014:23

har PTS funnit att det saknas skäl att underlåta att tillämpa de svenska reglerna om lagring.

Förvaltningsrätten avslog överklagandet den 13 oktober 2014. I sina skäl fastslog domstolen inledningsvis att EU:s rättighetsstadga är tillämplig, att de svenska reglerna innebär ett intrång i rättigheterna enligt stadgan och att inskränkningarna i rättigheterna som följer av den svenska lagstiftningen är betydande. Förvaltningsrätten konstaterade att de svenska reglerna tillkommit i syfte att bekämpa brott och skydda enskildas integritet, vilket är godtagbara ändamål enligt RF, Europakonventionen, rättighetsstadgan och direktiv 2002/58. Enligt domstolen var den svenska datalagringsskyldigheten mycket omfattande men mot bakgrund av att man inte på förväg kan veta vilka personer som kommer att bli inblandade i allvarliga brott eller på vilka platser brotten kommer att begås, skulle en begränsning av omfattningen äventyra syftet med lagringen. Detsamma gäller vid en eventuell begränsning till vissa kommunikationsslag, enligt domstolen. Följaktligen konstaterade förvaltningsrätten att bestämmelserna om lagring i sig inte kunde anses gå utöver vad som var nödvändigt för att uppnå det eftersträvade syftet. Förvaltningsrätten gjorde därefter en proportionalitetsprövning av tillgångsbestämmelserna, lagringstiden och bestämmelserna om säkerhet för de lagrade uppgifterna. En av de slutsatser som förvaltningsrätten kom fram till var att delar av den kritik som EU-domstolen riktat mot direktiv 2006/24 i Digital Rights-domen även kan riktas mot svensk lagstiftning, i synnerhet vad gäller omfattningen av lagringsskyldigheten. Vidare fanns det, enligt domstolen, en del svagheter i de svenska bestämmelserna om tillgång till uppgifterna och säkerhetsåtgärder. Domstolen påpekade bl.a. att det inte fanns någon begränsning till allvarliga brott vid inhämtning av abonnemangsuppgifter, att flera myndigheter själva kunde inhämta uppgifter, utan förhandsprövning av domstol, och att det saknades reglering om i vilket land uppgifterna får lagras. Vid en sammantagen bedömning ansåg förvaltningsrätten emellertid att svagheterna i regleringen vägdes upp av andra faktorer och att det totala intrånget i de grundläggande rättigheterna därför kunde anses godtagbart. Förvaltningsrätten ansåg sammanfattningsvis de berörda svenska bestämmelserna vara förenliga med grundlag, EU-rätt och Europakonventionen.

10.3 Målet i kammarrätten

10.3.1 Den inledande delen av rättegången

Tele2 överklagade förvaltningsrättens dom till Kammarrätten i Stockholm (mål nr 7380-14) och vidhöll sitt yrkande om att föreläggandet skulle upphävas. PTS bestred yrkandet. Parterna anförde i huvudsak detsamma som vid förvaltningsrätten.

Kammarrätten beslutade den 29 april 2015 att inhämta ett förhandsavgörande från EU-domstolen i enlighet med artikel 267 i funktionsfördraget. Förhandsavgörandet begärdes eftersom kammarrätten ansåg att svensk lagstiftning i första hand måste prövas mot artikel 15.1 i direktiv 2002/58 och att det inte entydigt framgår av Digital Rights-domen om proportionaliteten av lagringsskyldighetens omfattning ska bedömas för sig eller om det ska göras en sammanvägd bedömning med beaktande av bestämmelserna om tillgång till de lagrade uppgifterna, lagringstiden och säkerheten för de lagrade uppgifterna.

EU-domstolen besvarade kammarrättens frågor i Tele2-domen, som meddelades den 21 december 2016. De frågor som kammarrätten ställde och innehållet i EU-domstolens dom framgår av avsnitt 9 ovan.

Dagen efter EU-domstolens dom beslutade kammarrätten, efter begäran från Tele2, att PTS beslut om föreläggande tills vidare inte skulle gälla.

10.3.2 Kammarrättens dom

Kammarrätten meddelade dom i målet den 7 mars 2017. Genom domen biföll kammarrätten överklagandet och upphävde PTS beslut att förelägga Tele2.

I avgörandet redogjorde kammarrätten särskilt för omfattningen av domstolens prövning och förtydligade att prövningen endast gällde frågan om huruvida bestämmelserna i LEK och FEK om lagring av trafikuppgifter m.m. för brottsbekämpande ändamål strider mot unionsrätten och PTS beslut om föreläggande därmed skulle upphävas. Vidare förtydligade kammarrätten att prövningen inte omfattade frågan om huruvida reglerna avseende lagring för andra ändamål, exempelvis underlag för fakturering, tillgång till lag-

rade uppgifter, lagringstid och säkerhet för de lagrade uppgifterna var förenliga med EU-rätten.

Efter en redogörelse för tillämpliga lagregler och EU-domstolens motivering, konstaterade kammarrätten att det, med hänsyn till EU-domstolens uttalanden, är klarlagt att de svenska bestämmelserna om lagring av trafikuppgifter m.m. för brottsbekämpande ändamål inte är förenliga med artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan samt att de därför strider mot unionsrätten. Vidare fastslog kammarrätten att det får till följd att bestämmelserna inte kan tillämpas och att PTS därför inte haft rätt att förelägga Tele2 att lagra uppgifter i enlighet med 6 kap. 16 a § LEK och 37–43 §§ FEK.

11 Internationell utblick

Nedan redovisas översiktligt huvuddragen i gällande rätt och pågående arbete i Danmark, Finland, Tyskland, Österrike, Belgien och Portugal. Värt att notera är att EU-domstolens dom fått till följd att många länder påbörjat en översyn av berörda lagstiftningar. Dessa översyner har dock ännu inte lett till lagstiftning i något land, varför den nedanstående redogörelsen inte beskriver lagstiftning som har anpassats efter uttalandena i Tele2-domen.

11.1 Danmark

11.1.1 Tillämpliga bestämmelser

Leverantörernas skyldighet att lagra uppgifter om elektronisk kommunikation finns i 2 kap. logningsbekendtgørelsen (988/2006).

Bestämmelser om tillgång till de lagrade uppgifterna finns i 71 kap. retsplejeloven (1267/2016).

11.1.2 Lagring

Enligt dansk lagstiftning måste alla leverantörer av elektroniska kommunikationstjänster till slutkund lagra uppgifter om telefonsamtal från fasta och mobila nätet och om sms-, ems och mms-kommunikation. Informationen som ska lagras är uppringande nummer, uppringt nummer och nummer som samtalet styrts till, namn och adress för abonnenten eller den registrerade användaren till dessa nummer, mottagandebekräftelse för meddelanden, identiteten på kommunikationsutrustningen (IMSI- och IMEI-nummer), uppgift om den eller de celler en mobiltelefon är uppkopplad mot då kommunikationen påbörjades och avslutades samt de tillhörande master-

nas exakta geografiska eller fysiska placering vid tidpunkten för kommunikationen, tidpunkt när kommunikationen påbörjades och avslutades samt tidpunkt för den första aktiveringen av anonyma tjänster (oregistrerade kontantkort).

Vid en internetsessions inledande och avslutande paket ska leverantörerna lagra uppgifter om avsändande och mottagande ip-adress, transportprotokoll, avsändande och mottagande portnummer samt tidpunkten för kommunikationen. När det gäller internetåtkomst ska det lagras tilldelat användar-id, användar-id och telefonnummer som tilldelats kommunikationen i ett allmänt tillgängligt elektroniskt kommunikationsnät, namn och adress för abonnenten eller den registrerade användaren som tilldelats ett användar-id eller telefonnummer vid tidpunkten för kommunikationen samt tidpunkt för när kommunikationen påbörjades och avslutades. Vid trådlös internetåtkomst ska dessutom lagras information om det lokala nätverkets exakta geografiska eller fysiska placering samt identiteten på kommunikationsutrustningen. Härutöver ska, vid slutbrukarens användande av leverantörens egna e-posttjänster, lagras information om avsändande och mottagande e-postadress.

Vid sådana internettelefonitjänster som leverantören själv tillhandahåller ska uppgifter motsvarande dem för internetanvändning och -åtkomst, lagras.

Informationen ska sparas i ett år.

11.1.3 Tillgång

Tillgång till lagrade trafikuppgifter kan ges för utredning av brott för vilket inte är föreskrivet lägre straff än fängelse sex år, brott mot rikets säkerhet, terroristbrott och vissa andra brott, däribland barnpornografibrott. För att tillgång ska beviljas ska det finnas klara skäl att anta (bestemte grunde til at antage) att kommunikation sker till eller från en misstänkt och åtgärden ska antas vara av avgörande betydelse för utredningen.

Tillgång till abonnemangsuppgifter och lokaliseringsdata kan ges mer generöst; det finns inga krav på brottstyp utan en prövning görs i stället utifrån om åtgärden är proportionell i det enskilda fallet.

All tillgång kräver tillstånd från domstol. Domstolen avgör vilka uppgifter som ska lämnas ut. Uppgifterna som lämnas ut får avse även andra än misstänkta, exempelvis målsäganden eller vittnen.

Samma regler för tillgång gäller oavsett om uppgifterna begärs inom en förundersökning eller i underrättelseverksamhet och om det begärs av t.ex. polismyndigheten eller av Politiets Efterretningstjeneste (danska säkerhetspolisen).

Den som varit föremål för inhämtande av uppgifter ska underrättas om det. Underrättelse får skjutas upp eller underlåtas, till exempel om den kan skada utredningen eller röja hemlig information om polisens undersökningsmetoder.

11.1.4 Skydd för de lagrade uppgifterna

Leverantörernas lagring övervakas av en oberoende tillsynsmyndighet.

11.1.5 Förändringsarbete

Danmark överväger att inkludera ytterligare information i lagringsskyldigheten, exempelvis lokaliseringsuppgifter vid internetanvändning. Samtidigt pågår en analys av Tele2- domen.

11.2 Finland

11.2.1 Tillämpliga bestämmelser

Leverantörernas lagringsskyldighet av elektroniska kommunikationsuppgifter regleras i 19 kap. informationssamhällsbalken (Tietoyhteiskuntakaari) (917/2014).

Tillgång regleras i flera delar av lagstiftningen, bl.a. i 5 kap. polislagen (872/2011) och 10 kap. tvångsmedelslagen (806/2011).

11.2.2 Lagring

Leverantörer av elektroniska kommunikationstjänster är skyldiga att lagra följande uppgifter.

För telefoni-, internettelefoni- och textmeddelandetjänster som tillhandahålls av leverantören ska det lagras uppgifter om abonnentens och den registrerade användarens namn och adress, abonnemangets identifieringsuppgifter och uppgifter med vilkas hjälp en användare av kommunikationstjänster kan identifieras samt användarens transaktioner, inklusive omstyrda samtal, kan fastställas utifrån meddelandets typ och mottagare samt tidpunkt och varaktighet för kommunikationen. Lagringsskyldigheten omfattar även obesvarade samtal.

För telefoni- och textmeddelandetjänster ska det dessutom lagras uppgifter med vilkas hjälp den kommunikationsutrustning som använts och utrustningens och abonnemangets position när transaktionen inleddes kan fastställas.

För internetaccesstjänster som tillhandahålls av leverantören ska det lagras uppgifter om abonnentens och den registrerade användarens namn och adress, abonnemangets identifieringsuppgifter och installeringsadress samt uppgifter med vilkas hjälp en användare av kommunikationstjänster och den utrustning som använts kan identifieras samt tidpunkt och varaktighet för tjänsternas användning kan fastställas. Endast de uppgifter som med beaktande av tjänstens tekniska genomförande är nödvändiga för att specificera informationen får lagras.

Uppgifter avseende telefoni- och textmeddelandetjänster ska lagras i ett år, avseende internettelefonitjänster i sex månader och avseende internetaccesstjänster i nio månader, från att transaktionen inleddes.

11.2.3 Tillgång

De brottsbekämpande myndigheterna får inhämta trafik-, lokaliserings- och abonnemangsuppgifter avseende en person som är skäligen misstänkt för eller med fog kan antas göra sig skyldig till ett brott, för vilket det föreskrivna strängaste straffet är fängelse minst fyra år, ett brott som begåtts med användning av en teleadress eller teleterminalutrustning och för vilket det föreskrivna strängaste

straffet är fängelse minst två år, samt för vissa andra brott, till exempel narkotikabrott, lockande av barn i sexuella syften, koppleri, grovt tullredovisningsbrott och förberedelse till grovt rån eller brott i terroristiskt syfte. Vid misstanke om sådant brott får även basstationstömningar göras. Endast uppgifter som gäller den förmodade brottstidpunkten får då inhämtas och bara från en basstation som finns i närheten av den förmodade brottsplatsen. Om det finns särskilda skäl får uppgifter dock inhämtas även för någon annan tid eller plats. Det är också möjligt för myndigheten att inhämta lokaliseringsuppgifter i syfte att få reda på var en misstänkt eller dömd person befinner sig, om brottet är sådant som inhämtning i övrigt kan beviljas för.

Tillgång till uppgifterna beslutas, förutom i brådskande fall, av domstol. I brådskande fall kan en anhållningsberättigad tjänsteman besluta om inhämtning eller basstationstömning till dess domstolen avgjort frågan.

Den som varit föremål för inhämtandet ska underrättas om det så snart syftet med inhämtningen har uppnåtts. Det gäller dock inte vid basstationstömningar. Underrättelse får underlåtas om det är nödvändigt för att trygga statens säkerhet eller skydda liv eller hälsa.

11.2.4 Skydd för de lagrade uppgifterna

Kommunikationsverket utövar tillsyn över efterlevnaden av bestämmelserna i informationssamhällsbalken.

11.2.5 Förändringsarbete

Finland utvärderade sin lagstiftning avseende datalagring efter Digital Rights-domen. Lagstiftningen bedömdes då förenlig med EU-rätten, med beaktande av att tillgången till de lagrade uppgifterna var begränsad. Efter Tele2-domen tillsatte parlamentet en ny utredning för att bedöma den finska lagstiftningen. Utredningen kom i sin rapport, som redovisades den 22 juni 2017, fram till att den finska lagstiftningen om lagring inte krävde några omedelbara förändringar (Rapporter och utredningar 9/2017, finska Kommunikationsministeriet).

11.3 Tyskland

11.3.1 Tillämpliga bestämmelser

Leverantörernas skyldigheter avseende lagring finns i 113a–113g §§ Telekommunikationsgesetz.

Tillgång till lagrade uppgifter regleras i kap. VIII och IX Strafprozeßordnung.

11.3.2 Lagring

Från och med juli 2017 är leverantörer av elektroniska kommunikationstjänster skyldiga att lagra abonnemangs- och trafikuppgifter i tio veckor och lokaliseringsuppgifter i fyra veckor. Lagringsskyldigheten omfattar följande trafikuppgifter.

För allmänna telekommunikationstjänster ska det lagras uppgifter om uppringande nummer, uppringt nummer och nummer som samtalet styrts till, datum och tid när kommunikationen påbörjades och avslutades samt information om tjänsten som används, om olika tjänster kan användas som en del av telefonitjänsten. För mobiltelefoni ska dessutom lagras uppgifter om internationellt prefix för numren och vid kontantkortstjänster datum och tid för första aktiveringen. För internettelefoni ska ip-adresser och användar-id för den uppringande och uppringda användaren lagras. Lagringsskyldigheten gäller även obesvarade samtal.

Motsvarande uppgifter ska lagras vid kommunikation via sms, mms eller liknande meddelande. Avseende tidsangivelser ska dessa avse när meddelandet skickades respektive togs emot.

För allmänna internettjänster ska det lagras uppgifter om användarens ip-adress och användar-id, unikt id för anslutningsterminal samt datum och tid för påbörjandet och avslutandet av internetanvändningen under den tilldelade ip-adressen.

De lokaliseringsuppgifter som ska lagras avser endast mobil telefoni och internetanvändning. Leverantörerna är skyldiga att lagra information om den radiocell som används av det uppringande och uppringda numret vid början av kommunikationen. För internetanvändning ska den radiocell som användes när internetåtkomsten påbörjades lagras. Härutöver ska leverantörerna spara information

om den geografiska positionen och huvudsakliga riktningen för strålning hänförlig till respektive radiocell.

Uppgifter hänförliga till institutioner och organisationer med särskilda sekretesskrav får däremot inte lagras. För att undvika lagring ska dessa institutioner och organisationers terminaler vara upptagna i en lista, som finns tillgänglig för automatiserad behandling.

11.3.3 Tillgång

Tillgång till de lagrade uppgifterna får endast beviljas de brottsbekämpande myndigheterna för utredning av vissa brott.

För de uppgifter som leverantörerna frivilligt lagrar, exempelvis för fakturering, krävs att utredningen avser ett av flera särskilt listade allvarliga brott (schwere Straftat), exempelvis mord, narkotikabrott, rån, utpressning, bedrägeri och skattebrott, eller ett brott som begåtts genom telekommunikation.

Tillgång till de uppgifter som leverantörerna är skyldiga att lagra kräver att utredningen avser ett särskilt allvarligt brott (Straftat von erheblicher Bedeutung), med vilket avses vissa specifika brott, däribland mord, människohandel, vissa sexualbrott, allvarligare narkotikabrott, barnpornografibrott och vissa brott mot staten.

Inhämtning kan endast ske av uppgifter hänförliga till personer som är misstänkta för brott eller till andra personer, om det finns anledning att anta att de skickar eller tar emot meddelanden som kommer från eller är avsedda för den misstänkte.

Underrättelsetjänsten kan inte beviljas tillgång till uppgifterna. Däremot är det tillåtet för leverantörerna att använda den lagrade informationen för att besvara förfrågningar om abonnemangsuppgifter från bl.a. underrättelsetjänsten.

Förutom såvitt avser abonnemangsuppgifter krävs det domstolsbeslut för all tillgång till lagrade uppgifter. Vid brådskande fall kan allmän åklagare bevilja tillgång, men bara till de uppgifter som frivilligt sparas av leverantörerna. Abonnemangsuppgifter begärs ut direkt från leverantörerna av åklagare eller polis.

Underrättelse ska lämnas till den som varit föremål för inhämtningen. Underrättelse kan emellertid underlåtas i vissa fall, till exempel om den kan äventyra en pågående utredningen eller om personen

endast i liten omfattning berördes av inhämtningen och kan antas sakna intresse av att bli underrättad.

11.3.4 Skydd för de lagrade uppgifterna

De uppgifter som omfattas av lagringsskyldigheten får endast lagras inom Tyskland.

Leverantörernas lagring övervakas av en oberoende tillsynsmyndighet.

11.3.5 Förändringsarbete

EU-domstolens dom och dess konsekvenser för tysk rätt är under analys. I sammanhanget ska nämnas att en tysk regional domstol (Oberverwaltungsgericht für das Land Nordrhein-Westfalen) den 22 juni 2017 i ett interimistiskt beslut har meddelat att reglerna om lagring av uppgifter rörande internetåtkomst inte behöver följas då de har bedömts vara oförenliga med EU-rätten (Az. 13 B 238/17).

11.4 Övriga länder

11.4.1 Österrike

Efter Digital Rights-domen upphävde den österrikiska konstitutionsdomstolen berörd datalagringslagstiftning. Någon ny lagstiftning har inte trätt i kraft men det finns däremot planer på att se över lagstiftningen i ljuset av Tele2-domen.

11.4.2 Belgien

I Belgien gäller en skyldighet för leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter för alla abonnenter och registrerade användare. Efter Digital Rights-domen anpassades lagstiftningen genom att differentierade tillgångsregler infördes. Lagringsreglerna lämnades oförändrade men man införde regler som möjliggjorde mer omfattande tillgång till lagrad data ju allvarligare brottet var.

Efter Tele2-domen utmanades denna nya lagstiftning i den nationella konstitutionsdomstolen. Något utslag har ännu inte kommit.

11.4.3 Portugal

Den portugisiska konstitutionsdomstolen har nyligen prövat om den datalagring som föreskrivs i Portugal (lagring av ip-adresser och tillhörande uppgifter om abonnent i ett år) var förenlig med den portugisiska konstitutionen. Domstolen kom fram till att så var fallet (dom 420/2017, 13 juli 2017).

12 Överväganden

12.1 EU-rätten måste beaktas

Utredningens bedömning: EU-rätten har indirekt inflytande på det brottsbekämpande området.

EU:s kompetens och befogenhet framgår av EU:s grundfördrag. Ett av dem är fördraget om den Europeiska Unionen. I nämnda fördrag framgår, enligt principen om tilldelade befogenheter, att unionen endast ska handla inom ramen för de befogenheter som medlemsstaterna har tilldelat unionen i fördragen för att nå de mål som fastställs där. Varje befogenhet som inte har tilldelats unionen i fördragen ska tillhöra medlemsstaterna (artikel 5). Dessutom framgår av fördraget att unionen ska respektera medlemsstaternas väsentliga statliga funktioner, särskilt funktioner vars syfte är att hävda territoriell integritet, upprätthålla lag och ordning och skydda den nationella säkerheten. I synnerhet ska den nationella säkerheten också i fortsättningen vara varje medlemsstats eget ansvar (artikel 4.2). Sverige har inte tilldelat EU någon generell befogenhet på det brottsbekämpande området (jfr kapitel 4, avdelning V i FEUF).

Frågan är då i vilken utsträckning som EU-rätten och Tele2-domen kan ha inflytande på nationell lagstiftning som rör just brottsbekämpning, dvs. i detta fall LEK, IHL, RB, 2007 års preventivlag och LSU. Frågan behandlas i det följande.

Direktiv 2002/58 har som syfte att säkerställa ett likvärdigt skydd för grundläggande fri- och rättigheter vid behandling av personuppgifter inom sektorn för elektronisk kommunikation samt möjliggöra fri rörlighet för dessa uppgifter inom gemenskapen (artikel 1.1). Direktivet i sig har alltså inget brottsbekämpande syfte utan har i stället till syfte att uppfylla målen om fri rörlighet på den inre marknaden. Däremot innehåller direktivet bestämmelser som under vissa

förutsättningar möjliggör nationella undantag från direktivet om det sker för brottsbekämpande ändamål. Undantagen rör, i nu relevant hänseende, konfidentialitet vid kommunikation (artikel 5), utplåning av trafikuppgifter (artikel 6) och behandling av andra lokaliseringsuppgifter än trafikuppgifter (artikel 9). EU-domstolen konstaterar i detta sammanhang att, för att undantagsbestämmelsen inte helt ska förlora sin verkan, även statens verksamhet på det brottsbekämpande området måste omfattas av direktivets tillämpningsområde (p. 73 i domen).

Av domen framgår, i linje med det nu anförda, att EU-domstolen har ansett sig ha kompetens även på området för tillgång till datalagrade uppgifter för brottsbekämpande ändamål och även för vitala intressen som nationell säkerhet och försvar (p. 65–81 och 119). Slutsatsen kan således dras att oavsett för vilket ändamål uppgifterna används så är operatörernas lagring och myndigheternas tillgång till dessa uppgifter underkastade den reglering som följer av EU-rätten.

Detta innebär att oavsett om det är fråga om brottsbekämpning som handhas av den öppna polisen, Tullverket eller Ekobrottsmyndigheten eller om det är fråga om brottsbekämpning som handhas av Säkerhetspolisen så är datalagringsfrågan underkastad samma EU-rättsliga regelverk, låt vara att EU-domstolen öppnar för något mer tillåtande nationella regler när det gäller tillgång till uppgifter inom Säkerhetspolisens verksamhetsområde (p. 119 i domen).

12.2 Abonnemangsuppgifter omfattas inte av Tele2-domen men av EU-rätten

Utredningens bedömning: Tele2-domen rör bara trafikuppgifter och lokaliseringsuppgifter men inte abonnemangsuppgifter. Behandlingen av abonnemangsuppgifter omfattas av EU-rätten.

Kammarrätten berör i sin begäran om förhandsavgörande framför allt trafikuppgifter och lokaliseringsuppgifter, men genom en hänvisning till en tidigare punkt i redogörelsen omfattar begäran även abonnemangsuppgifter[1]. EU-domstolens avgörande berör dock inte

[1] Vad begreppet abonnemangsuppgifter omfattar diskuteras i avsnitt 6.2.1. Sammanfattningsvis avses, något förenklat, uppgift om vilken abonnent eller registrerad användare

abonnemangsuppgifter utan endast trafikuppgifter och lokaliseringsuppgifter.

Att EU-domstolen inte berör abonnemangsuppgifter är naturligt eftersom de inte behandlas i de artiklar i det direktiv (direktiv 2002/58) som tolkas av domstolen. Det finns t.ex. inte någon skyldighet att förstöra abonnemangsuppgifter och de omgärdas inte heller av någon tystnadsplikt enligt direktivet. Det motsatta gäller trafikuppgifter och lokaliseringsuppgifter vid kommunikation. De ska som huvudregel utplånas eller avidentifieras när de inte längre behövs för kommunikationen, artikel 6 i direktivet, och de är skyddade av tystnadsplikt enligt bestämmelsen i artikel 5, som gäller vid kommunikation och därmed förbundna trafikuppgifter.

Som framgår av domslutet förklarar EU-domstolen hur artikel 15.1 mot bakgrund av bestämmelserna i rättighetsstadgan ska tolkas. Artikel 15.1 reglerar när undantag får göras från bl.a. bestämmelsen om konfidentialitet i artikel 5 och förstörandeskyldigheten i artikel 6. Artikeln saknar alltså relevans för behandlingen av abonnemangsuppgifter, som inte omfattas av de rättigheter och skyldigheter som medlemsstaterna enligt den tolkade bestämmelsen får begränsa. Det är därför följdriktigt att EU-domstolen bara svarar på frågan om trafikuppgifter och lokaliseringsuppgifter men inte abonnemangsuppgifter. Den svenska regleringen av lagringen och tillgången till abonnemangsuppgifter påverkas således inte ens indirekt av domen. Det behöver knappast sägas att de uttalandena av mer generellt slag om t.ex. inskränkningar i skyddet för personuppgifter däremot är relevanta även för behandlingen av abonnemangsuppgifter.

Det finns av andra skäl än Tele2-domen ändå anledning att beröra regleringen av abonnemangsuppgifter i betänkandet. För det första är det oundvikligt att inte göra det, eftersom regleringen bitvis har nära samband med bestämmelserna om trafik- och lokaliseringsuppgifter. För det andra utgör behandling av abonnemangsuppgifter ett slags personuppgiftsbehandling och omfattas således av dataskyddsregleringen inom EU-rätten (t.ex. artikel 3 i direktiv 2002/58). Därmed omfattas behandlingen också av de krav som följer av rättighetsstadgan. Det finns även anledning att beröra regleringen av abonne-

som vid varje tillfälle kan sammankopplas med en viss adress, t.ex. ett telefonnummer eller en ip-adress.

mangsuppgifter på grund av integritetsskyddet som följer av Europakonventionen.

I utredningen har det väckts frågan om inte ip-adresser ändå omfattas av domen. De argument som förts fram redovisas nedan.

Ett argument utgår från att användningen av dynamiska ip-adresser och NAT-teknik (som gör det möjligt för flera abonnenter att använda samma publika ip-adress) har ökat. För att kunna veta vem som använt en ip-adress vid ett specifikt tillfälle kan det därför vara nödvändigt att ha tillgång till exakta tidsuppgifter för när adressen användes. Härigenom påstås det att de uppgifter man måste behandla sammantaget kan lämna mycket exakt information om abonnenternas internetkommunikation. Enligt utredningen har detta argument inte någon större bärkraft. Det kan nämligen inte vara någon skillnad ur integritetssynpunkt mellan att kartlägga någon via en fast ip-adress eller med hjälp av t.ex. en dynamisk ip-adress, tidsloggar och portnummer; inte i något fall lagras vilka webbsidor som användaren har besökt eller annan motsvarande information. Därtill finns det ingen tidsmässig koppling mellan ip-adressen och överföringen av information. Ip-adressen kan vara fast eller tilldelas en användare i samband med internetåtkomsten. Normalt används sedan den (dynamiska) ip-adressen under en i förväg bestämd lånetid eller tills användaren kopplar ner från internet; någon direkt koppling till trafik finns därför inte.

Ytterligare ett argument för att ip-adresser skulle omfattas av domen är att domstolen i punkt 98 nämner ip-adresser (och andra abonnemangsuppgifter) i beskrivningen av vilka uppgifter som leverantörerna är skyldiga att lagra enligt svensk rätt. EU-domstolen nämner också att dessa uppgifter tillsammans med vissa uppräknade trafikuppgifter kan göra det möjligt att dra mycket precisa slutsatser om privatlivet (punkt 99). Man bör emellertid inte lägga allt för stor vikt vid att ip-adresser finns med i uppräkningen. Formuleringarna tycks vara hämtade från Digital Rights-domen (p. 26 och 27), som domstolen också hänvisar till, och utgör en allmän beskrivning av den svenska rätten. Abonnemangsuppgifter omfattades av datalagringsdirektivet och därmed också av Digital Rights-domen. När domstolen därefter (p. 102 och framåt i Tele2-domen) uttalar sig om kraven som ställs på en lagstadgad lagringsskyldighet nämns endast trafik- och lokaliseringsuppgifter. Som nämns i inledningen av detta

avsnitt är det också logiskt att EU-domstolen begränsar uttalandena till dessa uppgifter.

Ett tredje argumentet gör gällande att utredningens slutsats vilar på det felaktiga antagandet att uppgifter om abonnemang utgör en kategori uppgifter som ur ett EU-rättsligt perspektiv kan skiljas från kategorierna trafik- och lokaliseringsuppgifter. Denna invändning är enligt utredningen inte korrekt. Utredningen gör nämligen bedömningen att det även inom EU-rätten görs en distinktion mellan de olika uppgiftsslagen. T.ex. är det så att datalagringsdirektivet uttryckligen reglerade abonnemangsuppgifter, medan de relevanta artiklarna i direktiv 2002/58 inte gör det, se avsnitt 4.2.

Om ip-uppgifter (och andra abonnemangsuppgifter) skulle anses omfattas av de uttalanden som görs om trafik- och lokaliseringsuppgifter i domen skulle det innebära att domens föreskrifter om t.ex. föregående domstolsprövning vid tillgång till information om vem som använt en ip-adress eller disponerar över ett telefonnummer skulle bli tillämpliga. Även reglerna om att tillgång endast skulle kunna beredas de brottsbekämpande myndigheterna vid grova brott skulle behöva beaktas. I sådant fall skulle det krävas överväganden även i dessa delar. Som ovan angetts är det dock utredningens bedömning att inte ip-adresser (eller några andra abonnemangsuppgifter) omfattas av domen. Några sådana överväganden redovisas därför inte. I detta sammanhang ska också nämnas att Förvaltningsrätten i Stockholm den 5 maj 2017 meddelade ett inhibitionsbeslut i ett mål (nr 6895-16) om utlämning av abonnemangsuppgifter. Domstolen beslutade att ett vitesföreläggande mot en internetoperatör tills vidare inte skulle verkställas, eftersom det kunde ifrågasättas om bestämmelserna om tillgång till lagrade uppgifter om elektronisk kommunikation är förenliga med de villkor som EU-domstolen i Tele2-domen uttalat ska gälla. Det ska dock noteras att frågan om huruvida abonnemangsuppgifter omfattas av Tele2-domen och de tolkade artiklarna i direktivet alls inte berörs i beslutet. PTS, som utfärdat föreläggandet, överklagade beslutet till Kammarrätten i Stockholm, som den 9 juni 2017 beslutade att inte meddela prövningstillstånd (mål nr 3256-17).

Slutligen ska påpekas att, som framgår i avsnitt 6.2.1, även de flesta medlemsstater i den informella rådsarbetsgruppen i EU som behandlar datalagringsfrågan efter Tele2-domen preliminärt har

kommit till slutsatsen att ip-adresser är abonnemangsuppgifter, som inte omfattas av domen.

Att ip-adresser och andra abonnemangsuppgifter är en särskild uppgiftstyp som inte förtjänar samma starka skydd är även en slutsats som den portugisiska konstitutionsdomstolen har kommit till (dom 420/2017, 13 juli 2017).

12.3 Det är nödvändigt att reformera svensk lagstiftning

Utredningens bedömning: Det är nödvändigt att reformera reglerna kring datalagring för att uppfylla Sveriges internationella åtaganden.

Som kommer att framgå i det följande uppställer EU-domstolen i vissa delar strängare krav på datalagringen och tillgången till datalagrade uppgifter än vad svensk lag gör.

Ett sätt att hantera den uppkomna situationen är att helt enkelt upphäva alla bestämmelser som står i strid med EU-rätten. Enligt utredningens bedömning är emellertid en sådan lösning utesluten av både brottsbekämpande och folkrättsliga skäl. Detta utvecklas i det följande.

Som framgår av direktiven till Utredningen om hemlig dataavläsning har under senare år den ökande internationaliseringen i kombination med teknikutvecklingen och en tilltagande internetanvändning inneburit att kriminaliteten delvis har ändrat karaktär (dir. 2016:36). Internet erbjuder lättillgängliga kontaktytor för brottsplanering inom och utom landets gränser och utgör bl.a. en etablerad plattform för våldsbejakande extremism och terrorismpropaganda. Viss typ av kriminalitet, t.ex. barnpornografibrott, har internet som brottsplats och den webbaserade narkotikahandeln har ökat massivt de senaste åren, Polismyndighetens och Tullverkets rapport Drogsituationen i Sverige (2016) s. 10, som hänvisar till globaldrugsurvey.com. Utvecklingen innebär att även förutsättningarna för att förhindra brott och säkra bevis för begångna brott har förändrats radikalt. Uppgifter om elektronisk kommunikation och andra elektroniska spår är i dag helt nödvändiga för brottsbekämpningen. Det sagda belyser att om de brottsbekämpande myndigheterna inte skulle

ha tillgång till adekvata utredningsverktyg i den elektroniska miljön så skulle brotten i vissa fall vara omöjliga att klara upp och brottsoffer i motsvarande omfattning vara skyddslösa. En sådan situation är högst problematisk ur ett brottsbekämpande perspektiv. Vissa brott skulle i praktiken kunna bli straffria och många målsägande skulle aldrig kunna få upprättelse.

Utöver detta brottsbekämpande perspektiv måste hänsyn tas till Sveriges internationella åtaganden. Var och en som vistas i Sverige har rätt att göra anspråk på att staten vidtar effektiva åtgärder för att skydda hans eller hennes säkerhet. I detta ligger att staten måste anstränga sig för att se till att brott förebyggs, utreds och att gärningsmän ställs till svars för sina brottsliga handlingar. Staten har alltså en skyldighet att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda och, om intrång görs, se till att brotten utreds (avsnitt 3.1.2–3.1.3). Enligt utredningen skulle det inte vara förenligt med Sveriges åtaganden att inte ge de brottsbekämpande myndigheterna möjlighet att effektivt utreda brott i den elektroniska miljön.

Utöver det generella ansvar Sverige har att upprätthålla en effektiv brottsbekämpning har Sverige gjort specifika åtaganden för vissa typer av brott. Här kan nämnas plikten att bekämpa tillhandahållande, spridning och innehav av barnpornografi enligt artikel 20 i Europarådets konvention om skydd för barn mot sexuell exploatering och sexuella övergrepp. Enligt konventionen har Sverige ett åtagande att vidta nödvändiga lagstiftningsåtgärder för att säkerställa effektiv utredning och åtal av sådana gärningar och tillåta möjligheten, där så är lämpligt, att genomföra hemliga utredningsåtgärder. Denna typ av brottslighet pågår i stor utsträckning på den elektroniska arenan. Utan möjligheter till effektiva utredningsverktyg skulle Sverige inte uppfylla sina folkrättsliga åtaganden enligt den nämnda konventionen.

Härtill kommer proportionalitets- och behovsargumenten. Om de brottsbekämpande myndigheterna fråntas möjligheten att komma åt trafikuppgifter i brottsutredningar måste de kompensera sig med andra metoder. Ett exempel på det skulle kunna vara följande. Anta att en person misstänks för ett brott utfört på en viss plats och att lokaliseringsuppgifter skulle kunna binda honom till den aktuella platsen (eller ge honom alibi). Om polis och åklagare inte skulle ges möjlighet att komma åt dessa uppgifter kan de, i enlighet med det

ovan anförda, inte lägga ned förundersökningen utan måste i stället arbeta vidare med de metoder som står till buds. En sådan metod är t.ex. hemlig avlyssning av elektronisk kommunikation. Det sagda innebär alltså att frånvaron av möjlighet att inhämta trafikuppgifter kan leda till ett ännu allvarligare integritetsintrång (avlyssning) för den enskilde – att jämföra med det minskade integritetsintrånget för dem som inte får sina uppgifter lagrade. En sådan ordning skulle för den enskilde rimma illa med proportionalitets- och behovsprinciperna, vilka utvecklats i praxis för all tvångsmedelsanvändning. Proportionalitetsprincipen innebär att en tvångsåtgärd i fråga om art, styrka, räckvidd och varaktighet ska stå i rimlig proportion till vad som står att vinna med åtgärden. Behovsprincipen innebär att en myndighet får använda ett tvångsmedel bara när det föreligger ett påtagligt behov och en mindre ingripande åtgärd inte är tillräcklig för att tillgodose behovet.

Den svenska lagstiftningen måste således anpassas till vad rättighetsstadgan kräver såvitt avser skyddet mot statens ingrepp i den personliga integriteten samtidigt som den måste tillgodose de skyldigheter Sverige har enligt bl.a. Europakonventionen att ge de brottsbekämpande myndigheterna effektiva verktyg och på så sätt upprätthålla effektiviteten i brottsbekämpningen och därigenom skydda den enskilda mot övergrepp från andra. Hur detta kan göras utvecklas mer i det följande.

12.4 Ingen generell och odifferentierad lagring som i dag

Utredningens bedömning: Lagring kan endast motiveras av intresset att bekämpa grov brottslighet, men inte ens detta ändamål kan ensamt motivera en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.

Det finns ett fortsatt utrymme för en begränsad lagringsskyldighet. Men lagringsskyldigheten måste göras mindre omfattande än i dag och anpassas till vad som är strängt nödvändigt.

12.4.1 Uppgifterna får endast lagras för att bekämpa grov brottslighet

EU-domstolen konstaterar att endast intresset att bekämpa grov brottslighet kan motivera en lagringsskyldighet av trafikuppgifter och lokaliseringsuppgifter. Det kan emellertid inte ensamt motivera en generell och odifferentierad lagring av samtliga sådana uppgifter.[2] (avsnitt 9.7.1 ovan och p. 102 och 103 i domen)

Hur den nationella lagstiftningen, utifrån ett brottsbekämpande syfte, motiverar ett krav på lagring visar sig uteslutande genom en analys av för vilka brott som de brottsbekämpande myndigheterna tillåts få tillgång till de lagrade uppgifterna. I denna del hänvisas därför till resonemangen nedan om tillgången till uppgifterna, avsnitt 12.8.1.

12.4.2 Utrymme finns för en fortsatt lagringsskyldighet

När det gäller lagringens omfattning fastslår EU-domstolen att rättighetsstadgan utgör hinder för en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel (p. 1 i domslutet). Eftersom det är så som EU-domstolen beskrivit den svenska lagstiftningen (p. 97 och 105 i domen) är det således uteslutet att lämna de svenska lagringsreglerna oförändrade, i vart fall om de endast kan motiveras utifrån bekämpning av grov brottslighet.

Även om domslutet endast förbjuder en allomfattande lagring framgår det av domskälen att utrymmet för att över huvud taget föreskriva lagring är begränsat. Frågan är då hur begränsat detta utrymme är. EU-domstolen delar upp sitt resonemang i denna fråga i två delar.

Den första delen av resonemanget återfinns i punkt 97–107 och handlar om generell lagring. EU-domstolen resonerar här kring den svenska lagstiftningen om datalagring och konstaterar att den föreskriver en generell och odifferentierad lagring av samtliga trafik-

[2] "general and indiscriminate retention of all traffic and location data" i den engelska versionen och "la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation" i den franska.

uppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel och ålägger leverantörer av elektroniska kommunikationstjänster att systematiskt och kontinuerligt lagra dessa uppgifter, utan undantag (p. 97). Därefter konstaterar EU-domstolen att denna mängd av uppgifter gör det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats (p. 99). EU-domstolens slutsats är att en sådan lagstiftning utgör ingrepp i de rättigheter som följer av stadgan (p. 100) och att därför endast grov brottslighet kan motivera lagring (p. 102). Dock kan inte ens grov brottslighet i sig ensamt motivera en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter (p. 103). Vid beskrivningen av den svenska lagstiftningen konstaterar domstolen att lagringen på ett allomfattande sätt berör samtliga personer som använder elektroniska kommunikationstjänster, utan att dessa personer ens indirekt befinner sig i en situation som kan föranleda lagföring (p. 105) och att lagringen inte är begränsad till tid, geografiskt område eller krets av personer (p. 106). Domstolens slutsats, som avslutar det första ledet av resonemanget, är att den svenska lagringen överskrider gränsen för vad som är strängt nödvändigt och därför står i strid med artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan (p. 107). Denna slutsats är också den som återfinns i domslutet (p. 1 i domslutet och p. 112 i domskälen). Denna del av resonemanget är alltså den nödvändiga delen av domskälen för att komma fram till domslutet. EU-domstolen skulle följaktligen ha kunnat sluta sitt resonemang här eftersom den redan har underkänt den svenska lagstiftningen och besvarat frågan från kammarrätten.

Domstolen fortsätter emellertid sina överväganden i en andra del av resonemanget. Denna del, som återfinns i punkterna 108–111, har ingen koppling till domslutet utan är närmast att se som ett *obiter dictum* (dvs. ett uttalande vid sidan om själva saken) och ett exempel på en möjlig form av lagringsskyldighet. Resonemanget här handlar om riktad lagring (jfr avsnitt 12.5.1) och i dessa punkter resonerar domstolen kring hur en sådan lagring skulle kunna vara utformad. Det föreskrivs här att riktad lagring, vad gäller vilka slags uppgifter som ska lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske, måste begränsas till vad som är strängt nödvändigt (p. 108). Bland kraven på en riktad

lagring märks särskilt att den berörda personkretsen måste vara avgränsad (p. 110).

Det har under utredningen framförts uppfattningen att endast en riktad lagring skulle vara förenlig med EU-rätten så som den har uttolkats i Tele2-domen. Det har då hänvisats just till EU-domstolens ovan angivna skrivningar om att villkoren för den nationella lagringen måste vara sådana att de klart avgränsar åtgärdens omfattning och följaktligen den berörda personkretsen (p. 110) samt att domstolen särskilt uttalar att stadgan inte hindrar en riktad lagring (p. 108). Som framgår ovan är emellertid utredningens slutsats att domstolens uttalande om riktad lagring endast är ett exempel och ett *obiter dictum*. Uttalandena i p. 110 om avgränsning av den berörda personkretsen tar sikte just på denna riktade lagring och således inte generellt på hur nationell lagstiftning om lagring ska vara utformad.

Förespråkarna av riktad lagring som den enda möjliga modellen har också hänvisat till att EU-domstolen i sin dom särskilt noterar att lagringsskyldigheten i Sverige även är tillämplig på personer där det inte föreligger något indicium som ger anledning att tro att deras beteenden ens kan ha ett indirekt eller avlägset samband med grov brottslighet (p. 105). Att tolka detta uttalande som att det skulle förbjuda en lagring också av andra än dem som räknas upp i nämnda punkt i domen förefaller långsökt. Om det skulle ha varit EU-domstolens avsikt att förbjuda sådan lagring hade det varit naturligare att utforma domslutet och skälen så att det tydliggjordes. Som antecknas nedan kan det dessutom noteras att EU-domstolen efter Tele2-domen i en näraliggande fråga har accepterat att lagring, i brottsbekämpande syfte, av flygbolags passageraruppgifter omfattar samtliga flygpassagerare och således inte är riktad till sådana passagerare om vilka de förelåg någon misstanke att de kunde hota den allmänna säkerheten (EU-domstolens yttrande 1/15, den 26 juli 2017 p. 41, 186 och 189). Man kan därutöver notera att en generell lagring i fem år förskrivs för vissa närmare angivna uppgifter enligt fjärde penningtvättsdirektivet[3]. Det förefaller inte heller som en rimlig tolkning att EU-domstolen på ett så ingripande sätt skulle ha

[3] Europaparlamentets och rådets direktiv (EU) 2015/849 av den 20 maj 2015 om åtgärder för att förhindra att det finansiella systemet används för penningtvätt eller finansiering av terrorism, om ändring av Europaparlamentets och rådets förordning (EU) nr 648/2012 och om upphävande av Europaparlamentets och rådets direktiv 2005/60/EG och kommissionens direktiv 2006/70/EG.

haft för avsikt att beröva de brottsbekämpande myndigheterna möjligheten till en effektiv brottsbekämpning utan ingående resonemang och överväganden i dessa delar.

Innebörden av domstolens sätt att resonera är uppenbarligen att den svenska lagringen inte är förenlig med stadgan. Vid sitt konstaterande av det betonar domstolen i flera punkter att det är just den allomfattande generella svenska lagringen som underkänns. I punkt 103 uttalar sig domstolen om en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter. Punkt 104 hänvisar till den svenska lagstiftning med de särdrag som beskrivits i punkt 97, dvs. en lagstiftning som föreskriver en systematisk, kontinuerlig, generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel utan undantag. Även resonemanget i punkt 105 avser en allomfattande lagringsskyldighet, närmare definierad som en lagstiftning som på ett generellt sätt omfattar samtliga abonnenter och registrerade användare och avser samtliga kommunikationsmedel och samtliga trafikuppgifter, utan åtskillnader, begränsningar eller undantag. Det stämmer också väl överens med EU-domstolens dom den 6 oktober 2015 i målet Schrems, C-362/14, punkt 93.

Det går inte av domen att utläsa hur en mindre omfattande men ändå i någon mening generell lagringsskyldighet skulle ha bedömts. Vad EU-domstolen antecknar om den riktade lagringen är som ovan konstaterats ett *obiter dictum* som beskriver hur en (mer tillåtande) riktad lagring skulle kunna utformas. Den delen av resonemanget ger ingen avgörande ledning i bedömningen av hur en sorts generell lagring ska vara utformad för att möta kraven i rättighetsstadgan.

Vidare är det inte självklart vad som avses med ”samtliga trafikuppgifter och lokaliseringsuppgifter”. Uttrycket verkar kunna härledas från kammarrättens fråga (punkt 51 i domen). Det kan emellertid noteras att det är flera trafik- och lokaliseringsuppgifter som inte ska lagras enligt den svenska lagstiftningen, t.ex. position när ett meddelande skickades och när det mottogs, position under ett mobilsamtal, position vid fast telefoni, utrustningsidentitet vid skickade och mottagna meddelanden, utrustningsidentitet vid fast telefoni, abonnemangsidentitet vid skickade och mottagna meddelanden, abonnemangsidentitet vid internetåtkomst, samtliga uppgifter om samtal med annat än vanligt telefonnummer, t.ex. med

användarnamn, (däribland uppringande och uppringt nummer, tid och position), uppgift om port och publik ip-adress vid internetåtkomst[4], meddelandehantering och ip-telefoni samt samtliga uppgifter om samtal som inte kopplas fram på grund av tekniskt fel eller dylikt (däribland uppringande och uppringt nummer eller användarnamn, tid, utrustning och position). Därtill ska det inte lagras några rena lokaliseringsuppgifter, dvs. positioner som inte är kopplade till kommunikation. Det finns också en hel del trafikuppgifter av mer tekniskt slag som inte omfattas av lagringsskyldigheten. Sådana uppgifter kan bl.a. avse peeringpunkter och kommunikationskoder (t.ex. ortogonala spridningskoder). Det är således långt ifrån samtliga trafik- och lokaliseringsuppgifter som omfattas av lagringsskyldigheten.

Även om det inte får någon bäring på vad som utgör samtliga trafik- och lokaliseringsuppgifter, enligt definitionerna i direktiv 2002/58, kan det dessutom noteras att kommunikationen på senare tid alltmer har övergått till en typ som inte ger upphov till någon lagringsskyldighet hos operatörerna (avsnitt 7.3.1), dvs. sådana tjänster som inte tillhandahålls av en lagringsskyldig operatör utan andra tjänsteleverantörer, exempelvis Apple Imessage och Facetime, Facebook Messenger, Skype, Gmail och Hotmail. Lagringsskyldigheten omfattar inte heller t.ex. webbplatsbesök (surfning), sökningar med sökmotorer, onlinespel eller uppgifter om filöverföring med hjälp av File Transfer Protocol (FTP).

Även om en rimlig utgångspunkt måste vara att EU-domstolen ansett att den svenska lagstiftningen, såsom den beskrivits i punkterna 15–19 i domen, föreskriver en alltför omfattande lagringsskyldighet, måste domstolens slutsats tolkas i ljuset av hur kammarrätten ställt sina frågor och utvecklingen av alternativa kommunikationstjänster i tiden därefter. Betydelsen av den ökade användningen av sådana alternativa kommunikationstjänster noteras även i den finska utredningen som nämns ovan (avsnitt 11.2.5). I den utredningen görs även bedömningen att den finska och svenska lagringsskyldigheten är tämligen likartade, men att den finska är mer riktad och alltså förenlig med EU-rätten.

Det sagda leder till tre slutsatser: För det första får det inte föreskrivas en generell och odifferentierad lagring av samtliga trafik-

[4] Enligt PTS bedömning, se PTS skrivelse till EBM den 26 februari 2015, dnr 15-1185.

uppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel. För det andra måste det svenska regelverket för lagring, oaktat att det inte föreskriver en sådan lagring, göras mindre omfattande. För det tredje kan det införas ett system med riktad lagring som tillåter en omfattande lagring men som är begränsad till tid, plats eller person. Även andra former av datalagring kan införas, så länge skyldigheten att lagra inte blir huvudregel och den begränsas i varje del till vad som är strängt nödvändigt.

Enligt utredningens bedömning är nyttan av uppgifterna från elektronisk kommunikation så stor för de brottsbekämpande myndigheterna att det finns skäl att behålla någon sorts lagring i preventivt syfte – dock mindre omfattande än i dag. Det torde däremot inte vara tillräckligt att endast differentiera lagringstiderna, eftersom det inte får någon påverkan på huruvida lagring blir undantag eller huvudregel (jfr punkt 104 i domen).

12.5 Olika modeller för lagring

Utredningens bedömning: En viss begränsad och differentierad lagring bör föreskrivas.

12.5.1 Ingen riktad lagring

Som nämnts ovan tillåter EU-rätten en riktad lagring. Riktad lagring innebär en situationsanpassad preventiv lagring av uppgifter hänförliga till vissa nummer, kommunikationsutrustningar eller platser. Lagringen kan vara tidsbegränsad. Frågan är om en sådan bör införas i Sverige. Vid bedömningen av denna fråga måste å ena sidan nyttan och behovet av en sådan vägas mot intrånget för de berörda personerna.

När det gäller den första frågan (nytta och behov) kan noteras att det är komplicerat att i förväg veta hur man ska rikta lagringen. Det är nämligen mycket svårt att i förväg veta när, var eller av vem ett allvarligt brott ska begås. Det är således vanskligt att på något meningsfullt sätt rikta lagringen till vissa tider, områden eller personer. Utredningen kan därför inte se någon större praktisk nytta eller

något större behov av en möjlighet till riktad lagring. Inte heller utredningens experter från de brottsbekämpande myndigheterna har sett något större värde med en sådan lagring.

När det gäller den andra frågan (intrånget för de berörda personerna) kan det noteras att all lagring innebär ett integritetsintrång. Att rikta lagringen till en viss person eller krets av personer (exempelvis i ett visst område eller personer med visst kön), utan att det finns någon konkret misstanke mot dessa personer, innebär rimligen en än större rättighetskränkning mot dessa människor. De brottsbekämpande myndigheterna måste nämligen vid sådan lagring peka ut vissa personer eller personkategorier som mer brottsbenägna än andra så att lagring av just deras uppgifter ska utföras. Därtill innebär en sådan riktad lagring att förutsättningarna för att lösa allvarlig brottslighet blir olika för olika delar av landet, vilket är problematiskt. I vissa fall kan det dock vara så att brottsrisken ökar i ett visst område vid speciella händelser, t.ex. vid ett statsbesök i Stockholms innerstad. I sådana fall skulle man kunna tänka sig en riktad lagring mot dessa delar av staden utan att kränka någons rättigheter ur den nu redovisade synvinkeln. Dock är värdet av en sådan lagring mycket lågt. Både underrättelseverksamheten och – i värsta fall – förundersökningsverksamheten avseende sådan brottslighet måste rikta sig mot betydligt större områden än själva attentatsplatsen. Planering och kontakter mellan gärningsmän sker nämligen med största säkerhet inte enbart på själva brottsplatsen och inte sällan under en längre tid.

Det ovan anförda ger vid handen att riktad lagring skulle vara av ringa nytta för de brottsbekämpande myndigheterna samtidigt som integritetsintrånget för de berörda personerna skulle vara påtagligt.

Utöver den nu redovisade bristande proportionaliteten, är riktad lagring förknippad med ett annat problem. Om man ska rikta lagringen mot vissa tider eller områden så måste operatörerna underrättas om detta beslut så att rätt uppgifter kan lagras. Antalet operatörer överstiger 500 stycken. Även om antalet mobiloperatörer, som mest torde beröras av en riktad lagring, är väsentligt färre och vissa stora operatörer står för en mycket stor marknadsandel, så riskerar en underrättelse att behöva gå till många operatörer. Det skulle bli utmanande rent expeditionsmässigt samtidigt som uppgiften om att ett visst område är av intresse för den brottsbekämpande verksamheten skulle spridas till en alltför stor krets av personer. Detta pro-

blem är särskilt betonat i underrättelseverksamheten där sekretesskraven gör sig gällande med särskilt stor kraft.

Det ska i sammanhanget även nämnas att den av Sverige undertecknade (men ännu inte ratificerade) it-brottskonventionen[5] innehåller en bestämmelse om s.k. skyndsamt bevarande (artikel 16). Enligt den bestämmelsen ska varje part till konventionen vidta nödvändiga lagstiftningsåtgärder för att dess behöriga myndigheter genom förelägganden eller på liknande sätt ska kunna åstadkomma skyndsamt säkrande av särskilt angivna datorbehandlingsbara uppgifter, innefattande trafikuppgifter, som har lagrats med hjälp av ett datorsystem, särskilt i de fall där det finns anledning att förmoda att de datorbehandlingsbara uppgifterna löper särskild risk att gå förlorade eller förändras. För det fall misstankar riktas mot en viss person kan således en sorts riktad lagring komma till stånd genom ett föreläggande om bevarande i enlighet med reglerna i it-brottskonventionen (SOU 2013:39, som bereds i Regeringskansliet).

Sammantaget leder det nu anförda till slutsatsen att riktad lagring varken framstår som proportionell eller lämplig. Utredningen lämnar därför inget förslag på riktad lagring. Det kan för övrigt noteras att slutsatsen om brist på nytta av riktad lagring överensstämmer med analysen i departementspromemorian Ds 2014:23 s. 53 (se avsnitt 8.3.1).

12.5.2 Inget bevarandeföreläggande av uppgifter som operatörerna behöver för egna ändamål

I stället för att förordna att operatörerna ska lagra vissa uppgifter viss tid, skulle ett möjligt alternativ vara att ge myndigheterna behörighet att förelägga operatörerna att bevara de uppgifter som redan finns sparade (även kallat *quick freeze*). Som framgår ovan följer en sådan skyldighet av it-brottskonventionen, enligt vilken även innehållet i kommunikationen ska kunna bevaras. Liknande lagstiftning återfinns också i flera andra länder.

Den uppenbara fördelen och nackdelen med ett sådant bevarande är att lagringen blir begränsad. Det kan bli lägre kostnader för operatörerna och färre personers uppgifter omfattas i jämförelse med en

[5] Europarådets konvention om it-relaterad brottslighet (ETS 185).

ständigt pågående lagring av uppgifter. Däremot blir integritetsintrånget för de personer vars uppgifter ändå lagras lika stort som vid ett generellt lagringskrav. Ett sådant bevarandesystem kan vid en första anblick därför framstå som mer proportionerligt än ett som innebär generell lagring. Det är emellertid inte självklart, eftersom proportionaliteten måste bedömas utifrån nyttan av åtgärden. Det är nämligen inte givet att ett bevarandeföreläggande kommer att ge tillräckliga resultat för brottsbekämpningen i jämförelse med annan typ av lagring.

För att ett bevarandeföreläggande ska bli meningsfullt krävs det att det finns uppgifter att bevara. Eftersom direktiv 2002/58 föreskriver en skyldighet för operatörerna att förstöra uppgifterna när de inte längre behövs för vissa egna ändamål finns det en överhängande risk att utbudet av uppgifter bli alltför begränsat. Utbudet av uppgifterna blir också varierande, beroende på hur varje operatör använder uppgifterna.

Inför förslaget till datalagringsdirektivet övervägde Kommissionen en reglering med endast en riktad bevarandeskyldighet. En sådan reglering bedömdes inte i tillräcklig grad kunna bidra till bekämpningen av organiserad brottslighet och terrorism, eftersom den i princip inte ger tillgång till historiska uppgifter och den kräver att det redan finns en misstänkt eller en krets av misstänkta (Kommissionens arbetsdokument ”Commission Staff Working Document”, som lades fram som bilaga till det förslag till direktiv som ledde fram till antagandet av datalagringsdirektivet, den 21 september 2005).

Kommissionens argument är riktigt för den typ av riktad lagring som beskrivits i avsnittet ovan. Ett bevarandeföreläggande skulle emellertid kunna användas även i andra situationer, som exempel skulle alla uppgifter kopplade till en mordplats eller mördad person kunna bevaras under viss tid. Nyttan av det förefaller dock vara begränsad; om utredarna vet vilka uppgifter som är intressanta är det mer logiskt att inhämta dem i stället för att förelägga operatören att bevara dem. Värdet blir något större om man skulle förelägga operatörerna att lagra alla tillgängliga uppgifter hänförliga till de kommunikationsutrustningar som befunnit sig i närheten av mordplatsen eller kontaktat offret strax före mordet. På så sätt skulle t.ex. trafikuppgifter som man inte förrän senare i utredningen vet att de är intressanta finnas bevarade, dock bara avseende en kortare tid före gärningen på grund av förstörandeskyldigheten.

Sammanfattningsvis framstår nyttan av en bevarandeskyldighet av detta slag som tydligt begränsad i jämförelse med en lagringsskyldighet som går utöver vad operatörerna behöver bevara för egna ändamål. Något förslag på bevarandeföreläggande lämnas därför inte av utredningen. En bevarandeskyldighet som den som föreskrivs i itbrottskonventionen, som även omfattar innehåll, kan däremot utgöra ett komplement till en mer generell lagringsskyldighet. Som nämnts ovan bereds denna fråga redan i Regeringskansliet.

12.5.3 Ingen lagring av senaste aktiviteten på abonnemanget

Ytterligare en alternativ lagringsform är att föreskriva att ett abonnemangs senaste aktiviteter ska sparas i viss tid, t.ex. ett år. Många gärningsmän vid grova brott gör sig av med eller slutar att använda sin mobiltelefon eller sitt sim-kort efter att den brottsliga aktiviteten begåtts. Telefoner utan aktivitet kommer då att ha t.ex. de två senaste månadernas trafik- och lokaliseringsuppgifter sparade en längre tid. Uppgifter från ett aktivt abonnemang kommer däremot aldrig att vara äldre än två månader, eftersom de hela tiden ersätts av senare uppgifter. Modellen blir i praktiken en automatisk *quick freeze* kombinerad med en mycket kort generell lagringsskyldighet. Fördelen med denna modell är att färre uppgifter lagras. Den största nackdelen är att utbudet av historiska uppgifter blir väldigt begränsat men även att modellen inte begränsar antalet personer som omfattas av lagringsskyldigheten utan endast differentierar tiden för lagring. Även om det finns undantag, uppmärksammas som regel grova brott närmast direkt efter att de begåtts och relevant inhämtning har antagligen då redan gjorts i nära anslutning till gärningen. Den enda nyttan som i så fall skulle bli följden av ett bevarande av senaste aktivitet är dels om telefonen använts i samband med brottet på en annan plats än vid gärningsplatsen och blivit intressant först senare i utredningen, dels om en inhämtning görs en tid efter gärningen i syfte att se vilka av de abonnemang som var uppkopplade vid gärningstillfället som därefter slutade användas. Det är dessutom långt ifrån alla kriminella som frekvent byter abonnemang. I synnerhet i underrättelseverksamheten kan också t.ex. vardagsmönster behöva kartläggas, varför även uppgifter från telefoner som inte använts vid brottslig verksamhet kan vara till stor nytta för brottsbekämpningen.

Sammanfattningsvis blir nyttan begränsad och skillnaden i integritetsintrång i jämförelse med nuvarande lagstiftning inte betydande. Något förslag på en skyldighet att endast lagra senaste aktivitet lämnas därför inte av utredningen.

12.5.4 Ingen bibehållen lagring med kryptering

Ett ytterligare alternativ är att bibehålla dagens omfattning på lagringen och i stället föreskriva krav på kryptering. Det skulle innebära att uppgifterna omedelbart vid lagring skulle krypteras och att de skulle avkrypteras först när det finns ett beslut om tillgång till uppgifterna för de brottsbekämpande myndigheterna. Härigenom skulle de lagrade personuppgifterna få ett skydd som skulle öka de berörda personernas integritetsskydd.

Frågan är om en sådan ordning skulle leva upp till domstolens krav i Tele2-domen.

Vid denna bedömning måste beaktas att kammarrätten i sin begäran om förhandsavgörande ställde just frågan om en generell och odifferentierad lagring kan vara tillåten om kraven på säkerhet för uppgifterna är utformade så som de är i Sverige, dvs. med bl.a. föreskrifter om tystnadsplikt, tillsyn och – viktigast i detta sammanhang – krav på tekniska och organisatoriska åtgärder för att skydda uppgifterna (p. 38–43 i begäran om förhandsavgörande). Härtill nämner kammarrätten kraven i 37 § FEK om att den lagringsskyldige ska vidta de åtgärder som krävs för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring och att sådana åtgärder även ska vidtas för att förhindra otillåten lagring, behandling av eller tillgång till och otillåtet avslöjande av uppgifterna (p. 40 i domen).

EU-domstolen konstaterar att direktiv 2002/58 inte medger att medlemsstaterna avviker från bestämmelserna i direktivet som kräver att leverantörerna vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa ett effektivt skydd av de lagrade uppgifterna mot riskerna för missbruk och otillåten tillgång till uppgifterna (p. 122). EU-domstolen besvarar kammarrättens fråga i denna del utan samband med kammarrättens första fråga, dvs. om en generell och odifferentierad lagring över huvud taget är tillåten (p. 122 i domskälen och p. 2 i domslutet).

Av det ovan nämnda framgår alltså att EU-domstolen har förutsatt att det finns nationella krav på tekniska och organisatoriska åtgärder som skyddar uppgifterna och att detta skydd inte påverkar tillåtligheten av en generell och odifferentierad lagring. Slutsatsen blir således att tillåtligheten av den svenska nuvarande lagringen inte skulle påverkas genom införandet av föreskrifter om kryptering.

Ett annat sätt att öka integritetsskyddet är att maskera de lagrade uppgifterna. Det har föreslagits att maskering ska användas vid lagring av flygpassageraruppgifter, för att uppfylla Sveriges åtaganden enligt PNR-direktivet (SOU 2017:57 och artikel 12.2 i PNR-direktivet). Efter sex månader ska PNR-uppgifterna (uppgifter om flygresenärer) i databasen maskeras, vilket innebär att tillgängliga uppgifter som direkt kan hänföras till en fysisk person ska göras osynliga för en användare som saknar särskild behörighet för tillgång till uppgifterna. Detta system är mycket näraliggande kryptering och är egentligen bara ett annat sätt att avskära en alltför stor grupp personer från att ha tillgång till uppgifterna. Det saknas därför skäl att bedöma maskering på något annat sätt än kryptering. Ett införande av maskering skulle därför inte påverka bedömningen av om det svenska systemet är förenligt med EU-rätten.

Sammanfattningsvis skulle en bibehållen lagringsskyldighet men med kryptering eller maskering inte uppfylla de krav som EU-rätten ställer. Utredningen lämnar därför inte något förslag på sådan lagring.

12.5.5 En begränsad lagringsskyldighet bör införas

Den enda rimliga kvarvarande modellen är en sorts ständigt bestående lagringsskyldighet men som inte omfattar alla kommunikationssätt, som är mindre omfattande än i dag och som är bättre anpassad efter vad som är strängt nödvändigt för att bekämpa grov brottslighet. Fördelarna med en sådan lagring är uppenbara och har redovisats tidigare i betänkandet. Nackdelarna är att den kommer att omfatta en stor mängd uppgifter och varav den allra största delen aldrig kommer att begäras tillgång till. Det betyder emellertid inte att lagringsskyldigheten omfattar uppgifter hänförliga till någon person som det är onödigt att lagra uppgifter för. Eftersom man inte vet vem som kommer att begå ett allvarligt brott och det för alla personer finns en risk att de kan utsättas för eller bevittna ett sådant brott, är det

omöjligt att på förväg veta vilka personer som på detta eller på annat sätt kommer att bli inblandade i grov brottslighet. Utredningen föreslår därför en lagring av beskrivet slag. En sådan lagring har också bedömts förenlig med EU-rätten av den ovan nämnda finska utredningen (avsnitt 11.2.5). I en näraliggande fråga rörande lagring, i brottsbekämpande syfte, av flygbolagens passageraruppgifter, har EU-domstolen bedömt att behandlingen av uppgifter inte har gått längre än vad som varit strängt nödvändigt, trots att den avsett samtliga resenärer (till och från Kanada), oberoende av om det förelegat någon objektiv omständighet som gör det möjligt att anse att passagerarna kunnat utgöra en risk för den allmänna säkerheten eller inte (EU-domstolens yttrande 1/15, den 26 juli 2017 p. 41, 186 och 189).

Hur en begränsad lagringsskyldighet kan utformas redovisas i det följande.

En lagringsskyldighet av detta slag kan inte omfatta uppgifter som sällan eller aldrig inhämtas eller för vilka nyttan eller behovet inte är stort. Det är inte tillräckligt att den lagrade uppgiften är användbar eller bra att ha för de brottsbekämpande myndigheterna. Informationen från uppgifterna måste vara påtagligt viktig och inte möjlig att få del av genom en mindre ingripande åtgärd. Både informationen och lagringen måste alltså vara nödvändiga. Även de olika uppgifternas karaktär som mer eller mindre integritetskänsliga måste beaktas. Det innebär inte bara att det måste göras ett noggrant urval av vilka uppgiftskategorier som ska lagras och vilka tjänster som ska omfattas av lagringsskyldigheten, utan även att lagringstiderna måste differentieras och anpassas till vad som är strängt nödvändigt för varje sorts uppgift. Slutligen får inte lagringen vara allomfattande i sådan mening att lagring blir huvudregel i stället för undantag. På detta sätt blir lagringsskyldigheten inte generell (i betydelsen huvudregel) men differentierad, dvs. i varje del anpassad efter vad som är strängt nödvändigt (punkt 103–105 i Tele2-domen).

För att denna modell ska vara förenlig med EU-rätten krävs alltså begränsningar av lagringsskyldigheten. Av allt att döma är de allra flesta uppgifter som omfattas av lagringsskyldigheten i dag till stor nytta för brottsbekämpningen, både i underrättelse- och i utredningsverksamheten. Vidare har det framkommit att de äldsta av de lagrade uppgifterna i många fall används i utredningar rörande de grövsta brotten. Varje begränsning i lagringsskyldigheten torde därför innebära att möjligheten att bekämpa grov brottslighet kommer

att försämras i vissa fall, till förmån för skyddet för privatlivet, en fri och privat kommunikation och yttrandefriheten.

De brottsbekämpande myndigheterna har uppgett att behovet av uppgifter om elektronisk kommunikation ökar markant från år till år och om någon uppgift skulle tas bort från lagringsskyldigheten skulle det ge mycket allvarliga konsekvenser; det skulle minska möjligheterna att bekämpa allvarliga brott, urholka förmågan att skydda nationella säkerhetsintressen och göra Sverige till ett farligare land att vistas i. Det ska emellertid framhållas att en begränsad och proportionerlig lagringsskyldighet som är förenlig med EU-rätten gör det möjligt att behålla något slags lagring som verktyg åt de brottsbekämpande myndigheterna. En lagringsskyldighet som inte är förenlig med EU-rätten och andra grundläggande rättigheter kommer inte att kunna tillämpas (jfr kammarrättens dom, avsnitt 10.3.2) och innebär i så fall i praktiken att inga uppgifter kommer att lagras i syfte att bekämpa brott. En begränsad lagringsskyldighet kan således öka förmågan för de brottsbekämpande myndigheterna att förhindra allvarliga brott och skydda nationella säkerhetsintressen samt göra Sverige till ett säkrare land att vistas i.

12.6 En begränsad lagringsskyldighet

12.6.1 Sammanfattning

Utredningens förslag innebär att nuvarande modell för lagringsskyldigheten reformeras kraftigt för telefonitjänst och meddelandehantering samt i viss utsträckning för internetåtkomst. De uppgifter som inte längre ska lagras för telefonitjänst och meddelandehantering enligt utredningens förslag finns sammanställda sist i avsnitt 12.6.3.

Genom de föreslagna förändringarna blir lagringsskyldigheten inte längre generell; en stor del av trafikuppgifterna kommer inte att omfattas av skyldigheten liksom alla lokaliseringsuppgifter som inte är trafikuppgifter. Lagringen blir därmed undantag och inte huvudregel (Tele2-domen p. 104). Dessutom blir lagringsskyldigheten differentierad genom att den anpassas till att omfatta endast de uppgifter som är strängt nödvändiga att lagra för att bekämpa grov brottslighet, med beaktande av nytta, behov, integritet och proportionalitet (Tele2-domen p. 105). Samtidigt differentieras lagrings-

tiderna utifrån skillnader i behov och uppgifternas integritetskänslighet (se avsnitt 12.7.2).

Förslaget innebär att integritetsintrånget för abonnenterna blir lägre men även att möjligheterna att förebygga, förhindra och utreda brott i vissa fall torde försämras.

Redaktionella ändringar och teknikneutralitet

Utredningen föreslår att lagringsskyldigheten delas upp i två delar, dels telefonitjänst och meddelandehantering, dels internetåtkomst. Bestämmelserna görs teknikneutrala. Det betyder bl.a. att operatörernas användning av NAT-teknik (en teknik för att tillåta att flera abonnenter delar på en och samma publika ip-adress, se avsnitt 6.1) inte påverkar möjligheterna till identifiering av abonnenten.

Telefonitjänst och meddelandehantering

För telefonitjänst och meddelandehantering föreslås att endast uppgifter om kommunikation via en mobil nätanslutningspunkt ska lagras. Det betyder att det inte kommer att lagras några uppgifter om telefonitjänster eller meddelandehantering som sker inom det fasta telefonnätet eller genom fasta internetanslutningar. Om någon av parterna kommunicerar via en mobil nätanslutningspunkt kommer däremot information att lagras, men bara hos den partens operatör.

Trafikuppgifter ska fortfarande lagras. Men lagringsskyldigheten begränsas till uppgifter om vem som kontaktat vem (nummer och abonnent eller registrerad användare samt för telefonitjänst även abonnemangs- och utrustningsidentitet) och vid vilken tidpunkt.

Uppgift om ip-adress ska i sig inte lagras vid telefonitjänst och meddelandehantering. Om en ip-adress använts som adress för att skicka ett meddelande i stället för t.ex. telefonnummer eller e-postadress kommer adressen däremot att lagras. Ip-adressen eller motsvarande uppgift kommer också indirekt att lagras när internetåtkomst krävs för kommunikationen (se nedan).

Uppgift om vilken tjänst som använts, tid för på- och avloggning i tjänsten samt uppgift om utrustning där kommunikationen vid iptelefoni slutligt avskiljs (se dock avsnitt 12.6.4) ska inte längre omfattas av lagringsskyldigheten enligt förslaget.

Lokaliseringsuppgifter ska fortfarande lagras vid ett samtals början och slut. Men precis som tidigare ska inga andra lokaliseringsuppgifter lagras.

För förbetalda anonyma tjänster (oregistrerade kontantkort) ska uppgifter för första aktivering fortfarande lagras.

Lagringsskyldigheten ska fortfarande omfatta misslyckade uppringningar, t.ex. obesvarade samtal – men inte samtal som inte kopplas fram.[6]

Internetåtkomst

För internetåtkomst föreslår utredningen att lagringsskyldigheten ska omfatta uppgifter som gör det möjligt att identifiera abonnenten eller den registrerade användaren. Därmed ska det lagras ip-adress och annan teknisk uppgift som är nödvändig för att identifiera abonnenten eller den registrerade användaren, tidsuppgifter för på- och avloggning i tjänsten som ger internetåtkomst, uppgifter om abonnent och registrerad användare samt uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs. Det ska däremot inte längre finnas någon skyldighet att lagra uppgifter om anslutningskapacitet.

12.6.2 Bara uppgifter som är strängt nödvändiga

Lagringsskyldigheten kan inte begränsas till en viss personkrets, eftersom det är strängt nödvändigt att alla abonnenters och registrerade användares uppgifter omfattas av denna skyldighet (avsnitt 12.5.1). Däremot borde en differentiering kunna göras utifrån användarkategori, t.ex. användare med anonyma abonnemang eller utrustning med mobil nätanslutningspunkt, om en sådan begränsning bedöms som meningsfull och proportionerlig. Dessutom måste lagringen begränsas till de trafik- och lokaliseringsuppgifter som de brottsbekämpande myndigheterna verkligen behöver, har nytta av och som inte kan fås på lämpligare sätt. En proportionerlig och strängt nödvändig lagring kan således som utgångspunkt inte omfatta sådana

[6] En mer utförlig beskrivning av skillnaderna mellan misslyckade uppringningar och samtal som inte kopplas fram finns i SOU 2007:76 s. 159–160.

kategorier av uppgifter som sällan eller aldrig inhämtas i brottsbekämpande syfte. Den kan inte heller omfatta uppgifter som med samma resultat kan inhämtas genom rimliga åtgärder som innebär ett mindre integritetsintrång. Vidare kan den inte omfatta uppgifter för vilken nyttan är liten. Denna bedömning är även i enlighet med Artikel 29-gruppens tolkning av direktivet.[7] Även för abonnemangsuppgifter krävs att lagringen av uppgifterna är strängt nödvändig och proportionerlig i ett demokratiskt samhälle (artikel 8 i Europakonventionen, artiklarna 8 och 52.1 i rättighetsstadgan, Tele2-domen p. 96 samt EU-domstolens yttrande 1/15 den 26 juli 2017 p. 122–124; se även avsnitt 12.9 för ett utförligare resonemang.

Vid bedömningen av vilka uppgifter som är strängt nödvändiga att lagra måste således beaktas behovet och nyttan utifrån bl.a. typ av uppgift, typ av abonnemang och uppgiftens ålder. Samtidigt kan en lagringsskyldighet inte begränsas alltför hårt med beaktande av skyldigheterna att upprätthålla en välfungerande och effektiv brottsbekämpning (avsnitt 12.3).

Vid en första anblick framstår alla begränsningar som ger möjlighet till alternativa kommunikationssätt, som inte omfattas av lagringsskyldigheten, som handlingsdirigerande för den brottsbenägne och därmed som olämpliga. Det argumentet har emellertid inte den tyngd som det framstår vid ett första påseende. Redan i dag är lagringen så begränsad att det är möjligt för en person med högt säkerhetsmedvetande att kommunicera på ett sätt som inte lämnar elektroniska fotspår som omfattas av lagringsskyldigheten. Begränsningar kommer därför inte att påverka möjligheterna till att utreda brott där dessa personer är inblandade på samma allvarliga sätt som det synes vid ett första påseende. Emellertid kommer varje begränsning att innebära en viss försämring för brottsbekämpningen, eftersom även den allra mest säkerhetsmedvetne förr eller senare gör misstag och ju färre uppgifter som lagras, desto svårare blir det att upptäcka dessa misstag.

Utredningens förslag till en förändrad lagringsskyldighet redovisas i det följande.

[7] Artikel 29-gruppens uttalande i WP 220 och WP 237.

12.6.3 Telefonitjänster och meddelandehantering

Utredningens förslag: Lagringsskyldigheten ska endast omfatta kommunikation via en mobil nätanslutningspunkt och avse uppgift om

1. uppringande och uppringt nummer eller motsvarande adress
2. såvitt avser telefonitjänst uppringandes och uppringds abonnemangsidentitet och utrustningsidentitet
3. uppgifter om abonnent och registrerad användare som uppgifterna i 1 och 2 kan hänföras till
4. datum och spårbar tid då kommunikationen påbörjades och avslutades eller ett meddelande skickades och mottogs
5. såvitt avser telefonitjänst lokaliseringsuppgifter då kommunikationen påbörjades och avslutades
6. datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst.

Även misslyckade uppringningar ska omfattas av lagringsskyldigheten.

En samlad bestämmelse för telefoni och meddelanden

Utredningen föreslår att bestämmelserna om telefoni-, mobiltelefoni- och ip-telefonitjänst samt meddelandehantering (39–42 §§ FEK) slås samman till en paragraf. Med de begränsningar som föreslås blir regleringen mer lättillgänglig utan en uppdelning.

Endast uppgifter om trafik via en mobil nätanslutningspunkt

Utredningen föreslår att lagringsskyldigheten begränsas till att, såvitt avser telefonitjänst (inklusive ip-telefoni) och meddelandehantering, endast avse kommunikation via en mobil nätanslutningspunkt. Detta gäller oavsett med vilken teknik utrustningen kommunicerar med det allmänna nätet. Således omfattas alltjämt t.ex. ip-telefoni via operatörernas wifi-zoner, men inte via ett privat trådlöst nätverk med fast anslutning till det allmänna nätet. På detta sätt skapas en teknikneutral reglering där lagringen differentieras till att omfatta endast de abonnenter och användare som inhämtningen främst avser.

Tidigare analyser av vilka uppgifter som inhämtas vid hemlig övervakning och inhämtning enligt IHL ger vid handen att det nästan uteslutande är uppgifter hänförliga till mobiltelefontrafik som inhämtas.[8] Denna bild är enligt de brottsbekämpande myndigheterna alltjämt korrekt, även om det också förekommer inhämtning av uppgifter från det fasta nätet. Det framstår vidare som logiskt att det främst är mobiltelefoner och inte fast telefoni som används i samband med grov brottslighet, jfr prop. 2010/11:46 s. 33. Lagring av telefoni- och meddelandeuppgifter hänförliga till annat än tjänster via en mobil nätanslutningspunkt framstår därmed som oproportionerlig.

Härtill kommer att en fast telefon typiskt sett används av fler personer än en mobiltelefon, som oftast är personlig. Integritetsintrånget vid lagring av uppgifter hänförliga till mobiltelefoner är därmed fokuserat till en snävare personkrets och det totala integritetsintrånget blir därmed mindre vid varje lagringstillfälle, jfr SOU 2012:44 s. 447 och 518. Även av denna anledning blir en lagringsskyldighet som endast omfattar trafik via en mobil nätanslutningspunkt mer riktad än den som följer av nuvarande lagstiftning.

Utredningen vill vara tydlig med att det, som nämnts ovan, inhämtas uppgifter från det fasta nätet och att dessa uppgifter ibland kan vara det enda sättet att komma vidare i det brottsbekämpande arbetet. En begränsning till mobil kommunikation kommer därför att påverka statens möjligheter att bekämpa allvarlig brottslighet i någon mån. Ytterligare en nackdel med begränsningen är att vidarekoppling via det fasta nätet kan användas för att dölja kommunikationens mottagare och slutpunkt. Detta kan motverkas genom att uppgift om nummer som samtalet vidarekopplas till lagras. Utredningen föreslår emellertid att även denna uppgift tas bort från lagringsskyldigheten. Motiveringen till det går att läsa nedan.

Det ska slutligen betonas att den snabba tekniska utvecklingen kan göra att bedömningen utfaller annorlunda inom en relativt snar framtid. Om t.ex. fast ip-telefoni får en mer framträdande roll inom kommunikation är det möjligt att det blir strängt nödvändigt att låta även den omfattas av lagringsskyldigheten. Man kan även tänka sig motsatt bedömning, t.ex. att den meddelandehantering som om-

[8] Se exv. SOU 2015:31 s. 215, 253 och 262 samt SOU 2012:44 s. 389, 447–448, 462 och 514.

fattas av lagringsskyldigheten blir så undanträngd av andra meddelandetjänster att det inte längre framstår som strängt nödvändigt att den omfattas av lagringsskyldigheten.

Lagring av nummer, abonnemangsidentitet, abonnent och registrerad användare

Utredningen föreslår att nummer (och för meddelandehantering, även annan adress), uppgifter om abonnent och registrerad användare och vid telefonitjänst abonnemangsidentitet även fortsättningsvis ska omfattas av lagringsskyldigheten.

Möjligheten för de brottsbekämpande myndigheterna att få reda på vem som har haft kontakt med vem utgör en viktig hörnsten för den brottsbekämpande verksamheten. Samtidigt är uppgifterna tämligen integritetskänsliga, eftersom lagring av dem inkräktar på själva kärnan i rätten till en privat kommunikation (även om inte innehållet i kommunikationen framgår och tillgången till uppgifterna är begränsad). En lagring som inte omfattar uppgift om vem som kontaktat vem är emellertid utesluten, eftersom det är just den informationen (tillsammans med lokaliseringsuppgifter) som över huvud taget motiverar en lagringsskyldighet. I vart fall uppringande och uppringt nummer måste därför lagras.

Abonnemangsidentitet (i praktiken IMSI-nummer, som finns lagrat på sim-kortet) är ofta nödvändigt för att spåra en användare och kan behövas även om telefonnumret är känt. IMSI-numret är särskilt viktigt när myndigheterna ska inhämta uppgifter från en s.k. virituell mobiloperatör (en som inte äger några egna kommunikationsnät), eftersom IMSI-numret i dessa fall kan vara den enda sökvägen för att få tillgång till relevanta trafik-, lokaliserings- och abonnemangsuppgifter, SOU 2015:13 s. 163–164. Uppgift om abonnemangsidentitet gör det också möjligt att spåra användare som behållit sitt sim-kort men bytt telefonnummer, vilket emellertid inte torde vara särskilt vanligt förekommande. Det är av dessa anledningar nödvändigt att fortsätta lagra uppgift om abonnemangsidentitet vid telefonitjänst.

Även om andra adresser än telefonnummer kan användas vid kommunikation genom telefonitjänster bör lagringskravet inte utvidgas till att avse även sådana adresser (SOU 2007:76 s. 303 och

prop. 2010/11:46 s. 29–30). Sådana andra adresser ska dock fortfarande lagras vid meddelandehantering.

Abonnemangsuppgifter, dvs. uppgifter om uppringande och uppringd abonnent och registrerad användare omfattas inte av Tele2-domen (avsnitt 12.2). Som tidigare nämnts krävs ändå att det är strängt nödvändigt att lagra uppgifterna, för att lagringsskyldigheten ska vara proportionerlig och förenlig med EU-rätten. Uppgifterna får även anses ha viss integritetskänslighet, i synnerhet när de lagras tillsammans med trafik- och lokaliseringsuppgifter, eftersom de utgör en länk mellan sådana uppgifter och en fysisk person. Det är också just denna egenskap som utgör den stora nyttan med uppgifterna. Nyttan av lagringen i övrigt blir alltså betydligt mindre om inte abonnemangsuppgifter lagras, eftersom möjligheten att sammanbinda en uppgift med en person då kraftigt begränsas. Uppgifterna är även viktiga vid bekämpning av brott som begås genom elektronisk kommunikation, t.ex. hot över telefon, upprepade trakasserier och överträdelse av kontaktförbud. Det är av båda dessa anledningar strängt nödvändigt att uppgifter om abonnent och registrerad användare omfattas av lagringsskyldigheten.

Lagring av tidsuppgifter

Utredningen föreslår att uppgift om vid vilken tid kommunikationen påbörjades och avslutades fortfarande ska omfattas av lagringsskyldigheten.

Information om vid vilken tidpunkt kommunikationen påbörjades är nödvändig bl.a. för att kunna knyta kommunikationsuppgifter till en gärning och för att kunna göra analyser inför spaningsåtgärder. Utan tidsinformation blir uppgiften om att kommunikationen ägt rum betydligt mindre värdefull. Utifrån ett integritetsperspektiv torde dessutom uppgiften om vem som kontaktat vem vara betydligt känsligare än informationen om vid vilken tid det skedde, även om också den informationen kan vara skyddsvärd. Den extra nytta som tidsuppgifter tillför övriga och mer känsliga kommunikationsuppgifter är enligt utredningens bedömning så stor att en lagring av uppgifterna gör lagringen i sin helhet mer proportionerlig.

Tid för när ett samtal ägde rum eller när ett meddelande skickades eller mottogs måste också lagras i någon form för att operatören ska veta när lagringstiden gått ut.

Ett sätt att begränsa lagringsskyldigheten skulle kunna vara att endast lagra tidpunkt för när kommunikationen påbörjades (men inte när den avslutades eller när ett meddelande mottogs). Även information om när kommunikationen avslutades (och därmed samtalets längd) är emellertid ofta mycket användbar och i vissa fall till och med avgörande. Den informationen gör det nämligen möjligt att kartlägga kommunikationsmönster och på så sätt bedöma när avvikelser sker. Den används också för att dra slutsatser om relationen mellan en person och den som han eller hon samtalar med. Vidare kan man genom samtalslängd filtrera fram intressanta nummer ur en omfattande samtalslista. Ytterligare ett sätt att använda uppgifterna är för att avläsa mer komplexa kommunikationssätt som t.ex. används mellan en underrättelseofficer och en agent. Sådan kommunikation sker inte sällan genom kodspråk; samtal av en viss förutbestämd längd kan i sig vara en informationsbärare, liksom förekomsten av ett visst antal korta respektive långa samtal per dag.

Tidsuppgift för samtalets slut bidrar också till förståelsen av den korresponderande lokaliseringsuppgiften (se nedan). Genom att både tidpunkt och lokalisering sparas vid kommunikationens början och slut blir det möjligt att dra slutsatser om i vilken riktning och fart som en gärningsman har färdats. Sådana uppgifter är extremt viktiga vid människorov men kan även vara avgörande vid andra situationer för att t.ex. hitta gärningsmän, övergivna fordon eller en skadad eller död målsägande. Uppgifterna kan även användas som kontrollinformation vid förhör eller för att dra andra slutsatser om t.ex. färdvägar och mötesplatser.

I sammanhanget kan noteras att tidsuppgifter ibland kan erhållas på andra sätt, exempelvis genom beslag av en mobiltelefon, men det förutsätter att samtals- och meddelandehistoriken finns sparad i telefonen. Det är också långt ifrån alltid som man kan beslagta en telefon, i synnerhet när det gäller underrättelseverksamhet. Som framgår av exempel i avsnitt 7.1 förekommer det dessutom att samtalshistorik raderas eller manipuleras i bevisförstörande syfte. Uppgifterna i en mobiltelefon kan även vara oriktiga av andra anledningar, t.ex. tekniska fel. Härutöver är det inte säkert att polisen, även om en mobiltelefon har tagits i beslag, kan komma åt uppgif-

terna eftersom telefoner ofta är krypterade och lösenordsskyddade. Möjligheten att få uppgifter på annat sätt är således begränsad och de brottsbekämpande myndigheternas behov av uppgifterna bedöms därför som stort.

Lagring av uppgift om när ett samtal avslutades utgör ett något ökat integritetsintrång gentemot att endast lagra tidpunkt för samtalets början. Det beror just på de ytterligare slutsatser som kan dras om t.ex. relation till samtalspartnern och den extra nytta som uppgifterna tillför lokaliseringsuppgifter.

Tidpunkt för när ett meddelande mottogs framstår inte som en lika viktig uppgift för brottsbekämpningen som informationen om när ett samtal avslutades. Den uppgiften kan nämligen inte ge någon uppfattning om relation eller bidra till att förbättra förståelsen för någon lokaliseringsuppgift (uppgift om lokalisering vid meddelanden omfattas inte av lagringsskyldigheten, varken enligt nuvarande lagstiftning eller med utredningens förslag). I de allra flesta fall mottas också meddelanden i mycket nära anslutning till att de skickades, i vart fall såvitt avser sms. Att ta bort uppgift om när ett meddelande mottogs framstår emellertid som problematiskt eftersom motsvarande tidsuppgift ändå måste sparas för att den mottagande operatören ska kunna veta när uppgiften ska raderas. Därutöver ger uppgiften viss annan nytta. Den kan nämligen förklara varför en persons aktivitet inleddes vid en specifik tid (vid mottagandet av meddelandet) eller motsatt: varför personen inte reagerade i samband med att ett visst meddelande skickades. Särskilt i förhörssituationer kan det vara en fördel för förhörsledaren (och den misstänkte) om det med objektiva uppgifter går att visa när ett visst meddelande mottogs. Uppgift om när ett meddelande mottogs är också av intresse i mer extrema situationer, som dock är mycket angelägna att kunna reda ut, t.ex. vid bomber som fjärrutlösts via sms. Uppgift om vid vilken tidpunkt som ett meddelande mottogs kan inte i sig anses utgöra något större ökat integritetsintrång, om uppgift att meddelandet mottagits ändå lagras.

Sammantaget har det framkommit att såväl nytta som behov av att lagra tidsuppgift, även vid kommunikationens slut, i många fall är mycket betydande. Uppgifterna bidrar även till att öka nyttan av lagringen av andra uppgifter. De används i princip vid varje analys av uppgifter från elektronisk kommunikation. Det ytterligare ingrepp i en persons integritet som följer av att det även lagras information

om vid vilken tid ett samtal avslutades och i synnerhet när ett meddelande mottogs bedöms inte som stort. Sammantaget är det strängt nödvändigt att lagra uppgifterna. De bör därför fortfarande omfattas av lagringsskyldigheten.

Lagring av uppgift om utrustningsidentitet

Utredningen föreslår att uppgift om utrustningsidentitet fortfarande ska lagras för telefoni men inte för meddelanden.

Uppgift om utrustningsidentitet utgör, liksom många andra trafikuppgifter, en länk i kedjan som binder samman en persons elektroniska fotspår.

Vissa brottslingar byter ofta sim-kort i sin telefon för att försvåra för de brottsbekämpande myndigheterna. Genom att lagra uppgift om telefonens identitet (t.ex. IMEI-nummer) vid kommunikation blir det möjligt att länka samman olika sim-kort som använts. Oavsett vilket av sim-korten som använts kommer nämligen numret för telefonens identitet att vara detsamma.

En stor del av de relevanta inhämtade uppgifterna hänför sig till oregistrerade kontantkort (förbetalda anonyma tjänster), SOU 2012:44 s. 447. I vart fall blir det allt vanligare bland gärningsmän som begår planerade brott att använda sådana anonyma abonnemang och det blir allt vanligare att kriminella förser sig med ett stort antal kontantkort, SOU 2015:31 s. 164–165. Dessa omständigheter talar för att uppgift om utrustningsidentitet är viktig att lagra men att lagringsskyldigheten skulle kunna begränsas till att bara omfatta uppgifter hänförliga till dessa abonnemangstyper. Man skulle även kunna argumentera för att integritetsintrånget är mindre vid lagring av uppgifter för oregistrerade kontantkort, just eftersom de är anonyma. Detta skulle sammantaget även kunna anföras som skäl för att lagringsskyldigheten i sin helhet endast ska gälla oregistrerade kontantkort. En sådan begränsning skulle emellertid leda till att en oförsvarligt stor mängd relevant data skulle gå förlorad och framstår därmed som alltför kraftig. Även om byte av sim-kort i syfte att försvåra för brottsbekämpningen i och för sig huvudsakligen lär avse anonyma kontantkort, begås en stor del av de grova brotten inte av personer med hög säkerhetsförmåga och föregås inte av noggrann planering. De brottsbekämpande myndigheterna har även uppgett

att ett vanligt misstag som görs av kriminella är att kontantkortet sätts in i en telefon som annars används med ett registrerat abonnemang. Det förekommer dels att kriminella har två sim-kort som används i en och samma telefon, ett sim-kort för sociala ändamål och ett för kriminella, dels att sim-kort som vanligtvis används i en särskild telefon flyttas till en ”abonnemangstelefon”, t.ex. på grund av batteribrist.

Därutöver används utrustningsnumret även för andra syften än att koppla samman abonnemang på nyss nämnda sätt. Ett exempel är att länka samman en MAC-adress med trafikuppgifter. MAC-adressen är ett unikt identifikationsnummer på nätverkskortet och används bl.a. när utrustningen (telefonen i detta exempel) kommunicerar med ett lokalt nätverk, t.ex. en trådlös router (wifi). MAC-adress och IMEI-nummer (telefonens utrustningsidentitet för mobilnätet) kan kopplas samman med hjälp av uppgifter från tillverkare, försäljare eller leverantörer av mobilappar. Lagras IMEI-numret eller annat utrustningsnummer utgör det således en vägvisare till rätt kommunikationsuppgifter. På detta sätt har flera misstänkta gärningsmän kunnat identifieras av de brottsbekämpande myndigheterna. Lagring av uppgiften innebär alltså att nyttan av övriga lagrade uppgifter i vissa fall ökar.

Ytterligare en nytta med att känna till utrustningsidentitet är att det talar om vilken typ av utrustning som använts, såsom att det är en telefon av visst varumärke och modell. Det leder till flera fördelar, t.ex. att rätt utrustning tas i beslag och att det vid spaning blir lättare att identifiera användaren.

Enligt uppgift från de brottsbekämpande myndigheterna används information om utrustningsidentitet också i stor utsträckning i samband med att myndigheterna bistår andra länder i utredningar om t.ex. internationell terrorism.

Det kan också noteras att utrustningsnummer kan vara av stor vikt för att kunna verkställa hemlig dataavläsning, som det för närvarande utreds om det ska införas (dir. 2016:36). Den omständigheten får emellertid i nuläget inte någon inverkan på bedömningen av om uppgiften bör omfattas av lagringsskyldigheten eller inte.

Utrustningsidentitet utgör för de flesta människor en inte särskilt integritetskänslig uppgift. Numret kan som nämnts vara ett insteg till andra uppgifter men i sig ger den i princip endast information om varumärke och modell på utrustningen som används.

Sammantaget framstår det som strängt nödvändigt att uppgift om utrustningsidentitet vid telefonitjänst alltjämt omfattas av lagringsskyldigheten för alla slags abonnemang som använder en mobil nätanslutning.

Enligt dagens lagstiftning ska inte utrustningsidentitet lagras vid meddelandehantering. Utredningen har svårt att se några bärande skäl för denna skillnad. Det finns två huvudargument för att låta lagringsskyldigheten för denna uppgift även omfatta meddelanden: dels blir bestämmelsen teknikneutral, dels tycks en stor del av de relevanta uppgifterna som inhämtas avse sms. Att på detta sätt utöka lagringsskyldigheten kan emellertid inte anses ligga i linje med det krav på begränsning som EU-rätten ställer. Utredningen föreslår därför inte någon sådan utökning.[9]

Lagring av lokaliseringsuppgifter

Utredningen föreslår att lokaliseringsuppgifter vid kommunikationens början och slut fortfarande ska lagras vid telefonitjänst men inte vid meddelandehantering.

Lokaliseringsuppgifter är nödvändiga för att kunna analysera såväl kända som okända gärningsmäns rörelsemönster. Det är också ett sätt att bekräfta andra källors uppgifter. Kartläggningen av misstänktas rörelser före, under och efter ett allvarligt brott gör att brottsutredarna kan få information om bl.a. förberedelser och flyktvägar och hur andra tvångsmedel kan användas, t.ex. var spaning eller husrannsakan ska genomföras. Lokaliseringsuppgifter används även för att bedöma om den misstänkte har haft möjlighet att utföra gärningen och om personen befunnit sig på andra platser som kan kopplas till brottet, t.ex. där en flyktbil stals eller ett vapen inhandlades, eller till någon person av speciellt intresse. Genom att se på vilka platser en okänd innehavare av en telefon har kommunicerat är det också möjligt att med hjälp av t.ex. bilder från övervakningskameror på dessa platser identifiera innehavaren. Utredningen bedömer det redan av dessa anledningar som strängt nödvändigt att

[9] Se motsvarande resonemang för lokaliseringsuppgifter nedan. Samma skillnad finns också för abonnemangsidentitet.

lagringsskyldigheten även fortsättningsvis ska omfatta lokaliseringsuppgifter av något slag.

Lokaliseringsuppgifter är även viktiga för att få reda på vilka mobiltelefoner som har varit på en viss plats, t.ex. där ett lik har hittats. Denna information kan fås genom basstationstömningar (avsnitt 6.2.3). Som beskrivs i avsnitt 6.2.1 och 12.8.6 får alla tillgängliga lokaliseringsuppgifter begäras in från operatören, inte bara dem som lagras för brottsbekämpande ändamål. Av vad som framkommit är det trots det i princip uteslutande de uppgifter som omfattats av lagringsskyldigheten som myndigheterna får tillgång till vid en basstationstömning (möjligen med undantag för lokaliseringsuppgifter vid sms). Ett rimligt antagande är därför att andra lokaliseringsuppgifter förstörs relativt omgående efter att de genererats. Dessutom är det inte alltid ett brott upptäcks direkt efter att det har begåtts och det kan först senare i utredningen bli intressant att få information hänförlig till en viss plats. Det finns därför även av denna anledning skäl att låta lagringsskyldigheten fortsatt omfatta lokaliseringsuppgifter.

Ytterligare ett sätt att använda lokaliseringsuppgifter är för att identifiera en person som är inblandad i brottslig verksamhet (eller egentligen dennes telefon). Vet man t.ex. att en misstänkt eller en gärningsman använt sin mobiltelefon vid vissa tidpunkter på en eller flera specifika platser kan man samköra listor från basstationstömningar och på så sätt få fram intressanta telefon- eller utrustningsnummer. Ju fler uppgifter som finns, desto träffsäkrare blir analysen.

Den kanske största nyttan av lokaliseringsuppgifter är att trafikuppgifterna blir mer begripliga. Lokaliseringsuppgifter vid kommunikation utgör därmed en mycket viktig pusselbit vid analysen av en misstänkts eller en målsägandes kommunikation; en uppgift om att A ringt B är betydligt mindre värd än en uppgift om att A ringde B just när A var på en specifik plats och B på en annan sådan plats. Det kan alltså sägas att lokaliseringsuppgifter bidrar till att öka nyttan av övriga trafikuppgifter och gör lagringen av dessa uppgifter mer proportionerlig. Det behöver knappast sägas att det därutöver i sig självt är av synnerligen stort intresse att få information om kommunikation som skett i anslutning till en känd brottsplats och brottstidpunkt, vilket uppenbarligen kräver att positionen för kommunikationen är lagrad. De lokaliseringsuppgifter som ska omfattas

av lagringsskyldigheten bör sammanfattningsvis fortsatt vara kopplade till kommunikation.

När det gäller skyldighet att lagra lokaliseringsuppgifter vid samtalets avslut bör följande beaktas. Nyttan av att lagra position både när kommunikationen påbörjas och avslutas utgör även det en viktig beståndsdel i analysen för att upptäcka, utreda och beivra allvarlig brottslighet. Information om att en person avslutar ett samtal just när han eller hon kommit till en specifik plats kan ha stor betydelse och t.ex. ge indikationer om intressanta platser och ge upphov till spaningsuppslag. Ett samtal kan t.ex. avslutas när två personer möts, när någon kommit hem eller till arbetet eller när en person nått fram till den plats som samtalspartnern gett en vägbeskrivning till. Därtill gör två positioner kopplade till samma samtal det möjligt att få fram en riktning i vilken personen har rört sig, vilket gör det enklare att spåra personen. Tillsammans med tidsuppgifter kan man också uppskatta hastighet och därmed bedöma om personen använt sig av ett fordon och i hur stort område personen kan ha rört sig. Vidare bidrar fler lokaliseringsuppgifter till att analysen av vardagsmönster blir mer pricksäker. Det gör både att nyttan blir större för de brottsbekämpande myndigheterna i såväl underrättelse- som förundersökningsverksamheten men även att uppgifterna blir mer integritetskänsliga.

I sammanhanget ska noteras att ett genomsnittligt samtal för en privatperson från mobiltelefon är omkring tre minuter långt (avsnitt 7.3.1). Det ska också nämnas att en begränsning till att bara lagra uppgift om position vid samtalets början redan finns i andra länder och att datalagringsdirektivet endast föreskrev en sådan lagring (artikel 5.1 f) 1). Utredningen bedömer också att lokaliseringsuppgifter generellt sett är tämligen integritetskänsliga. Som EU-domstolen nämner i Tele2-domen, kan man dra mycket precisa slutsatser om privatlivet för de personer vars uppgifter lagras. Samtidigt används informationen vid i princip varje analys av elektroniska kommunikationsuppgifter. Just att man kan dra mycket precisa slutsatser gör att lokaliseringsuppgifter utgör ett välanvänt och extremt värdefullt verktyg, inte minst i underrättelseverksamheten. Som nämnts följer många fördelar av att mer än en position sparas vid varje samtal.

Vid en sammantagen bedömning finner utredningen att det är strängt nödvändigt att uppgifterna sparas och föreslår därför att lag-

ringsskyldigheten alltjämt ska omfatta uppgift om lokalisering vid samtalets början och slut. Det är dock viktigt att lagringstiden anpassas till uppgifternas höga integritetskänslighet (avsnitt 12.7.2).

Enligt den nuvarande lagstiftningen ska inte några lokaliseringsuppgifter lagras vid meddelandehantering. Av vad som framkommit finns det för de brottsbekämpande myndigheterna ett minst lika stort behov av att få del av uppgifter om lokalisering vid meddelandehantering som vid telefoni; det är t.ex. vanligt att sms används som det enda kommunikationssättet mellan gärningsmän vid allvarlig brottslig verksamhet. Det skulle därför kunna argumenteras för att även lokaliseringsuppgift vid meddelandehantering borde omfattas av lagringsskyldigheten, dels för att en mycket stor mängd relevanta uppgifter annars går om intet, dels för att bestämmelsen blir mer teknikneutral.[10] Det synes också ha varit lagstiftarens avsikt, eftersom begränsningen till telefonitjänst endast finns i FEK; lokaliseringsuppgifter får nämligen lagras enligt LEK. Ytterligare ett argument för att införa en sådan skyldighet är att uppgifterna kan ge mervärde åt andra lagrade uppgifter, vilket i sin tur kan göra den övriga lagringen mer proportionerlig. En förutsättning för att en lagringsskyldighet alls ska vara förenlig med EU-rätten är emellertid att färre uppgifter lagras. I linje härmed föreslår utredningen inte att lokaliseringsuppgifter vid meddelandetjänst ska omfattas av lagringsförslaget. Ett förändrat kommunikationsmönster kan dock framöver leda till att det blir strängt nödvändigt att lagra lokaliseringsuppgifter även vid meddelandehantering, jfr även de trender om meddelandehantering som beskrivs i avsnitt 7.3.1.

Uppgift om ip-adress ska inte lagras

Utredningen föreslår att ip-adress inte ska omfattas av lagringsskyldigheten för telefonitjänst och meddelandehantering.

Vid ip-telefoni ska det enligt dagens lagstiftning lagras uppringande och uppringds ip-adresser. Motsvarande gäller vid meddelandehantering. De brottsbekämpande myndigheterna har värderat denna information högt och man kan se exempel där informationen varit till nytta.

[10] Se motsvarande resonemang för uppgift om utrustningsidentitet ovan.

Ip-adresser utgör en länk mellan å ena sidan internetanvändande och å andra sidan telefoni och meddelandehantering. Eftersom ip-adress kan användas vid samtliga dessa tjänster kan ett spår från internetanvändning därför användas för att hitta rätt kommunikationsuppgifter, om ip-adressen finns sparad. En ip-adress kan också ge en uppfattning om positionen för den som kommunicerar.

I relation till andra uppgifter är det dock svårt att se att det är strängt nödvändigt att uppgift om ip-adress ska omfattas av lagringsskyldigheten. Behovet av att använda ip-adress för att länka samman internetanvändning med uppgifter om samtal och meddelanden minskar dessutom med utredningens förslag om en mer teknikneutral reglering för lagring vid internetåtkomst, avsnitt 12.6.4. Den regleringen kommer att leda till att det oftare går att identifiera abonnenten bakom en ip-adress. Därtill har ip-adresser i vissa fall ett skyddsvärde, eftersom de kan utgöra en nyckel till en persons internetanvändning (under förutsättning att information om hur ip-adressen trafikerat internet finns tillgänglig). Sammantaget får därför uppgiften ge vika för att kunna möjliggöra en proportionerlig lagringsskyldighet för högre prioriterade uppgifter.

Om ip-adressen har använts som adress för att skicka ett meddelande, dvs. angetts av användaren i stället för t.ex. ett telefonnummer (något som, om det alls förekommer, torde vara ovanligt), så ska den däremot lagras.

Uppgifter om tjänst som använts samt datum och spårbar tid för på- och avloggning i tjänsten ska inte lagras

Utredningen föreslår att uppgifter om den eller de tjänster som har använts samt datum och spårbar tid för på- och avloggning i de tjänsterna tas bort från lagringsskyldigheten.

Värdet av att få information om använd tjänst värderas generellt lågt i förhållande till andra uppgifter, av de brottsbekämpande myndigheterna.

Uppgifterna kan bidra till förståelsen vid analys av kommunikationsmönster och det kan ibland vara avgörande att veta om kommunikationen utgjordes av t.ex. sms, mms eller videosamtal eller om samtalet vidarekopplades till röstbrevlådan. Uppgifterna är således nyttiga men sällan av mycket stor vikt.

Det har framförts att uppgift om vilken typ av tjänst som använts kan vara bra att ha för att veta om det t.ex. är ett meddelande som har skickats och myndigheten därmed kan begära tillstånd att få del av innehållet i meddelandet genom hemlig avlyssning. För det fall innehållet i ett meddelande fortfarande finns sparat hos operatören lär emellertid även uppgiften om tjänst göra det. Motsvarande torde gälla vidarekoppling till röstbrevlåda. Argumentet ter sig därför inte övertygande.

Även om uppgift om tjänst får anses ha en relativt låg integritetskänslighet är utredningens sammantagna bedömning att en lagring av uppgiften inte är strängt nödvändig. Utredningen föreslår därför att uppgiften tas bort från lagringsskyldigheten.

Vad gäller datum och spårbar tid för på- och avloggning i den eller de tjänster som använts är det svårare att konkretisera nyttan av uppgiften. Ett exempel som dock framförts är s.k. *dead drop*. Om t.ex. en underrättelseofficier och en agent vill utbyta information med varandra kan de skriva e-postmeddelanden och spara dem som utkast, men välja att inte skicka dem. Om den andre har tillgång till inloggningsuppgifterna kan han eller hon därefter logga in på samma konto och läsa utkastet. På så sätt lämnas färre elektroniska spår. Uppgift om på- och avloggning i e-posttjänsten, i kombination med uppgift om ip-adress, gör det därför möjligt att enklare upptäcka detta upplägg och identifiera författare och läsare av den hemliga informationen. Eftersom uppgift om såväl ip-adress som använd tjänst tas bort från lagringsskyldigheten utgör denna nytta inte ett bärande skäl att behålla lagringen av uppgiften. Därtill får det antas att den som planerar ett sådant relativt sofistikerat kommunikationssätt inte använder sig av en operatörs e-posttjänst utan en i sammanhanget anonymare tjänst, tillhandahållen av andra aktörer på internet.

Nummer som samtalet styrs till ska inte lagras

Utredningen föreslår att nummer som samtalet styrs till tas bort från lagringsskyldigheten.

Vad gäller vidarekopplade samtal har det inte framkommit något omfattande behov av att veta vilket nummer som samtalet styrts till. Det har t.ex. inte framkommit något stöd för att vidarekoppling är

särskilt vanligt förekommande. Däremot står det klart att uppgiften i vissa fall kan bidra till stor nytta för brottsbekämpningen.

Det får inledningsvis antas att den som initierat kommunikationen vanligtvis vill ha kontakt med den som använder det uppringda numret. I normalfallet vid vidarekoppling styrs troligen också samtalet vidare till något annat nummer som tillhör samma användare. Nyttan av att få information om det nummer som samtalet styrts till gör sig därför främst gällande om samtalet omstyrts i syfte att försvåra för de brottsbekämpande myndigheterna. Som nämnts ovan, skulle det t.ex. kunna vara möjligt att ”tvätta” ett nummer via det fasta nätet, för att på så sätt dölja kommunikationen. Det ska emellertid noteras att personer med ett högt säkerhetsmedvetande har möjlighet att kommunicera på andra och mindre komplicerade sätt, som inte lämnar sådana elektroniska spår som ska lagras.

Ytterligare ett exempel på uppgiftens nytta utgörs av att den kan användas för avkodning av mer sofistikerade kommunikationssätt. Tidigare i detta avsnitt har det redogjorts för hur förutbestämd information kan kommuniceras genom samtalsmönster. Vidarekoppling kan också vara del av den informationen.

Om vidarekoppling görs till någon annan persons telefonnummer kan det ge en antydan om att personerna har en nära relation. Görs det till ett eget nummer, som inte är registrerat i personens namn, utgör vidarekoppling en länk till ytterligare uppgifter om personen. Det kan också vara intressant för den brottsbekämpande myndigheten att veta om samtalet styrts till röstbrevlådan, eftersom det då kan finnas meddelanden som myndigheten kan söka tillstånd att få del av.

Uppgiftens integritetskänslighet är beroende av till vilket nummer som samtalet kopplas till. En vidarekoppling till ett registrerat nummer för samma person eller till röstbrevlådan är i normalfallet inte en särskilt integritetskänslig uppgift medan en uppgift om en vidarekoppling till en annan persons nummer normalt måste bedömas som något mer känslig.

Vid en sammantagen bedömning kan det inte bedömas vara strängt nödvändigt att lagra uppgift om vidarekoppling. Även om den bidrar till viss nytta, finns det flera uppgifter som är betydligt viktigare att lagra. Det saknas därför tillräckliga skäl att låta uppgifter om det nummer som samtalet styrs till omfattas av lagringsskyldigheten.

Uppgift om utrustning där kommunikationen avskiljs ska inte lagras

Utredningen föreslår att uppgift som identifierar den utrustning där kommunikationen slutligt avskiljs inte ska omfattas av lagringsskyldigheten för telefonitjänst och meddelandehantering.

Uppgift som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige ska enligt dagens lagstiftning lagras vid ip-telefoni. Vid fast telefoni kan denna utrustning vara t.ex. ett telefonjack eller ett fibermodem, medan det vid mobil ip-telefoni ofta är en cell i en basstation (mobilmast), men den kan även vara en router, om det är ett allmänt trådlöst nätverk. Uppgiften används bl.a. för att ge information om var utrustningen geografiskt finns och har av de brottsbekämpande myndigheterna bedömts som oerhört viktig för att kunna lokalisera den plats varifrån någon kommunicerar.

Den nytta som uppgiften genererar torde kunna erhållas på annat sätt. Samma uppgift genereras och lagras nämligen vid internetåtkomst, låt vara att det kan vara vid en annan tidpunkt än när ip-telefonisamtalet ringdes. Eftersom lokaliseringsuppgifter, vid kommunikation från en mobil nätanslutningspunkt, ska lagras vid samtalets början och slut kan lokaliseringsuppgift även fås på detta sätt.

Även om uppgifterna kan ge stor nytta är behovet av att lagra dem inte påtagligt. Redan av denna anledning framstår en skyldighet att lagra uppgiften inte som proportionerlig. Sammantaget bör uppgiften inte omfattas av lagringsskyldigheten.

Lagring av misslyckade uppringningar

Utredningen föreslår att misslyckade uppringningar (obesvarade samtal) fortfarande ska omfattas av lagringsskyldigheten, men inte samtal som inte kopplats fram.

Enligt nuvarande lagstiftning ska även obesvarade samtal omfattas av lagringsskyldigheten. Dessa samtal ska inte blandas ihop med sådana som över huvud taget inte kopplats fram, t.ex. på grund av tekniskt fel. Dessa omfattas inte av lagringsskyldigheten enligt dagens lagstiftning.

Lagringsskyldigheten bör inte vara beroende av om den uppringda parten svarar eller inte. Ett försök att kontakta någon kan

betyda lika mycket som att personerna har haft kontakt med varandra. Obesvarade samtal används dessutom för att meddela medgärningsmän förutbestämd information, t.ex. att en målsägande är på plats eller att gärningen eller en förberedelse är utförd SOU 2007:76 s. 159. På liknande sätt kan de användas som koder mellan en underrättelseofficier och en agent. Det bedöms därför som strängt nödvändigt att uppgifter från misslyckade uppringningar ska omfattas av lagringsskyldigheten.

Det har inte framkommit något behov av att utöka lagringsskyldigheten till att även omfatta uppgifter om samtal som på grund av tekniskt fel inte har kopplats fram. Det får dessutom antas att det i de allra flesta fall görs ett nytt försök att initiera samtalet, varvid motsvarande uppgifter kommer att genereras och lagras.

Lagring av uppgifter för första aktiveringen av en förbetald anonym tjänst

Utredningen föreslår att uppgifter för första aktiveringen av en förbetald anonym tjänst fortfarande ska lagras.

Uppgifterna används bl.a. efter basstationstömningar. Som nämnts ovan blir det allt vanligare att brottslingar använder anonyma kontantkort, som aktiveras innan ett grovt brott ska begås. En analys av vilka av de kontantskortsabonnemang som kan kopplas till en gärningsplats och som nyligen har aktiverats kan därför ge en bild av vilka telefoner som är särskilt intressanta. Första aktiveringen kan ge indikationer om inköpsställe eller bostadsort, som i sin tur kan leda till identifiering av innehavaren. Sådana uppgifter kan också användas för att hitta bomber, som kan fjärraktiveras genom elektronisk kommunikation. (SOU 2015:31 s. 164–165)

Dessa uppgifter är inte särskilt integritetskänsliga. De avser anonyma tjänster och avslöjar mycket lite om personens övriga kommunikation, aktiviteter eller privatliv. Även om några av de brottsbekämpande myndigheterna inte har värderat dessa uppgifter särskilt högt i förhållande till andra uppgifter, är det utredningens uppfattning att nyttan med råge överträffar det ringa integritetsintrång som en lagring av uppgifterna innebär. Det har även framkommit att uppgifterna ofta används i det inledande skedet av vissa utredningar och när andra spaningsuppslag saknas. Även behovet av

uppgifterna framstår därmed som påtagligt. Det bedöms sammantaget som strängt nödvändigt att fortsätta lagra dessa uppgifter.

Uppgifter som tas bort för telefonitjänst och meddelandehantering

Kommunikation som inte går via en mobil nätanslutningspunkt

Fast telefoni (ej ip-telefoni), 39 § FEK

1. uppringande nummer
2. uppringt nummer och nummer som samtalet styrts till
3. uppgifter om uppringande och uppringd abonnent och, i förekommande fall, registrerad användare
4. datum och spårbar tid då kommunikationen påbörjades och avslutades
5. uppgifter om den eller de tjänster som har använts

Fast ip-telefoni, 39 och 41 §§ FEK

1. uppringande nummer
2. uppringt nummer och nummer som samtalet styrts till
3. uppgifter om uppringande och uppringd abonnent och, i förekommande fall, registrerad användare
4. datum och spårbar tid då kommunikationen påbörjades och avslutades
5. uppgifter om den eller de tjänster som har använts
6. uppringandes och uppringds ip-adresser
7. datum och spårbar tid för på- och avloggning i den eller de tjänster som använts
8. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten

9. uppgifter som identifierar den utrustning där kommunikationen avskiljs från den lagringsskyldige till den som slutligt avskiljer kommunikationen till den enskilda abonnenten, om den senare inte är lagringsskyldig

Meddelandehantering som inte går via mobil nätanslutningspunkt, 42 § FEK

1. avsändares och mottagares nummer, ip-adress eller annan meddelandeadress
2. uppgifter om avsändande och mottagande abonnent och, i förekommande fall, registrerad användare
3. datum och spårbar tid för på- och avloggning i den eller de tjänster som använts
4. datum och spårbar tid för avsändande och mottagande av meddelande
5. uppgifter om den eller de tjänster som har använts

Uppgifter om kommunikation via en mobil nätanslutningspunkt

Mobiltelefoni (ej ip-telefoni), 39 och 40 §§ FEK

1. nummer som samtalet styrts till från uppringt nummer
2. uppgifter om den eller de tjänster som har använts

Mobil ip-telefoni, 39–41 §§ FEK

1. nummer som samtalet styrts till från uppringt nummer
2. uppgifter om den eller de tjänster som har använts
3. uppringandes och uppringds ip-adresser
4. datum och spårbar tid för på- och avloggning i den eller de tjänster som använts

5. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten
6. uppgifter som identifierar den utrustning där kommunikationen avskiljs från den lagringsskyldige till den som slutligt avskiljer kommunikationen till den enskilda abonnenten, om den senare inte är lagringsskyldig

Mobil meddelandehantering, 42 § FEK

1. datum och spårbar tid för på- och avloggning i den eller de tjänster som använts
2. uppgifter om den eller de tjänster som har använts

12.6.4 Internetåtkomst

Utredningens förslag: Lagringsskyldigheten ska endast omfatta

1. användares ip-adress och annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare
2. uppgifter om abonnent och registrerad användare
3. datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomst
4. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.

Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten är någon som inte är lagringsskyldig, ska lagringsskyldigheten i stället avse uppgift om utrustningen där kommunikationen avskiljs till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.

Lagring av ip-adress och uppgifter om abonnent och registrerad användare

Utredningen föreslår att uppgift om ip-adress samt uppgifter om abonnent och registrerad användare fortfarande ska lagras.

Abonnemangsuppgifter omfattas inte av Tele2-domen men väl av skyddet för personuppgifter i såväl Europakonventionen och rättighetsstadgan, avsnitt 12.2. En skyldighet att lagra uppgifterna måste därför vara strängt nödvändig för att den ska kunna godtas, avsnitt 12.6.2.

För brott begångna över internet är abonnemangsuppgifterna, dvs. vilken person som innehar en specifik ip-adress eller annan unik användaradress vid varje tillfälle, den absolut viktigaste informationen. Denna information är uppenbart nödvändig för att kunna få fram identiteten på den som över internet t.ex. tillgängliggör barnpornografi eller upphovsrättsskyddat material, säljer narkotika och vapen, hotar och förtalar, tar kontakt med barn i sexuellt syfte eller gör dataintrång och andra digitala attacker mot privatpersoner, företag eller myndigheter. Uppgifterna är också viktiga för att kunna identifiera dem som använder internet för att kommunicera med t.ex. medgärningsmän eller sin underrättelseofficier eller för att rekrytera andra till terrorbejakande organisationer.

I takt med att fler och fler använder internet och användningsområdet för internet utökas, ökar också internetbrottsligheten och därmed behovet av verktyg för brottsbekämpningen även på denna arena, se avsnitt 7.3, 12.3 och 12.9 (särskilt hänvisningen till Europadomstolens mål K.U. mot Finland). Nyttan av uppgifterna är således synnerligen stor. Det saknas i praktiken ofta andra möjligheter att identifiera en aktör på internet på annat sätt än genom uppgift om ip-adress i kombination med andra abonnemangsuppgifter. Även behovet av uppgifterna är således påtagligt.

Abonnemangsuppgifter för internet utgörs i princip av uppgift om vilken abonnent som vid varje tidpunkt var användare av en specifik ip-adress. Dessa uppgifters integritetskänslighet har varit föremål för diskussion. I sig själv är uppgifterna inte särskilt känsliga, eftersom de bara berättar att ett abonnemang någon gång har getts internetåtkomst. Men med hjälp av uppgifterna går det att sammankoppla en fysisk person med de eventuella avtryck som användaren har lämnat efter sig vid besök på webben eller andra delar av internet,

vilket gör uppgifterna mer skyddsvärda. Vid bedömningen av känsligheten ska vidare beaktas att det huvudsakligen är dynamiska ip-adresser som används, åtminstone av privatpersoner. Det innebär att en ensam uppgift om vilken abonnent som använt en viss ip-adress bara gör det möjligt att sammankoppla abonnenten med avtryck på internet under en begränsad tid. Ska man kunna följa en abonnents internetanvändning krävs således, förutom tillgång till digitala avtryck, även tillgång till en stor mängd abonnemangsuppgifter. Det ska också påpekas att inga uppgifter om t.ex. besök på webbsidor eller annat internetanvändande, förutom operatörens egna tjänster för telefoni och meddelandehantering, omfattas av lagringsskyldigheten, varken enligt dagens lagstiftning eller enligt utredningens förslag. Sådana uppgifter är operatörerna i stället skyldiga att förstöra, om de inte behövs för vissa egna ändamål. Tillgång till endast de uppgifter som enligt utredningens förslag ska lagras kan således aldrig innebära att det kan kartläggas hur en person har trafikerat internet.

För att inte helt slå undan de brottsbekämpande myndigheternas möjlighet att bekämpa brott som begåtts eller planlagts över internet är det strängt nödvändigt att ip-adress och uppgifter om abonnent och registrerad användare lagras (se även avsnittet Bestämmelsen blir teknikneutral nedan). Nyttan och behovet av att lagra uppgifterna är så stora att de tydligt uppväger det integritetsintrång som lagringen innebär. Uppgifterna bör således alltjämt omfattas av lagringsskyldigheten.

Lagring av tidsuppgifter

Utredningen föreslår att datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomst ska omfattas av lagringsskyldigheten.

Uppgifterna har värderats högt av de brottsbekämpande myndigheterna.

Uppgift om på- och avloggning är ofta avgörande för att kunna spåra rätt internetanvändare, eftersom samma publika ip-adress kan tilldelas olika användare vid olika tidpunkter. Som framgår nedan är emellertid inte alltid ens det tillräckligt för att kunna hitta rätt användare. Om t.ex. polisen genom en leverantör av en chattapp får

reda på att en användare med en viss ip-adress vid en viss tidpunkt har kontaktat barn i sexuellt syfte kan polisen, genom att bl.a. ip-adress och tidsuppgift lagras, få information om vilken abonnent som använt ip-adressen vid just den tidpunkten. Detta fungerar även åt motsatt håll. Vet man om att en misstänkt person varit uppkopplad mot internet en viss tid, kan man ta kontakt med t.ex. en appleverantör och fråga om ip-adressen varit inloggad den aktuella tiden och vilka som den då varit i kontakt med. Det ska dock understrykas att den information som chattjänsten kan bidra med inte omfattas av lagringsskyldigheten. Den här nyttan av uppgifterna gäller förstås inte bara i förhållande till chattjänster och sexualbrott mot barn. Även i andra fall kan det vara viktigt att kunna sammankoppla tid för internetåtkomst eller användande av en ip-adress med brottsliga aktiviteter som begåtts över internet.

Precis som vid telefonitjänst och meddelandehantering blir uppgiften om internetåtkomst betydligt mindre nyttig om det inte finns någon tid kopplad till den. Genom tidsuppgiften kan bl.a. kommunikationsmönster och i viss mån vanor i vardagen analyseras.

I sammanhanget ska emellertid noteras att nyttan, med undantag för möjligheten att göra ip-spårningar, begränsas av att många användare i princip har en ständig uppkoppling mot internet. Kommunikationsutrustningar, såsom en laptop, är ofta uppkopplade mot internet genom en privat router med trådlöst nätverk, som i sin tur är kopplat till ett modem med fast nätanslutning. Tidpunkten för när just laptopen kopplade upp sig mot internet kommer då inte att lagras. Vid användning av fast internetanslutning är det således vanskligt att ens indirekt genom uppgifter om på- och avloggningstid få fram några tidpunkter för när en viss aktivitet på internet ägde rum. Vad gäller datorer och mobiltelefoner som kopplar upp sig direkt mot internet (och inte via ett privat trådlöst nätverk) är internetsessionerna kortare.

För mobil uppkoppling blir tidsuppgifterna särskilt viktiga. Eftersom utrustningen kopplar upp sig direkt mot en cell (mast) lagras en lokaliseringsuppgift vid internetåtkomsten, se avsnittet strax nedan. För att den lokaliseringsuppgiften ska medföra någon större nytta krävs att det finns en tidsuppgift kopplad till den. Det är också nödvändigt för att uppgiften ska vara tillgänglig vid en basstationstömning. Då begärs det ut uppgifter om vilka uppkopplingar som gjorts mot en viss cell under en specifik tidsperiod.

Vidare måste någon form av tidsuppgift lagras för att operatören ska veta när lagringstiden för uppgiften har gått ut och uppgiften ska förstöras.

Av vad som framkommit är nyttan av tidsuppgifter för på- och avloggning i tjänsten som ger internetåtkomst mycket stor, i synnerhet såvitt avser ip-spårning. Utan uppgifter om tid blir den övriga lagringen av uppgifter om internetåtkomst betydligt mindre nyttig. Uppgifterna är sedda för sig själva inte särskilt integritetskänsliga, eftersom de inte ger någon information om hur användaren har brukat internet, utan endast om vilken tid som abonnenten haft internetåtkomst. Den informationen kan visserligen säga något om en persons kommunikationsmönster, men som nämnts ovan är det vanskligt att dra några säkra slutsatser, eftersom internetsessionerna inte behöver korrespondera mot användandet av internet. Därutöver har uppgifterna ett visst skyddsvärde, eftersom de tillsammans med annan information möjliggör att en ip-adress kan sammankopplas med en abonnent. Sammantaget bedömer utredningen uppgifterna som strängt nödvändiga att lagra. Uppgifterna ska därför fortfarande omfattas av lagringsskyldigheten.

Lagring av uppgifter som identifierar utrustning där kommunikationen avskiljs

Utredningen föreslår att uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilde abonnenten ska omfattas av lagringsskyldigheten. Denna utrustning är den sista punkten som den lagringsskyldige ansvarar för. Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten inte är lagringsskyldig ska det i stället lagras uppgifter som identifierar utrustningen vid den punkt där kommunikationen avskiljs till den som slutligt avskiljer kommunikationen till den enskilda abonnenten. Bestämmelsen gäller alltså punkten mellan å ena sidan det sista i kedjan av nät som ägs av någon som omfattas av lagringsskyldigheten och å andra sidan ett nät som inte omfattas av lagringsskyldigheten.

Den utrustning som finns där kommunikationen slutligt avskiljs kan vid fast internetförbindelse vara t.ex. ett fibermodem, ett telefonjack eller en router. Det lär då oftast vara utrustningens identifieringsnummer, t.ex. MAC-nummer, som lagras. Vid mobil internet-

åtkomst torde den sista utrustningen oftast vara en viss cell i en basstation. Uppgifterna motsvarar då de uppgifter som lagras för lokalisering vid telefonitjänst (prop. 2010/11:46 s. 33).

Uppgifterna är viktiga för att kunna hitta den geografiska plats som användaren kommunicerar från. Värdet av lokaliseringsuppgifter har beskrivits i avsnitt 12.6.3. Eftersom det blir allt vanligare med samtals- och meddelandekommunikation genom appar och tjänster från leverantörer som inte omfattas av lagringsskyldigheten (avsnitt 7.3.1) blir uppgifterna hänförliga till internetåtkomst ännu viktigare än tidigare.

Internetåtkomst är inte bara kopplat till webbesök, samtal och meddelanden; fler och fler maskiner och fordon behöver åtkomst till internet (7.3.4). I hemmet är de flesta uppkopplade produkter anslutna genom samma internetmodem som används för datorer och annan kommunikationsutrustning. De genererar därmed som regel inte några ytterligare uppgifter som lagras. Uppkopplade fordon däremot begär internetåtkomst genom en egen mobil uppkoppling. Vid en mer utbredd användning av internet i fordon skulle det därmed kunna bli möjligt att dra än mer långtgående slutsatser om folks privatliv, om uppgifterna lagras. Det skulle självklart bli till stor nytta för de brottsbekämpande myndigheterna om de kan få tillgång till uppgifter om var ett fordon ansluter till eller kopplar från internet. Men det skulle också innebära ett stort integritetsintrång. Lagringen skulle därigenom kunna bidra till att rörelsefriheten (2 kap. 8 § RF) i praktiken inskränks. Sammanfattningsvis finns det vissa betänkligheter med att låta dessa uppgifter lagras, om fordon i framtiden kommer att använda internet i större omfattning, i vart fall utan någon begränsning.

Uppgifterna används också för att säkra uppgifter om hela kommunikationskedjan, då främst enligt bestämmelsen i 43 § andra stycket FEK. Det är inte ovanligt att kommunikationskedjan sista del är ett nät som inte omfattas av lagringsskyldigheten, t.ex. en bostadsrättsförenings egna nät. De punkter där kommunikationen avskiljs är viktiga att få information om för att kunna gå till nätägaren för att få ytterligare uppgifter som kan leda fram till abonnenten. För att bestämmelserna ska bli meningsfulla och oberoende av infra- och bolagsstrukturella lösningar bör lagringsskyldigheten därför även omfatta uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs mellan den lagringsskyldige och den

som slutligt avskiljer kommunikationen till den enskilde abonnenten, om den senare inte är lagringsskyldig.

Sammanfattningsvis är de nu diskuterade uppgifterna i många fall nödvändiga för att hitta rätt slutanvändare, vilket gör dem viktiga. De är också nyttiga för att de i någon mån gör bestämmelserna om lagring av kommunikation mer teknikneutrala och anpassade till dagens teknik och användning av kommunikationstjänster. Uppgifterna är således strängt nödvändiga att lagra. Samtidigt innebär uppgifterna, i vart fall vid mobil internetåtkomst, ett relativt stort integritetsintrång, eftersom de i praktiken utgör lokaliseringsuppgifter. Intrånget är emellertid mindre än vid telefonitjänst och meddelandehantering, eftersom det inte finns någon korresponderande uppgift om t.ex. vem som personen kommunicerat med eller när kommunikationen ägt rum. Vid en sammantagen bedömning är det därför ändå proportionellt att uppgifterna lagras. Det ska emellertid noteras att om användandet av internet i fordon blir mer omfattande och mer utbrett kan det finnas anledning att göra en annan bedömning och införa någon form av begränsning i lagringen.

Kapacitet för överföring av internetåtkomst ska inte lagras

Utredningen föreslår att uppgift om den typ av kapacitet för överföring som har använts ska tas bort från lagringsskyldigheten.

Information om kapacitet för överföring vid internetåtkomst har i jämförelse med andra uppgifter värderats lägre av de brottsbekämpande myndigheterna. Uppgiften har även tidigare bedömts som mindre viktiga men bra att ha vid brottsbekämpning, Ds 2014:23 s. 52 (se dock SOU 2015:31 s. 166–167).

Som skäl för att behålla lagringsskyldigheten för uppgifterna har angetts att uppgifterna ger information om huruvida anslutningsformen är fast eller mobil, vilket i sig kan ge lokaliseringsinformation och uppgift om vem som är abonnent. Vidare har angetts att uppgiften kan vara av intresse för att verkställa andra hemliga tvångsmedel.

Uppgiften torde främst vara relevant för att enklare kunna identifiera rätt anslutning när kommunikationen övergår i ett nät som tillhandahålls av någon som inte är lagringsskyldig, t.ex. ett lokalt nät

för en bostadsrättsförening. Något omfattande behov av uppgiften har emellertid inte framkommit.

Uppgifterna bedöms inte som särskilt integritetskänsliga.

Sammantaget är utredningens bedömning att det inte är strängt nödvändigt att behålla lagringsskyldigheten för uppgift om den typ av kapacitet för överföring som har använts.

Bestämmelsen blir teknikneutral

Utredningen föreslår att uppgift som är nödvändig för att identifiera abonnent och registrerad användare ska omfattas av lagringsskyldigheten.

Möjligheten att koppla en användare till en viss uppgift bör inte skilja sig åt beroende på vilken teknik en operatör använder sig av. Som uppmärksammades i Datalagringsutredningens betänkande, påverkar användandet av NAT-teknik (dvs. en teknik för att låta flera användare dela på en och samma publika ip-adress) om de brottsbekämpande myndigheterna kan identifiera den slutliga användaren eller inte (SOU 2015:31 s. 320). Detta framstår som orimligt och även oavsiktligt, se prop. 2010/11:46, särskilt s. 30. Lagstiftningen bör i stället vara teknikneutral. Även om en sådan förändring inte är omedelbart föranledd av EU-domstolens dom har den ett sådant samband med övriga föreslagna förändringar att den bör genomföras samtidigt. Det bör således införas en skyldighet att lagra uppgifter som gör det möjligt att identifiera en abonnent.[11] En mer teknikneutral bestämmelse är även rimlig med beaktande av att det aktuella teknikområdet är under konstant metamorfos och alltför specifika bestämmelser riskerar att snabbt bli inaktuella, SOU 2007:76 s. 137.

Det har tidigare i detta betänkande anförts att en utvidgning av lagringsskyldigheten inte ligger i linje med bedömningen att färre uppgifter måste omfattas av en lagringsskyldighet för att den alls ska vara förenlig med EU-rätten (se t.ex. angående lokaliseringsuppgifter vid meddelandehantering, avsnitt 12.6.3). Den nu aktuella ändringen av lagringsskyldigheten kan visserligen föranleda att fler uppgifter lagras (om leverantörens teknik så kräver), men skiljer sig ändå

[11] Se även den av PTS beställda rapporten från ÅF: NAT i mobila nätverk, 23 november 2015.

markant från en utvidgning av det slag som avses i föregående mening. De ytterligare uppgifter som eventuellt behöver lagras avser nämligen samma sakförhållande och krävs för att huvudinformationen (ip-adressen) inte ska vara värdelös. Den begränsning som dagens lagstiftning leder till är, som nämnts ovan, oavsedd och föranledd av att operatörerna nu använder sig av en viss teknik. Av samma anledning ökar inte integritetsintrånget i sig särskilt mycket av att dessa uppgifter lagras. De extra uppgifter som behöver lagras torde oftast vara portnummer och ytterligare en ip-adress.

En teknikneutral bestämmelse har fördelar även utifrån den lagringsskyldiges perspektiv, eftersom det blir tydligt att det finns en skyldighet att lagra uppgifter som möjliggör identifikation av abonnenten. Nackdelen är dock att lagringsskyldighetens exakta omfattning inte går att utläsa direkt ur författning. Eftersom det är fråga om ett offentligrättsligt åliggande gentemot de lagringsskyldiga kan det finnas en poäng i att mer tydligt ange exakt vad som ska lagras. Eftersom den tekniska utvecklingen snabbt kan förändra förutsättningarna för vad som behöver lagras bör den exakta tekniska utformningen av lagringsskyldigheten fastställas i myndighetsföreskrifter. Ramarna av föreskriftsrätten bör dock alltjämt finnas i lag och förordning.

Enligt utredningen bör PTS vara den myndighet som utformar de tekniska detaljerna för vad som ska lagras. Ett sådant bemyndigande torde PTS redan ha, 6 kap. 16 a § fjärde stycket LEK och 44 § FEK. Detta bemyndigande bör dock förtydligas (se avsnitt 12.6.6).

Man kan förmoda att ipv6-adresser kommer att bli vanligare framöver. Ipv6 är en senare version av internetprotokollet, som gör det möjligt att använda 128 bitar långa ip-adresser, vilket möjliggör omkring 340 sextiljoner ($3{,}4 \cdot 10^{38}$) unika adresser. Det skulle innebära att användandet av NAT-teknik, utifrån brist på ip-adresser som enda grund, blir obehövligt. Däremot kan det ändå finnas anledning för operatörerna att fortsätta att använda tekniken. Om endast ipv6-adresser används borde någon annan uppgift än ip-adress och tillhörande uppgift om abonnent inte behöva lagras för att det ska vara möjligt att identifiera rätt abonnent eller registrerad användare. Det lär emellertid inte bli verklighet inom överskådlig framtid (Europols rapport IOCTA 2016, Internet Organised Crime Threat Assessment, s. 58).

Slutligen ska nämnas att lagring av destinations-ip, dvs. den adress som användaren kontaktat, vilket t.ex. kan vara en webbsida eller en mail-, chatt- eller spelserver, skulle kunna användas för att identifiera rätt användare vid användning av NAT-teknik. Lagras den uppgiften och tiden för kontakten begränsas nämligen antalet användare till dem med samma publika ip-adress som samtidigt haft kontakt med samma destinations-ip (t.ex. besökt samma webbsida). En sådan lagring skulle innebära ett alltför stort integritetsintrång, eftersom en användares trafik över internet skulle finnas lagrad och tillgänglig. I linje med att innehållet av kommunikationen inte ska lagras bör därför inte heller sådan information tillåtas att lagras för att uppfylla lagringsskyldigheten i denna del.

12.6.5 Inget undantag för personer med tystnadsplikt

Utredningens bedömning: Det bör inte införas något undantag från lagringen för personer med tystnadsplikt. Datalagringsutredningens förslag om att införa en förstörandeskyldighet för uppgifter som omfattas av yrkesmässig tystnadsplikt bör övervägas.

EU-domstolen noterar i domen att den svenska lagstiftningen inte innehåller något undantag för personer vilkas kommunikationer enligt nationell rätt omfattas av tystnadsplikt (p. 105, jfr även Digital Rights-domen p. 58). Däremot uppställer inte domstolen något krav på en sådan begränsning av lagringsskyldigheten.

Som Datalagringsutredningen konstaterade (se avsnitt 8.4.3) är det i svensk rätt huvudsakligen uppgiftens innehåll som avgör om den omfattas av skydd mot att de brottsbekämpande myndigheterna eller någon annan tar del av uppgiften. Förekomsten av kommunikation är däremot normalt inte skyddad. Tystnadsplikten omfattar inte heller vissa personer utan endast uppgifter som personerna fått del av i sin yrkesutövning (jfr 36 kap. 5 § RB, se även rättsfallet NJA 2010 s. 122, särskilt punkten 8). Ett förbud mot att lagra eller hämta in uppgifter som enligt svensk rätt omfattas av tystnadsplikt skulle därför kräva att man tar del av innehållet i kommunikationen, vilket framstår som ogörligt, både praktiskt och utifrån ett integritetsperspektiv. Ett förbud mot att lagra uppgifter av nu aktuellt slag

skulle alltså innebära ett ökat integritetsintrång samtidigt som det inte är något som krävs enligt EU-rätten.

I vissa fall kan redan det faktum att det förevarit en kontakt mellan en person med tystnadsplikt och någon annan vara känsligt. Exempel på det kan vara kontakter med advokater, läkare eller präster. I detta sammanhang måste följande beaktas. För det första innehåller samtliga brottsbekämpande myndigheternas datalagar ett ramverk kring hur personuppgifter får behandlas, se polisdatalagen (2010:361), åklagardatalagen (2015:433) och tullbrottsdatalagen (2017:447). Det ger ett skydd för att uppgifter där behandlas korrekt, gallras om de inte behövs och inte sprids. För det andra skulle det vara en administrativt svår uppgift att ha ett system för att undanta vissa abonnenter från operatörernas lagringsskyldighet. Även om en sådan ordning skulle kunna införas är det ändå inte önskvärt att göra så. Skälet till det är att även advokater, läkare och präster kan misstänkas för brott. När de uppträder som brottsmisstänkta har de i princip ingen privilegierad ställning. Det är dock viktigt att notera att tystnadsplikten till förmån för klienten alltjämt gäller.

Mot bakgrund av det nu anförda lämnar utredningen inget förslag på något undantag för personer med tystnadsplikt. Bedömningen om en uppgift ska inhämtas från en person vars uppgifter kan omfattas av tystnadsplikt bör i stället göras i varje enskilt fall med utgångspunkt i proportionalitetsprincipen (jfr även prop. 1988/89:124 s. 28 och NJA 2015 s. 631 p. 29).

I sammanhanget bör även påpekas att det råder ett grundlagsskyddat förbud för det allmänna att efterforska vem som lämnat uppgifter till t.ex. en journalist (3 kap. 4 § tryckfrihetsförordningen och 2 kap. 4 § yttrandefrihetsgrundlagen). Utredningen instämmer i Datalagringsutredningens bedömning att endast förekomsten av strukturerad data eller ens inhämtning av uppgifterna inte kan leda till att efterforskningsförbudet överträds, om det inte funnits ett syfte att efterforska en källa. Samtidigt delar utredningen slutsatsen att myndigheternas insyn i att kommunikation förevarit i någon mån kan riskera att hota meddelarskyddet eller sekretessen. Även om innehållet i informationen inte direkt framgår av de uppgifter som ska lagras, kan den som får tillgång till uppgifterna dra slutsatser och göra kvalificerade gissningar om sekretessbelagd information utifrån både lokaliseringsuppgifter, exempelvis vilka som varit på en viss klinik, och trafikuppgifter, t.ex. en journalists, advokats eller utredande polis

samtalslista. Datalagringsutredningens förslag om en skyldighet att förstöra uppteckningar från hemlig övervakning av elektronisk kommunikation och inhämtning enligt IHL i de delar de innehåller uppgifter som omfattas av frågeförbudet i 36 kap. 5 § andra–sjätte styckena RB bör därför övervägas. Det ska dock i sammanhanget noteras att en sådan skyldighet är behäftad med vissa svårigheter. Som Ekobrottsmyndigheten anför i sitt remissvar över Datalagringsutredningens betänkande SOU 2015:31 så är frågeförbudet i vissa fall (t.ex. när det gäller advokater och läkare) utformat på så sätt att det avser vad som har ”anförtrotts” befattningshavaren i sin yrkesutövning, eller vad han eller hon i samband därmed har ”erfarit” I fråga om rättegångsombud, biträden och försvarare gäller dock frågeförbudet endast vad som har ”anförtrotts” dem, och alltså inte vad de har ”erfarit”. Det är svårt att se hur det ska vara möjligt att – när det gäller just trafikuppgifter – bedöma vad som ska anses ha anförtrotts t.ex. en advokat under ett samtal. Därtill kan det finnas en rättssäkerhetsproblematik med att uppgifter som inhämtats av en brottsbekämpande myndighet raderas efter att de analyserats. Även i denna del hänvisas till vad som anförs i remissyttranden över Datalagringsutredningens betänkande från Ekobrottsmyndigheten, Polismyndigheten och Säkerhetspolisen.

12.6.6 Lagringskyldighetens ramar bör framgå av lag

Utredningens bedömning: Lagringsskyldighetens yttre ramar bör framgå av lag och de mer detaljerade föreskrifterna av förordning. I viss utsträckning ska regeringen kunna delegera denna föreskriftsrätt.

Som ovan beskrivits är området för elektronisk kommunikation i ständig förändring med nya kommunikationstjänster som tillkommer. Dessa nya kommunikationstjänster leder till nya kommunikationsmönster hos användarna (avsnitt 7.3). Det leder i sin tur till att bedömningen av vad som är strängt nödvändigt att lagra kan förändras över tid (avsnitt 12.6.3). Sådana förändringar kan komma snabbt och regelverket kring lagringsskyldigheten måste därför kunna ändras snabbt, dels för att människor inte ska utsättas för lagring som inte längre är strängt nödvändig, dels för att de brotts-

bekämpande myndigheterna måste kunna bibehålla sin brottsutredande förmåga även vid teknisk utveckling. Av dessa skäl bör riksdagen i lag föreskriva de yttre ramarna för lagringen medan de mer detaljerade föreskrifterna huvudsakligen bör regleras i förordning. Det gör att även om många uppgifter nu tas bort från lagringsskyldigheten så bör ramarna för lagringen i LEK inte ändras mer än nödvändigt.

När det gäller lagring av abonnemangsuppgifter vid internetåtkomst kräver föreskrifternas utformning särskilt god och aktuell kunskap om tekniska lösningar hos operatörerna. Det är därför lämpligt att regeringen får rätt att delegera föreskriftsrätten till PTS i dessa fall, jfr 6 kap. 16 a § fjärde stycket LEK. Ett förtydligande om PTS behörighet kan därför behöva göras (avsnitt 12.6.4).

12.7 En differentierad lagringstid

Utredningens förslag: Det ska i lag anges att de uppgifter som omfattas av lagringsskyldigheten ska lagras den tid regeringen föreskriver dock som längst i tio månader räknat från den dag då kommunikationen avslutades.

Lokaliseringsuppgifter vid samtal ska lagras i två månader. Uppgifter om internetåtkomst, förutom uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs, ska lagras i tio månader. Övriga uppgifter ska lagras i sex månader.

12.7.1 Riksdagen ger en ram för lagringstiden

Som framgår ovan måste lagringen vara anpassad till vad som är strängt nödvändigt. En viktig komponent i en sådan anpassning är att differentiera lagringstiderna utifrån hur gamla uppgifter det finns ett påtagligt behov av. Som nämnts tidigare, är en differentiering av lagringstiderna emellertid ensamt inte en tillräcklig åtgärd för att göra den svenska lagstiftningen förenlig med EU-rätten.

Utredningen föreslår att det skapas en flexibel ordning där riksdagen i lag föreskriver en längsta lagringsfrist och att regeringen inom denna ram får föreskriva kortare lagringsfrister. Härigenom differentieras lagringsskyldigheten för respektive uppgiftsslag.

12.7.2 Inom den av riksdagen angivna ramen bör regeringen föreskriva kortare frister för vissa uppgifter

Utredningen föreslår att lokaliseringsuppgifter vid samtal ska lagras i två månader. Uppgifter om internetåtkomst, förutom uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs, ska lagras i tio månader och övriga uppgifter ska lagras i sex månader.

De uppgifter om elektronisk kommunikation som inhämtas av polisen i underrättelseverksamheten är i de flesta fall yngre än en månad. I polisens utredningsverksamhet är den största andelen yngre än tre månader, endast omkring 20–25 procent är äldre och ungefär en tiondel av den totala mängden är äldre än fem månader. De utredningar i vilka det finns ett behov av äldre uppgifter avser främst grova våldsbrott av spaningskaraktär samt bekämpning av grova seriebrott som våldtäkter och mordförsök. (SOU 2015:31 s. 129) Detta bör beaktas vid bestämmandet av lagringstiden. En annan faktor att beakta är att – som framgår av avsnitt 7.5 – de brottsbekämpande myndigheterna har behov av längre lagringstid för ip-adresser vid ärenden som har internationell koppling, t.ex. barnpornografibrott.

Ytterligare en utgångspunkt vid dessa resonemang är att datalagringsdirektivet ålade medlemsstaterna att i en viss tid se till att uppgifter skulle lagras. Denna tid för lagring överläts till medlemsstaterna att bestämma men skulle ligga i intervallet sex till tjugofyra månader räknat från dagen för kommunikationen. Sverige valde den kortaste tiden för lagring, dvs. sex månader.

Som framgår ovan är de flesta uppgifterna som inhämtas i polisens verksamhet yngre än fem månader. Tullverkets verksamhet torde inte kräva några särskilt annorlunda lagringstider, vilket också stämmer med vad Tullverket har uppgett. Det talar för att man inte behöver föreskriva en lagringstid som överskrider fem månader. Samtidigt måste några andra viktiga faktorer beaktas. När nu lagringsskyldighetens omfattning sett till vilka uppgifter som ska lagras minskar så minskar nyttan av tillgång till de datalagrade uppgifterna. Denna minskade omfattning av lagringen kan leda till att kartläggningen av elektroniska spår i brottsutredningar blir något långsammare. Dessutom – och kanske viktigare – är det, som framgår ovan, framför allt vid bekämpning av grova brott som de äldre uppgifterna behövs. I underrättelseverksamheten är behovet av äldre

uppgifter inte särskilt stort, möjligen med undantag av vissa delar av Säkerhetspolisens verksamhet.

Mot bakgrund av det sagda bör lagringstiden alltjämt som huvudregel vara sex månader. De allra flesta uppgifterna för telefonitjänst och meddelandehantering bör omfattas av huvudregeln. Vad gäller lokaliseringsuppgifter bör dock lagringstiden vara betydligt kortare.

Lokaliseringsuppgifter kan potentiellt ge mer integritetskänslig information om en person än övriga uppgifter. En kortare lagringstid bör därför föreskrivas för dessa uppgifter. Enligt den tyska lagstiftningen gäller en lagringsskyldighet för lokaliseringsuppgifter i fyra veckor. Det är dock svårt att jämföra en viss rättsordning med den svenska och utifrån det göra bedömningar om hur det ska vara här. Lagringsskyldighetens längd är nämligen en del i en helhet där bl.a. den övriga regleringen kring tvångsmedel spelar in. Med detta sagt är det emellertid klart att det bör införas en kortare lagringsskyldighet för lokaliseringsuppgifter än för andra uppgifter. En rimlig avvägning mellan den nytta uppgifterna innebär för de brottsbekämpande myndigheterna och det integritetsintrång uppgiften innebär ger enligt utredningen att en lagringstid om två månader bör föreskrivas för lokaliseringsuppgifter.

Uppgifter för den första aktiveringen av en förbetald anonym tjänst bör behandlas som en enhet, dvs. även inkluderat lokaliseringsuppgiften. Uppgifterna är inte särskilt integritetskänsliga. Det finns ett behov hos de brottsbekämpande myndigheterna att få tillgång till i vart fall sex månader gamla uppgifter, avsnitt 7.5. Någon bärande anledning att lagra uppgifterna längre än huvudregeln om sex månader har inte framkommit.

De flesta uppgifter kopplade till internetåtkomst är mindre integritetskänsliga eftersom de i sig inte innefattar uppgifter om kommunikation (t.ex. vem internetanvändaren har haft kontakt med). Myndigheterna har – liksom vid övriga uppgifter – olika behov av dessa uppgifter. Polismyndigheten står för den absolut största delen av brottsbekämpningen varför lagringstiden främst bör anpassas till den. Som nämnts i avsnitt 7.5 är det flera av polisens utredningar som behöver läggas ned på grund av att lagringstiden om sex månader är för kort när det gäller ip-adresser, eftersom dessa uppgifter ofta är helt avgörande för att kunna identifiera misstänkta gärningsmän. Uppgifter om ip-adresser (och andra uppgifter som krävs för att identifiera abonnenten) ger också ett tidsbegränsat användnings-

område, eftersom uppgifterna ofta byts ut med korta mellanrum (avsnitt 12.6.4). Det leder både till att uppgifternas integritetskänslighet är lägre än annars och att det finns ett större behov av att spara uppgifterna en längre tid. Övriga uppgifter om internetåtkomst krävs för att öka förståelsen och nyttan av de lagrade ip-uppgifterna. Utredningen finner att en lagringstid om tio månader för uppgifter hänförliga till internetåtkomst (förutom uppgifter som identifierar utrustningen, se nedan) utgör en rimlig avvägning mellan de olika myndigheternas behov samtidigt som hänsyn tas till integritetsaspekten.

När det gäller uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten, är de uppgifterna mer integritetskänsliga än övriga uppgifter om internetåtkomst eftersom uppgifterna i princip utgör en lokaliseringsuppgift. I vart fall gäller det vid mobil åtkomst till internet. Även om dessa uppgifter inte har samband med någon kommunikation och därför inte är lika integritetskänsliga som lagrade lokaliseringsuppgifter för telefonitjänst, får de alltså anses mer känsliga än övriga uppgifter. En kortare lagringstid än tio månader bör därför föreskrivas. Sådana uppgifter bör i stället sparas i sex månader.

12.8 Tillgången till trafik- och lokaliseringsuppgifter

12.8.1 Endast för att bekämpa grov brottslighet

Utredningens bedömning: Tillgång till lagrade trafik- och lokaliseringsuppgifter ska endast ges för bekämpning av grov brottslighet. Med grov brottslighet avses samma kategorier av brott som i dag möjliggör hemlig övervakning av elektronisk kommunikation i en förundersökning, för att förhindra vissa särskilt allvarliga brott och för särskild utlänningskontroll samt inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Som anges ovan menar EU-domstolen att endast bekämpning av grov brottslighet[12] kan motivera att brottsbekämpande myndigheter ges tillgång till lagrade uppgifter (avsnitt 9.8.1).

Det finns inte någon generell definition av grov brottslighet inom EU-rätten eller inom svensk rätt. Däremot förekommer i olika sammanhang, både i EU-rätten och i svensk rätt, uppräkningar av brott som – i det sammanhanget uppräkningen förekommer – ska jämställas med grova brott eller som på annat sätt ska särbehandlas. Ett exempel på en sådan uppräkning är bilagan till lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder. I den bilagan finns angivet brott som spänner över en stor del av straffskalan; från mord och våldtäkt till förfalskning, piratkopiering och barnpornografi. Just denna uppräkning har rådet uppmanat medlemsstaterna att ta ”vederbörlig hänsyn” till vid införandet av det numera upphävda datalagringsdirektivet (prop. 2010/11:46 s. 21).

Inom EU-lagstiftningen finns ytterligare exempel. I Europaparlamentets och rådets direktiv 2016/681 av den 27 april 2016 (direktivet om PNR-uppgifter) definieras grov brottslighet som brott som anges i direktivets bilaga vilka kan leda till fängelse i minst tre år enligt en medlemsstats nationella rätt, artikel 3.9. De brott som finns med i bilagan är inte identiska men i huvudsak desamma som i bilagan till lagen om överlämnande från Sverige enligt en europeisk arresteringsorder.

Ett exempel på en sådan uppräkning i svensk rätt är den som finns i bestämmelsen om när hemlig övervakning av elektronisk kommunikation är tillåten trots att det aktuella straffbudet inte innehåller straffminimum på minst sex månaders fängelse, 27 kap. 19 § RB. I den uppräkningen finns t.ex. narkotikabrott och barnpornografibrott.

Hemlig övervakning av elektronisk kommunikation kan förekomma även inom ramen för förhindrande av vissa särskilt allvarliga brott. De brott som kan berättiga till hemlig övervakning tillhör de absolut grövsta brotten i vårt samhälle, som t.ex. mord, terroristbrott och spioneri, 1 § lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott.

[12] Det kan noteras att den svenska språkversionen av domen varierar mellan ”grov brottslighet” och ”allvarligt brott” medan de engelska och franska språkversionerna är mer konsekventa i sin respektive begreppsanvändning (”serious crime” och ”criminalité grave”).

Ytterligare ett annat exempel förekommer i IHL. Inhämtning enligt IHL kräver som utgångspunkt att det är fråga om brottslig verksamhet som innefattar brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Härutöver finns en uppräkning av vissa brott inom främst Säkerhetspolisens verksamhetsområde som t.ex. spionerі och brott mot medborgerlig frihet, 3 § IHL.

Enligt LSU finns möjligheter att tillgripa hemlig övervakning av elektronisk kommunikation vid misstankar om medverkan till terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott eller försök, förberedelse eller stämpling till sådant brott.

Den brottslighet som omfattas av de ovan uppräknade tvångsmedelslagarna har lagstiftaren ansett vara så grova att utredningsintresset av den väger tyngre än det integritetsintrång som drabbar dem som blir föremål för tvångsmedlet. Inget i avgörandet från EU-domstolen ger anledning att tro att de avvägningar som gjorts beträffande detta måste rubbas.

Mot bakgrund av det nu anförda är utredningens bedömning att de brott som ger rätt att använda tvångsmedel enligt RB, IHL, 2007 års preventivlag och LSU är att betrakta som grov brottslighet. Det ska i detta sammanhang nämnas att regeringen och riksdagen nyligen – och alltså efter Tele2-domen – har ansett att unionsrätten inte hindrar en förlängning av den tidsbegränsade bestämmelsen i 3 § IHL och att domen måste anses innebära att det finns ett utrymme för att hämta in uppgifter för att förebygga, förhindra eller upptäcka sådan brottslig verksamhet som avses i paragrafen, prop. 2016/17:186 s. 9, bet. 2016/17:JuU28 och rskr. 2016/17:343.

12.8.2 Precisa krav måste fastställas

Utredningens bedömning: Reglerna som styr tillgången till de lagrade uppgifterna för de brottsbekämpande myndigheterna måste ange tydliga och precisa villkor för när tillgång ska ges.

Enligt EU-domstolen måste medlemsstaterna föreskriva klara och precisa bestämmelser som anger under vilka omständigheter och på vilka villkor leverantörer av elektroniska kommunikationstjänster måste ge behöriga nationella myndigheter tillgång till uppgifterna (avsnitt 9.8.2). Både materiella och formella villkor för de behöriga

nationella myndigheternas tillgång till de lagrade uppgifterna måste anges i den nationella lagstiftningen.

Detta krav som EU-domstolen uppställer är inte möjligt att resonera kring självständigt; i stället måste man vid utformningen av respektive lagrum se till att kravet möts.

12.8.3 Tillgång bara till uppgifter om personer som på något sätt är inblandade i brott – som huvudregel

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

Inledningsvis kan noteras att det i sig inte är tillräckligt att det finns en indirekt koppling till bekämpning av allvarlig brottslighet för att myndigheterna ska få tillgång till uppgifterna. Det krävs, som huvudregel, att personen på något sätt är inblandad i den allvarliga brottsligheten. Domstolen beskriver denna personkrets, för vilka uppgifter kan inhämtas, med de exakta orden som används av Europadomstolen i målet Roman Zakharov mot Ryssland, 4 december 2015, som EU-domstolen hänvisar till. Därtill lägger domstolen ”på något sätt inblandad”[13], vilket alltså innebär att personkretsen är vidare än endast misstänkta gärningsmän och medhjälpare. Detta stöds även av att Europadomstolen i samma dom (§ 245), med hänvisning till tidigare praxis, konstaterade att det kan vara berättigat med en hemlig övervakningsåtgärd även mot en person som kan ha upplysningar om ett brott, utan att vara misstänkt. I begreppet måste t.ex. även en målsägande ingå. Eftersom en hänvisning görs till Europadomstolens praxis torde dock begreppet vara vidare än så. I Greuter mot Nederländerna, 19 mars 2002, som hänvisades till från Roman Zakharov mot Ryssland (§ 245), bedömdes det nämligen

[13] “being implicated in one way or another in such a crime” i den engelska versionen.

befogat att avlyssna en telefon tillhörande partnern till en dödad person, eftersom det fanns misstankar om att gärningsmannen skulle kunna kontakta henne.

I särskilda fall kan det, enligt EU-domstolen, vara befogat att ge myndigheterna tillgång även till andra personers uppgifter. Det bör särskilt noteras att det uppenbarligen inte endast är när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism som tillgång kan beviljas till uppgifter som rör personer som inte är inblandade i ett allvarligt brott. Av domstolens formulering framgår att det endast är fråga om ett exempel.[14]

Vad avser personer med tystnadsplikt bör inte något specifikt undantag göras avseende tillgången till dessa personers uppgifter. I denna del hänvisas till vad som anförs i avsnitt 12.6.5.

Hemlig övervakning av elektronisk kommunikation

Utredningens bedömning: Nuvarande tillgångsregler i RB uppfyller de krav som EU-rätten ställer.

Huvudsakligen beviljas åtkomst till lagrade uppgifter vid hemlig övervakning endast avseende misstänkta personer (27 kap. 20 § första stycket 1 RB). I de fall övervakningen riktar sig mot ett telefonnummer som inte innehas eller har innehafts av den misstänkte så krävs att det föreligger synnerlig anledning att anta att den misstänkte kommer att kontakta eller har kontaktat det aktuella telefonnumret (27 kap. 20 § första stycket 2 RB). Även om den person som på detta sätt blir föremål för tvångsmedlet inte behöver ha något samröre med brottet så riktar sig det hemliga tvångsmedlet fortfarande mot den misstänkte. På ett principiellt plan skiljer sig således inte denna typ av övervakning från när man övervakar ett telefonnummer som tillhör den misstänkte eftersom man även i sådana fall fångar upp trafikuppgifter avseende personer som inte alls har med brottet att göra. För att minimera antalet trafikuppgifter som inte har med brottsutredningen att göra begränsas typiskt sett

[14] Detta framgår tydligt av den engelska versionen av Tele2-domen: ”access can, as a general rule, be granted […] However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities […]”.

ett tillstånd till nu nämnd övervakning till att endast avse inkommande samtal (prop. 2002/03:74 s. 38–39).

Som redogjorts för ovan tillåter EU-rätten i viss utsträckning övervakning även mot andra än misstänkta. Mot denna bakgrund gör utredningen bedömningen att den övervakning som regleras i 27 kap. 20 § första stycket är förenlig med de krav som EU-rätten uppställer.

Enligt 27 kap. 20 § andra stycket RB får hemlig övervakning av elektronisk kommunikation även utföras i syfte att utreda vem som skäligen kan misstänkas för ett brott om åtgärden är av synnerlig vikt för utredningen. För att tillstånd till sådan övervakning ska ges krävs att det är fråga om mycket allvarlig brottslighet med ett straffminimum på fängelse två år (27 kap. 19 § fjärde stycket RB).

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

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

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

domstolen ger är tillräckligt för att de svenska reglerna i detta hänseende ska lämnas oförändrade.

Reglerna om tillgång genom hemlig övervakning av elektronisk kommunikation är tydliga och precisa och uppfyller de krav som EU-rätten ställer.

Inhämtning av uppgifter i underrättelseverksamhet

Utredningens bedömning: Nuvarande tillgångsregler i IHL uppfyller de krav som EU-rätten ställer.

Som ovan beskrivits inhämtas uppgifter enligt IHL endast i underrättelseverksamhet. På det stadiet saknas kunskap om ett specifikt brott (avsnitt 6.2.4). Av naturliga skäl blir det därmed svårt att tala om någon ”misstänkt” person, i vart fall så som uttrycket används i RB.

Enligt EU-domstolen kan tillgång i princip bara beviljas, i samband med bekämpning av brott, till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott.

Även om underrättelseanalysen inte alltid kan peka ut ett specifikt brott eller en misstänkt person så inriktas underrättelsearbetet i någon mening mot en viss person när inhämtning ska göras av dennes uppgifter. Trots att denna person inte är misstänkt på sätt som avses i t.ex. 23 kap. 18 § RB så finns det i många fall en misstanke om att den person som är föremål för inhämtningen på något sätt är inblandad i den brottsliga verksamheten som underrättelseverksamheten avser. Det är i dessa fall dessutom inte möjligt att precisera personkretsen mer. Den svenska rätten får därmed anses uppfylla de villkor som nu har uppställts av EU-domstolen.

IHL tillåter emellertid även inhämtning av uppgifter avseende personer som inte är inblandade i brottslig verksamhet. Det ska då hållas i minne att, för att inhämtning ska få utföras, det krävs att åtgärden är av särskild vikt för syftet med inhämtningen och att brottet är av mycket allvarlig art (2 § IHL). I de fall brottsligheten avser sådant som utreds inom Säkerhetspolisens verksamhetsområde behöver dock inte brottsligheten vara av fullt så grovt slag, i vart fall om man ser till straffvärdet (3 § IHL). Däremot är samtliga dessa brott allvarliga med hänsyn till att de är samhällsfarliga. EU-dom-

stolens tolkning av rättighetsstadgan tillåter också en mer vidsträckt inhämtning i dessa fall (p. 119 i domen och avsnitt 9.8.3). Utredningen gör mot denna bakgrund bedömningen att regelverket i IHL i denna del inte står i strid med EU-rätten och därför kan behållas.

2007 års preventivlag

Utredningens bedömning: Nuvarande tillgångsregler i 2007 års preventivlag uppfyller de krav som EU-rätten ställer.

Som anges ovan får hemlig övervakning av elektronisk kommunikation enligt 2007 års preventivlag endast avse en teleadress som under den tid tillståndet omfattar innehas eller har innehafts av den som kan antas komma att utöva den brottsliga verksamheten, en teleadress som annars kan antas ha använts eller komma att användas av honom eller henne, eller en teleadress som det finns synnerlig anledning att anta att han eller hon under den tid tillståndet avser har kontaktat eller kommer att kontakta (avsnitt 6.2.5).

På samma sätt som tillgångsreglerna vid hemlig övervakning av elektronisk kommunikation bedöms förenliga med EU-rätten gör utredningen bedömningen att även 2007 års preventivlag uppfyller EU-rättens krav i detta hänseende.

LSU

Utredningens bedömning: Nuvarande tillgångsregler vid särskild utlänningskontroll uppfyller de krav som EU-rätten ställer.

Som framgår ovan får rätten meddela tillstånd till hemlig övervakning av elektronisk kommunikation om det är av betydelse för att utröna om den aktuella utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott och det finns synnerliga skäl (avsnitt 6.2.6).

På samma sätt som tillgångsreglerna vid hemlig övervakning av elektronisk kommunikation bedöms förenliga med EU-rätten gör

utredningen bedömningen att även LSU uppfyller EU-rättens krav i detta hänseende.

12.8.4 Förhandskontroll av domstol eller oberoende myndighet

Som framgår ovan ställer EU-rätten upp ett krav på att de brottsbekämpande myndigheternas tillgång till datalagrade uppgifter, utom i motiverade brådskande fall, ska föregås av en kontroll av domstol eller en oberoende myndighet (avsnitt 9.8.4).

Hemlig övervakning av elektronisk kommunikation

Utredningens bedömning: De svenska reglerna om förhandskontroll vid hemlig övervakning av elektronisk kommunikation uppfyller de krav som EU-rätten ställer.

Frågor om hemlig övervakning av elektronisk kommunikation prövas av rätten efter ansökan av en åklagare, 27 kap. 21 § RB. Om det kan befaras att det skulle medföra en fördröjning av väsentlig betydelse för utredningen att inhämta rättens tillstånd till hemlig övervakning av elektronisk kommunikation får tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut, 27 kap. 21 a § RB. Rätten ska därefter skyndsamt pröva ärendet och kan upphäva beslutet om den finner att det inte finns skäl för åtgärden.

Enligt utredningens bedömning lever det svenska regelverket på detta område upp till EU-rättens krav.

Inhämtning av uppgifter i underrättelseverksamhet

Utredningens förslag: Åklagare ska besluta om tillstånd för inhämtning av trafik- och lokaliseringsuppgifter i underrättelseverksamhet. Ansökan ska upprättas av Polismyndigheten, Säkerhetspolisen respektive Tullverket.

Utredningens bedömning: Besluten bör inte kunna överklagas. Inga interimistiska beslut bör tillåtas. Skyldigheten att omedel-

bart häva ett beslut som det inte längre finns skäl för bör alltjämt ankomma på Polismyndigheten, Säkerhetspolisen respektive Tullverket. Skyldigheten att underrätta SIN om ett beslut om inhämtning bör alltjämt ankomma på Polismyndigheten, Säkerhetspolisen respektive Tullverket.

Som framgår ovan får inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet beslutas utan förhandskontroll av domstol eller annan oberoende myndighet (avsnitt 6.2.4). Inhämtningen beslutas i stället av myndigheten själv.

EU-domstolens krav på att inhämtningen ska beslutas av en domstol eller en oberoende myndighet har uppenbarligen ett slags rättssäkerhetssyfte; en myndighet ska inte tillåtas att fatta beslut som är ingripande mot den enskilde samtidigt som beslutet underlättar myndighetens egen verksamhet. Oavsett hur korrekt än ett sådant beslut skulle vara skulle det kunna uppfattas som om myndigheten offrar den enskildes integritet för att kunna uppnå fördelar för den egna verksamheten.

Den nuvarande beslutsordningen i IHL innehåller andra rättssäkerhetsgarantier för att säkerställa att besluten fattas på riktiga grunder.

För det första följer det redan av lagtexten att ett beslut om inhämtning som utgångspunkt ska fattas av myndighetschefen och att dennes delegeringsmöjligheter är begränsade till sådana personer som har den särskilda kompetens, utbildning och erfarenhet som behövs. I förarbetena anges att beslutanderätten bör kunna delegeras endast till en tämligen begränsad skara. De som nämns är myndighetschefens ställföreträdare, rikskriminalchefen, biträdande rikskriminalchefen, biträdande säkerhetspolischefen, biträdande länspolismästare, länskriminalchefer, chefer för operativ verksamhet och chefer för underrättelseverksamhet (prop. 2011/12:55 s. 123). Redan det förhållandet att beslutsnivån finns tämligen högt upp i organisationen utgör i viss mån en garant för att besluten fattas på ett korrekt sätt.

För det andra, får den som har fått beslutanderätt delegerad till sig inte fatta beslut om inhämtning i sådan operativ verksamhet som han eller hon själv deltar i. Härigenom undviks jävssituationer.

Genom det ovan beskrivna skyddet mot felaktigt grundade beslut skulle det kunna argumenteras för att den svenska ordningen upp-

fyller de krav som EU-rätten ställer. Med beaktande av uttalandena i Tele2-domen och vad Europadomstolen uttalat i Roman Zakharov mot Ryssland, 4 december 2015, §§ 268-270, bör dock den ytterligare rättssäkerhetsgaranti som följer av att anförtro beslutsbehörigheten till en oberoende myndighet tas till vara. I detta sammanhang kan det vara värt att notera att SIN:s granskningar har visat att myndigheternas tillämpning av IHL i vissa fall är bristfällig. Som exempel på sådana brister kan nämnas inhämtning trots att det för angiven brottslighet inte var rättsligt möjligt med inhämtning[15] och inhämtning i strid med 5 § IHL av lokaliseringsuppgifter för en tid som överstigit en månad från dagen för besluten[16].

Utredningen bedömer mot bakgrund av det nu anförda att beslutsbehörigheten enligt IHL bör anförtros en domstol eller annan oberoende myndighet. Det ska härvid inledningsvis konstateras att den svenska förvaltningsmodellen gör att samtliga svenska myndigheter uppfyller kravet på oberoende. Av 12 kap. 2 § RF framgår nämligen att en myndighet inte får bestämma hur en annan förvaltningsmyndighet i ett särskilt fall ska besluta i ett ärende som rör myndighetsutövning mot en enskild.

Frågan är vilken myndighet som ska ha denna uppgift. Som framgår ovan övervägde Datalagringsutredningen om domstol, särskild nämnd eller åklagare skulle ha en roll vid beslutsfattandet enligt IHL (avsnitt 8.4.4). Datalagringsutredningen avfärdade samtliga alternativ. Utredningen delar i och för sig de argument som Datalagringsutredningen förde fram mot att involvera någon annan myndighet i beslutsprocessen men som ovan konstateras finns det ett rättssäkerhetskrav på att låta beslutsbefogenheten tillkomma en extern myndighet.

Domstolar bör inte fatta beslut enligt IHL

Som Datalagringsutredningen konstaterade och som redogörs för ovan finns det nackdelar med att låta domstolar ha en roll som beslutsorgan enligt IHL (avsnitt 8.4.4). De mest framträdande argumenten mot en domstolsinblandning, som också redovisas i förarbetena till

[15] Nämndens uttalanden den 14 september 2016, dnr 130-2016, och den 18 november 2015, dnr 169-2015.
[16] Nämndens uttalande den 16 mars 2016, dnr 206-2015.

IHL (prop. 2011/12:55 s. 88–89), är följande. Beslut enligt IHL fattas i underrättelseverksamhet, vilket gör att domstolsmiljön, som har kontradiktion som utgångspunkt, blir onaturlig. Underrättelseverksamheten är nämligen främst inriktad mot en företeelse till skillnad från förundersökningen, som inriktar sig mot en person (23 kap. 2 § RB). Även om beslutsfattande enligt 2007 års preventivlag ligger på domstolar så är underrättelseverksamhet typiskt sett främmande för domstolarna. Slutligen är inte domstolsväsendet ordnat på så sätt att det kan erbjuda det snabba beslutsfattande som kan behövas i ärenden enligt IHL. Enligt utredningen bör därför domstolar inte komma i fråga som beslutsorgan. Längre ner i detta avsnitt beskrivs ändå, för fullständighetens skull, hur en ordning med domstol som beslutsfattare skulle kunna vara utformad.

SIN bör inte fatta beslut enligt IHL

En myndighet som skulle kunna fatta beslut enligt IHL är SIN. Det finns dock två bärande argument mot en sådan ordning.

För det första är SIN tämligen långt ifrån att ha organisatoriskt nödvändig beredskap för att kunna fatta de snabba beslut som ibland behövs i underrättelseverksamhet.

För det andra har SIN i uppdrag att utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel, 1 § lag (2007:980) om tillsyn över viss brottsbekämpande verksamhet. Att anförtro beslutsfattandet till SIN samtidigt som nämnden skulle utöva tillsyn över verksamheten inger starka betänkligheter (jfr Europadomstolens dom Roman Zakharov mot Ryssland, 4 december 2015, § 280).

Mot bakgrund av det ovan nämnda bör SIN inte bli beslutsmyndighet enligt IHL.

Åklagare bör fatta beslut enligt IHL

Av redan existerande myndigheter är det enda rimliga kvarvarande alternativet åklagare. Åklagare utgör en central del i rättskedjan. Även om de främst är vana att agera under en förundersökning har de god vana att ta beslut om tvångsåtgärder och att göra bedömningar om i vilket skede (underrättelse- eller förundersöknings-

skedet) som ett ärende befinner sig i. Även viktiga bedömningar där effektivitet vägs mot integritet har en naturlig plats i åklagarens vardag. Av redan existerande myndigheter är det därför rimligt att överväga åklagare som beslutsfattare enligt IHL. Det finns emellertid en del viktiga argumentet även mot att involvera åklagare. Enligt utredningen är ett av de mest bärande argumenten mot detta att åklagare inte bör befatta sig med underrättelseverksamhet, eftersom det är artfrämmande för åklagarnas kärnverksamhet. Samtidigt kan det konstateras att åklagare redan i dag i olika författningar har ålagts vissa arbetsuppgifter som ligger utanför det brottsutredande området. Här kan nämnas beslut om förstörande enligt lagen (2011:111) om förstörande av vissa hälsofarliga missbrukssubstanser samt de sällan eller närmast aldrig förekommande ärendena om hävande av mönsterrätt i vissa fall och talan om äktenskapsskillnad i vissa fall. Av större praktisk betydelse och intresse är att åklagare redan i dag har uppgifter inom ramen för underrättelseverksamhet. Det rör sig här främst om tillämpningen av 2007 års preventivlag. Därutöver har åklagare i viss begränsad utsträckning en roll i polisens regionala underrättelsecenter (RUC).

Åklagare utför således i dag arbetsuppgifter på relevant område för IHL. Även om just dessa arbetsuppgifter inte är särskilt spridda i organisationen kan dock konstateras att de beslut som nu är aktuella på ett principiellt plan ligger nära de beslut som åklagare fattar inom ramen för förundersökningsverksamhet. Det är nämligen i båda fallen fråga om att väga effektiviteten i brottsbekämpningen mot intresset av att värna den personliga integriteten. Argumentet om att IHL skulle innebära ett artfrämmande inslag i åklagarnas verksamhet kan således inte anses utgöra något hinder mot en ordning med åklagare som beslutsfattare.

Ett annat argument mot att involvera åklagare i beslutsprocessen är att det skulle vara systemfrämmande att låta åklagare besluta om ett hemligt tvångsmedel när alla övriga hemliga tvångsmedel beslutas av domstol. Samtidigt som en sådan ordning ur ett perspektiv alltså skulle bryta mot systemet kan likväl påstås att det ur ett annat perspektiv skulle vara väl förenligt med systemet. Beslutsfattande av åklagare enligt IHL skulle nämligen följa den ansvarsfördelning som gäller rent hierarkiskt i rättskedjan. Om en åklagare vill utverka ett beslut som han eller hon inte har rätt att fatta själv (t.ex. häktning eller hemlig avlyssning av elektronisk kommunikation) så vänder sig

åklagaren till nästa instans i rättskedjan, dvs. domstol. När det nu har konstaterats att det finns ett värde i att flytta beslutsbehörigheten från Polismyndigheten, Säkerhetspolisen och Tullverket så är det naturligt att dessa myndigheter vid önskan om ett beslut enligt IHL ska vända sig till nästa instans i rättskedjan, dvs. åklagare. På så sätt är också regelsystemet uppbyggt i de flesta andra fall som t.ex. vid anhållande.

Ytterligare ett argument mot att involvera åklagare i beslutsprocessen är att det kan påstås att avståndet mellan underrättelseverksamhet och förundersökningsverksamhet minskar, vilket skulle kunna göra det svårare för åklagaren att leva upp till sin objektivitetsplikt. Sådana tankegångar lyftes fram av Åklagarmyndigheten i sitt remissvar över betänkandet En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen (SOU 2009:1). Enligt utredningen är det viktigt att åklagarnas objektivitetsplikt inte på något sätt blir urholkad av föreslagna förändringar. Det är därför grundläggande att analysera om en beslutanderätt enligt IHL skulle kunna äventyra åklagarnas objektivitetsplikt. Utredningen gör i denna del följande bedömning. Den lagstadgade objektivitetsplikten gäller inte bara under förundersökningen utan även i underrättelsestadiet (23 kap. 4 § tredje stycket RB). Även om åklagarna skulle få en uppgift i underrättelseskedet så skulle de alltså ha samma lagstadgade objektivitetsplikt att förhålla sig till. Frågan är då om det allmännas förtroende för åklagarnas objektivitetsplikt skulle kunna undergrävas enbart genom att åklagare skulle kunna påstås vara frestade att hålla kvar ett ärende i underrättelsestadiet för att därigenom lättare få tillgång till övervakningsuppgifter enligt IHL i stället för att behöva vända sig till domstol och utverka ett tillstånd till hemlig övervakning av elektronisk kommunikation. Denna risk ska enligt utredningen inte överdrivas. Det saknas nämligen helt tecken på att åklagare av någon sorts bekvämlighetsskäl generellt sett skulle ha en tendens att tillämpa regelverk i strid med sin andemening för att på så sätt underlätta för sig. Inte heller detta argument har därför någon större bärkraft.

Datalagringsutredningen framhöll att det har ansetts olämpligt att tilldela åklagare (och domstolar) beslutsfunktioner i de brottsbekämpande myndigheternas allmänna underrättelsearbete. Detta hängde enligt Datalagringsutredningen samman med att underrättelseåtgärderna kan leda vidare till förundersökning (och rätte-

gång), 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 (SOU 2015:31 s. 285–286). Enligt utredningen är detta argument inte särskilt bärkraftigt. Det tillhör nämligen den normala gången i rättskedjan att beslut i olika stadier fattas på olika nivåer och att ärendena sedan åter kan hamna hos beslutsfattaren. Exempel på detta är anhållande och häktning, beslut om husrannsakan i vissa fall, beslut om hemliga tvångsmedel i förundersökning och beslut enligt 2007 års preventivlag. Det finns inget stöd för att det inte skulle vara en fungerande ordning. En åklagare som vid beslutsfattandet fått del av information som inte bör ingå i en förundersökning kan också lämna ärendet vidare till en kollega, som inte besitter samma kunskaper.

Som ovan noteras så är samtliga svenska myndigheter oberoende och självständiga. När det gäller just åklagarnas oberoende finns det skäl att lyfta fram en rapport av Venedigkommissionen[17] från 2010.[18] Rapporten synes främst ha fokus på åklagares verksamhet i förundersökningsfasen. Det hindrar dock inte att några generella rekommendationer om åklagare är intressanta även i relation till åklagares arbete inom underrättelseverksamheten.

En viktig komponent i ett oberoende är anställningsformen och här finns det skäl att uppmärksamma att den svenska riksåklagaren har ett mycket starkt anställningsskydd och anställs som en av få myndighetschefer med fullmakt (7 kap. 3 § RB). En sådan anställningsordning går mycket väl i linje med Venedigkommissionens rekommendationer (p. 73). Möjligheterna att skilja riksåklagaren från ämbetet är klart definierade i lagen (1994:261) om fullmaktsanställning (4 §), vilket även det går väl i linje med rekommendationerna från Venedigkommissionen (p. 39). Även om övriga åklagare har ett svagare anställningsskydd så anställs de tills vidare, vilket innebär att de är anställda till pensionen, vilket också är en rekommendation av kommissionen (p. 50).

Till oberoendet hör också det viktiga förhållandet att en åklagare i sitt beslutsfattande är helt självständig. Även om åklagarväsendet är hierarkiskt uppbyggt så får inte en överordnad åklagare ge bindande

[17] Venedigkommissionen är en rådgivande kommission till Europarådet i konstitutionella frågor.
[18] European Standards as regards the independence of judicial system: Part II – The Prosecution Service, European Commission for Democracy Through Law (Venice Commission).

instruktioner till en underordnad åklagare om vilka beslut han eller hon ska fatta. En annan sak är att en överordnad åklagare kan överta en arbetsuppgift av en lägre åklagare (7 kap. 5 § RB).

Det sagda leder till slutsatsen att i valet mellan de olika alternativ som finns för beslutsfattande enligt IHL, så framstår åklagare som det mest rimliga. Enligt utredningens bedömning bör därför åklagare anförtros uppgiften att fatta beslut om inhämtning enligt IHL. Åklagare har som utgångspunkt generell befogenhet att utöva sitt ämbete, 6 § åklagarförordningen (2004:1265). Som utvecklas i författningskommentaren finns dock skäl att för de nu aktuella ärendena begränsa kretsen av behöriga åklagare genom myndighetsinterna föreskrifter (avsnitt 14.2).

De särskilda regler som i dag finns i 4 § IHL om att endast befattningshavare på vissa nivåer får fatta beslut och att dessa inte får fatta beslut om inhämtning i operativ verksamhet som de själva deltar i, behövs inte vid den nu föreslagna beslutsordningen. De kan därför utgå ur lagstiftningen. En annan sak är att det finns ett värde i att uppgifterna utförs av utvalda personer inom myndigheten med särskild kunskap om förutsättningarna för inhämtning. Den närmre strukturen för ansökningsförfarandet bör emellertid bestämmas inom respektive myndighet.

Den närmare ordningen för hur beslutsfattande av åklagare bör vara utformad redogörs för nedan.

Ansökan ska upprättas av Polismyndigheten, Säkerhetspolisen respektive Tullverket

Eftersom IHL föreskriver att myndigheterna själva får fatta beslut om inhämtning finns det av uppenbara skäl inga regler i IHL om vilken myndighet som ska upprätta ansökningar om tillstånd. När nu beslutsbehörigheten placeras på åklagare måste det dock finnas sådana regler. Eftersom inhämtning enligt IHL görs i Polismyndighetens, Säkerhetspolisens respektive Tullverkets intresse finns det inga andra rimliga alternativ än att föreskriva att ansökningarna ska upprättas av respektive myndighet.

Inga interimistiska beslut

EU-rätten lämnar ett utrymme för interimistiska beslut i brådskande fall. En sådan ordning skulle ge Polismyndigheten, Säkerhetspolisen och Tullverket rätt att i brådskande fall själva besluta om inhämtning. Frågan är om det finns skäl att införa en sådan ordning.

Datalagringsutredningen analyserade hur en interimistisk beslutsordning skulle fungera i underrättelseverksamhet (avsnitt 8.4.4). Det mest framträdande argumentet mot en interimistisk ordning är att ett ändrat beslut av den ordinarie beslutsinstansen inte i praktiken kan leda till rättning hos den operativa myndigheten som har fattat det interimistiska beslutet. Utredningen instämmer i Datalagringsutredningens analys och bedömer därför att det inte bör införas någon interimistisk beslutsmöjlighet. Behovet av interimistiska beslut är inte heller särskilt påtagligt om beslutet om inhämtning fattas av åklagare, eftersom det för dem finns rutiner för jour- och beredskapstjänstgöring, 13 § åklagarförordningen (2004:1265).

Besluten ska inte vara överklagbara

Åklagarbeslut är som huvudregel inte överklagbara. Det har inte framkommit något skäl att behandla beslut om inhämtning enligt IHL på annat sätt. Det kommer i normalfallet inte heller vara möjligt för den ansökande myndigheten att få till stånd en överprövning av beslutet inom Åklagarmyndigheten, även om det i undantagsfall skulle kunna förekomma (Riksåklagarens riktlinjer RåR 2013:1 s. 15). Eftersom överklagande endast kan bli aktuellt vid avslagsbeslut, såvida inte ett offentligt ombud skulle delta i processen, skulle inte heller en överklagandemöjlighet innebära någon rättssäkerhetsgaranti för den enskilde. Att införa offentliga ombud vid en prövning inför åklagare är inte aktuellt.

Plikten att omedelbart häva beslut ska åvila den ansökande myndigheten

IHL innehåller en föreskrift med innebörd att ett beslut om inhämtning omedelbart ska hävas om det inte längre finns skäl för det (5 §). Även om det initiala beslutet nu föreslås ska fattas av åklagare

bör skyldigheten att häva beslutet alltjämt vila på Polismyndigheten, Säkerhetspolisen och Tullverket. Skälet till det är att de nämnda myndigheterna har bäst förutsättningar att bedöma om det saknas skäl för ett beslut om inhämtning. För den beslutande åklagaren är det varken lämpligt eller möjligt att följa ett underrättelseärende så nära att denna bedömning kan göras med någon större precision.

Underrättelse till SIN ska göras av den ansökande myndigheten

Dagens reglering innebär att Polismyndigheten, Säkerhetspolisen och Tullverket har en skyldighet att underrätta SIN om ett beslut om inhämtning enligt IHL. Underrättelsen ska lämnas senast en månad efter det att ärendet om inhämtning avslutades, 6 § IHL.

En första fråga att besvara är om det även med utredningens förslag, att åklagare ska fatta beslut enligt IHL, ska finnas en skyldighet att underrätta SIN. Ett argument för att ta bort denna skyldighet är att om besluten fattas av en oberoende myndighet så tunnas behovet av tillsyn ut (prop. 2011/12:55 s. 90 och 111). Det talar för att underrättelsekravet skulle kunna slopas. Emellertid är det så att tillsynen inte är det enda argumentet för en underrättelse. Som utvecklas närmare i avsnitt 12.8.5 kan underrättelseskyldigheten till SIN kompensera för att någon underrättelse till den enskilde inte görs vid beslut enligt IHL. Enligt utredningen bör därför underrättelseskyldigheten till SIN alltjämt finnas kvar.

Även om beslutsrätten enligt IHL skulle placeras hos åklagare bör skyldigheten att underrätta SIN även fortsättningsvis ligga kvar hos respektive myndighet. Skälet till det är att tidpunkten för underrättelseskyldighetens fullgörande är kopplad till när ärendet om inhämtning avslutas. Det är endast Polismyndigheten, Säkerhetspolisen och Tullverket som har kännedom om när ett ärende avslutas.

Personuppgifts- och sekretessregler utgör inget hinder för beslutsfattande av åklagare

Om åklagare får en roll som beslutsfattare enligt IHL så kommer personuppgifter och sekretessbelagd information att behöva lämna Polismyndigheten, Säkerhetspolisen och Tullverket för att skickas till den åklagare som ska fatta beslutet. De berörda myndigheternas

personuppgiftsbehandling är emellertid kringgärdade med integritetsskyddande lagstiftning som reglerar både den egna myndighetens personuppgiftsbehandling och hur personuppgifter får lämnas ut till någon annan. Exempel på sådana lagar är polisdatalagen (2010:361) och åklagardatalagen (2015:433). Härutöver finns bestämmelser om sekretess i offentlighets- och sekretesslagen (2009:400).

Enligt utredningens bedömning finns inget hinder i någon av de nämnda lagarna för att uppgifter (även sekretessbelagda) ska kunna skickas till åklagare i anslutning till att denne ska fatta beslut. Åklagardatalagen utgör tillräckligt stöd för att åklagare ska kunna behandla personuppgifterna på automatiserad väg. Någon särskild sekretessbestämmelse för uppgifterna bedöms inte heller behövas, eftersom uppgifterna även hos åklagaren omfattas av sekretessbestämmelserna i 18 kap. offentlighets- och sekretesslagen.

En särskild nämnd skulle vara mer lämpad än åklagare

När det gäller val av beslutsmyndighet finner utredningen skäl att lyfta fram följande. Polismetodutredningen föreslog i sitt betänkande Särskilda spaningsmetoder (SOU 2010:103) att det skulle inrättas en särskild nämnd som skulle fatta beslut i underrättelseverksamhet om tillstånd till särskilt ingripande åtgärder, t.ex. ljud- eller bildupptagning, identifiering av mobil elektronisk kommunikation och störning av sådan kommunikation (s. 311–313). Detta förslag bereds alltjämt i Regeringskansliet, vilket innebär att någon sådan nämnd inte finns för närvarande. En sådan nämnd skulle vara mer lämpad än åklagare att besluta om tillstånd till inhämtning enligt IHL. Enligt utredningens bedömning bör därför – om Polismetodutredningens förslag genomförs i denna del – regeringen överväga att då lägga beslutsbefogenheten på denna nämnd i stället för på åklagare.

Särskilt om alternativet med domstol som beslutsorgan

Som ovan beskrivits gör utredningen bedömningen att domstol inte bör komma på fråga som beslutsorgan för ärenden enligt IHL. För det fall det i den fortsatta beredningen av detta betänkande skulle bedömas vara mer lämpligt med en domstolsprövning lämnas nedan en grundstruktur för hur en sådan ordning skulle kunna vara utformad.

Ansökningar bör göras av respektive myndighet

Om domstol skulle bli beslutsmyndighet enligt IHL måste avgöras vilken myndighet som ska göra ansökan hos domstolen. Det som ligger närmast till hands är att respektive myndighet gör ansökan. Det är dock inte självklart att en sådan ordning är den mest lämpliga. Vid införandet av 2007 års preventivlag övervägdes nämligen om Polismyndigheten och Säkerhetspolisen skulle få ansöka direkt hos domstol (efter samråd med åklagare) eller om åklagare i stället skulle ha denna behörighet (prop. 2005/06:177 s. 67–68). Det noterades i det sammanhanget som en parallell att Polismyndigheten och Säkerhetspolisen har rätt att framställa yrkanden om hemliga tvångsmedel i domstol i ärenden enligt LSU (21 § LSU). Regeringen pekade dock på att i de större utredningar om allvarlig brottslighet som utförts med framgång regelmässigt har förevarit samarbete mellan åklagare, spanings- och underrättelseavdelning samt utredningsenheter på ett mycket tidigt stadium. Regeringen pekade också på att en ansökning enligt 2007 års preventivlag inrymmer svåra juridiska avvägningar. Regeringen bedömde därför att åklagare var mest lämpade att göra ansökan hos rätten enligt 2007 års preventivlag.

Det finns emellertid inte stöd för antagandet att behovet av att involvera åklagare är lika omfattande vid ärenden enligt IHL som vid ärenden enligt 2007 års preventivlag. Även om ärenden enligt IHL inrymmer svåra överväganden så har myndigheterna egen beslutsbefogenhet i dag och ärendenas komplexitet är inte ensamt skäl att förlägga rätten att göra ansökningar hos åklagare. Enligt utredningen finns det, om domstolar ska få beslutsbefogenhet enligt IHL, i stället skäl att ta tillvara den vinst det innebär att inte behöva låta åklagare ha en större roll än nödvändigt i underrättelseprocessen. Ansökningen bör därför göras direkt av respektive myndighet.

Stockholms tingsrätt bör vara exklusivt forum

Det är svårt att hitta någon lämplig behörig domstol. På grund av ärendenas mycket känsliga natur där i princip hela ärendet är sekretessbelagt bör inte samtliga tingsrätter kunna handlägga ansökningar enligt IHL. Samtidigt kan det på grund av ärendenas potentiellt brådskande natur innebära en nackdel om det inte finns behöriga domstolar i en stor del av landet. Det kan dock samtidigt noteras att

2007 års preventivlag har Stockholms tingsrätt som ensamt behörigt forum. För det fall allmän domstol ska få en roll som beslutsfattare enligt IHL gör utredningen samantaget bedömningen att Stockholms tingsrätt bör vara exklusivt forum.

Offentliga ombud bör inte delta i handläggningen

Om beslutsbefogenheten i ärenden enligt IHL ska ligga hos allmän domstol är frågan om förfarandet, liksom vid vissa andra beslut om hemliga tvångsmedel, ska utformas som ett slags kontradiktorisk process (prop. 2002/03:74 s. 23). Av uppenbara skäl skulle i så fall inte den berörda kunna uppträda som part i domstolen. Dessutom finns inte alltid någon tydligt berörd person. För att uppnå det kontradiktoriska inslaget skulle det i stället kunna övervägas att inrätta en funktion med offentliga ombud (27 kap. 26–30 §§ RB). Ett sådant ombud skulle inte primärt ha till uppgift att företräda den enskilde som utsätts för tvångsmedlet utan i stället att företräda enskildas integritetsintressen i allmänhet. Ett offentligt ombud deltar i handläggningen vid domstol när det gäller hemlig avlyssning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning, men inte när det är fråga om hemlig övervakning av elektronisk kommunikation.

När bestämmelserna om offentligt ombud infördes bedömde regeringen att behovet av offentliga ombud var mindre för hemlig övervakning av elektronisk kommunikation än för andra hemliga tvångsmedel. Offentliga ombud skulle därför inte delta vid sådana ärenden men regeringen ansåg att frågan behövde övervägas ytterligare (prop. 2002/03:74 s. 24). Efter att Utredningen om vissa hemliga tvångsmedel lämnat sitt betänkande SOU 2012:44 övervägde regeringen frågan på nytt (prop. 2013/14:237 avsnitt 7.2). Det bedömdes då att det integritetsintrång som tvångsmedlet kan medföra typiskt sett är mindre än när det gäller de övriga tvångsmedlen samt att sådana frågor som offentliga ombud särskilt bevakar (t.ex. att ett tillstånd utformas på ett sådant sätt att legitima integritetsintressen tillgodoses) mer sällan torde komma upp vid hemlig övervakning av elektronisk kommunikation; de möjliga variationerna av integritetsintrånget är typiskt sett avsevärt mindre för hemlig övervakning av elektronisk kommunikation än för andra hemliga tvångs-

medel. Dessutom ansåg regeringen att det finns ett värde i att de offentliga ombudens medverkan koncentreras till ärenden där behoven och funktionen av detta har visat sig vara starka.

De uppgifter som hämtas in enligt IHL är i princip samma uppgifter som kan erhållas genom hemlig övervakning av elektronisk kommunikation. De är dock något färre eftersom inhämtningen i fråga om uppgifter om meddelanden är begränsad till historiska uppgifter som finns hos den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Integritetsintrånget blir därför i motsvarande utsträckning mindre. Utredningen anser att det är en välmotiverad ordning att offentliga ombud inte deltar i ärenden om hemlig övervakning av elektronisk kommunikation; det har inte framkommit något, vare sig genom Tele2-domen eller i övrigt, som ger anledning till någon annan bedömning än den som regeringen gjorde efter översynen av Utredningen om vissa hemliga tvångsmedel. Eftersom inhämtning enligt IHL får anses mindre integritetskränkande än hemlig övervakning av elektronisk kommunikation bör det inte föreskrivas mer långtgående rättssäkerhetsgarantier i IHL. Om domstol skulle anförtros uppgiften som beslutsmyndighet enligt IHL är det därför utredningens uppfattning att offentliga ombud inte bör delta i beslutsprocessen.

Interimistiska beslut bör inte tillåtas

Som utvecklas ovan lämnar EU-rätten ett utrymme för interimistiska beslut. Tillämpat på IHL skulle det innebära att Polismyndigheten, Säkerhetspolisen och Tullverket vid brådskande fall själva skulle få fatta beslut om inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet (alltså som i dag).

Vid val av domstol som beslutsorgan blir behovet av interimistiska beslut större än om åklagare skulle vara beslutsfattare, eftersom det får förmodas att domstolarna inte kan förmå att ha samma beredskap för ett snabbt beslutsfattande. Det gäller i än högre grad om förfarandet utformas med krav på muntlig förhandling. Samtidigt måste beaktas att om interimistiska beslut tillåts så blir i många fall den efterföljande domstolsprövningen en chimär. Det beror på att de flesta fall av inhämtning enligt IHL avser historiska uppgifter

och om tjänstemannen på den brottsbekämpande myndigheten redan har tagit del av informationen så går det inte att göra ogjort.

Att inrätta en ordning där en överprövning av interimistiska beslut i många fall endast blir en illusion rimmar illa med rättsstatliga principer. Det nu anförda leder utredningen till slutsatsen att inga interimistiska beslut bör tillåtas. Den rättssäkerhetsvinst som uppnås genom ett förbud mot interimistiska beslut betalar sig olyckligtvis genom en något sämre effektivitet i inhämtningen.

Underrättelse till SIN ska göras av den ansökande myndigheten

I SIN:s uppdrag ingår bl.a. att utöva tillsyn över de brottsbekämpande myndigheternas användning av hemliga tvångsmedel (avsnitt 6.4.2). Det finns därför ett intresse för SIN att bli informerad om att domstolen gett en brottsbekämpande myndighet tillstånd att inhämta uppgifter om elektronisk kommunikation. På samma sätt som om beslutsrätten läggs på åklagare skulle en underrättelseskyldighet till SIN också kompensera för att någon underrättelse till enskild inte görs vid beslut enligt IHL (se även avsnitt 12.8.5). Enligt utredningen bör därför underrättelseskyldigheten till SIN alltjämt finnas kvar även om domstol fattar besluten.

Även om beslutsrätten enligt IHL skulle placeras hos domstol bör skyldigheten att underrätta SIN även fortsättningsvis ligga kvar hos respektive myndighet. Skälet till det är desamma som om åklagare skulle haft beslutsrätten, dvs. att tidpunkten för underrättelseskyldighetens fullgörande är kopplat till när ärendet om inhämtning avslutas.

RB bör tillämpas på förfarandet

På förfarandet bör tillämpas de regler i RB om styr handläggning av frågor om hemliga tvångsmedel i brottmål och om överklagande av beslut i sådana frågor. Procedurreglerna blir då i överensstämmelse med vad som gäller för andra hemliga tvångsmedel. Det innebär t.ex. att rättens beslut blir möjligt att överklaga för den ansökande myndigheten.

2007 års preventivlag

Utredningens bedömning: De svenska reglerna om förhandskontroll vid preventiva tvångsmedel uppfyller de krav som EU-rätten ställer.

Som framgår ovan krävs huvudsakligen domstolsbeslut innan preventiva tvångsmedel får användas (avsnitt 6.2.5). Om det kan befaras att inhämtande av rättens tillstånd skulle medföra en fördröjning av väsentlig betydelse för möjligheterna att förhindra den brottsliga verksamheten, får dock tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut.

Enligt utredningens bedömning lever det svenska regelverket på detta område upp till EU-rättens krav.

LSU

Utredningens bedömning: De svenska reglerna om förhandskontroll vid särskild utlänningskontroll uppfyller de krav som EU-rätten ställer.

Som framgår ovan krävs domstolsbeslut för användning av hemliga tvångsmedel vid särskild utlänningskontroll (avsnitt 6.2.6).

Enligt utredningens bedömning lever det svenska regelverket på detta område upp till EU-rättens krav.

12.8.5 Information till berörda

EU-domstolen fastslår att EU-rätten kräver att de myndigheter som har beviljats tillgång till lagrade uppgifter, enligt tillämpliga nationella förfaranden, informerar de berörda personerna om detta så snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar. Den informationen är enligt EU-domstolen nödvändig bl.a. för att dessa personer ska kunna utöva sin rätt till rättslig prövning vid kränkning av deras rättigheter (avsnitt 9.8.5).

Hemlig övervakning av elektronisk kommunikation

Utredningens bedömning: Reglerna om information till de berörda när det gäller hemlig övervakning av elektronisk kommunikation uppfyller de krav som EU-rätten ställer.

Som framgår ovan finns det föreskrivet en underrättelseskyldighet i RB gentemot den enskilde vid användningen av hemliga tvångsmedel (avsnitt 6.4.2). Det finns dock vissa möjligheter att skjuta upp underrättelsen om de uppgifter som den ska innehålla omfattas av vissa typer av sekretess (27 kap. 33 § första stycket RB). 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 (1947:948). Vissa brott som faller inom Säkerhetspolisens ansvarsområde är helt undantagna från underrättelseskyldighet (27 kap. 33 § tredje stycket RB).

EU-domstolen anger att risk för skada för utredningen kan motivera en uppskjuten underrättelse till den enskilde (p. 121 i domen). De svenska bestämmelserna är dock bredare och ger även möjlighet att skjuta upp underrättelse t.ex. vid sekretess på grund av risker för skada för landets försvar, 27 kap. 33 § RB och 15 kap. 2 § offentlighets- och sekretesslagen (2009:400). Det får dock anses att EU-domstolen inte uttömmande har angett vilka sekretessgrunder som kan anföras som skäl för att skjuta upp underrättelse. Det skulle nämligen vara svårbegripligt om den nu angivna sekretessgrunden (skydd för landets försvar) inte skulle få åberopas men man skulle få skjuta upp underrättelse för att skydda en enda brottsutredning. Även sekretess för att skydda polisens arbetsmetoder måste rimligen få åberopas till stöd för att skjuta upp underrättelse (18 kap. 1 § offentlighets- och sekretesslagen). Att EU-domstolen inte uttömmande har angett i vilka fall underrättelse får skjutas upp framgår också av hänvisningen till ”tillämpliga nationella förfaranden” (p. 121 i domen). Enligt utredningens bedömning bör således de svenska reglerna för att kunna skjuta upp underrättelse bibehållas.

EU-domstolen gör ingen bedömning i fråga om helt underlåten underrättelse. Domstolen berör endast uppskjuten underrättelse. Att den svenska rättordningen i vissa fall föreskriver att underrättelse till den enskilde helt kan underlåtas är dock inget som enligt utred-

ningen står i strid med EU-rätten. För det första måste nämligen syftet med underrättelsen beaktas vid denna bedömning. Syftet är att bereda den enskilde möjlighet till en rättslig prövning vid kränkning av dennes rättigheter. Ju längre tiden går desto mer klingar intresset av en rättslig prövning av. För det andra så säkerställs att det utförs en kontroll av att tvångsmedelsanvändningen har skett på ett korrekt sätt genom att SIN underrättas i de fall den enskilde inte underrättas (14 b § förundersökningskungörelsen). Endast i de fall tvångsmedelsanvändningen avser vissa brott som utreds av Säkerhetspolisen kan underrättelse underlåtas helt och hållet (27 kap. 33 § tredje stycket RB och 14 b § andra stycket förundersökningskungörelsen). Utrymmet för staten att avvika från skyddsreglerna för att värna sina vitala intressen är också något som bejakas av domstolen (p. 119 i domen, som i och för sig rör för vilka personer myndigheterna ska få tillgång till uppgifter om).

När det gäller basstationstömning, dvs. vilka mobiltelefoner m.m. som har funnits inom ett visst geografiskt område, kan många icke misstänkta omfattas av åtgärden. Dessa personer underrättas typiskt sett inte om inhämtningen (27 kap. 31 § andra stycket RB). Enligt utredningen finns det två skäl som talar för att EU-rätten inte utgör hinder för en bibehållen sådan ordning. Det första är att EU-domstolen själv synes ge medlemsstaterna visst nationellt handlingsutrymme i denna fråga genom att hänvisa till ”tillämpliga nationella förfaranden” (p. 121). Det andra är att underrättelseinstitutet enligt EU-domstolen är avsett att möjliggöra för personer att kunna utöva sin rätt till rättslig prövning vid kränkning av deras rättigheter (p. 121). I fallet med basstationstömning som drabbar icke misstänkta är integritetsintrånget för varje enskild individ mycket begränsat, eftersom det normalt endast är fråga om en positionsbestämning vid ett specifikt tillfälle (avsnitt 12.8.3). Något egentligt behov av att ha tillgång till rättslig prövning finns därför inte för dessa personer. Det ska även i sammanhanget noteras att den behandling av de icke misstänktas personuppgifter som utförs hos polisen och Tullverket är kringgärdad av ett integritetsskyddande regelverk i form av polisdatalagen (2010:361) och tullbrottsdatalagen (2017:447).

Utredningen gör mot bakgrund av det nu anförda bedömningen att de svenska reglerna om uppskjuten och underlåten underrättelse är förenliga med de krav som EU-rätten uppställer.

Inhämtning av uppgifter i underrättelseverksamhet

Utredningens bedömning: Reglerna om information till de berörda när det gäller inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet uppfyller de krav som EU-rätten ställer.

När det gäller inhämtning av uppgifter i underrättelseverksamhet enligt IHL finns ingen motsvarighet till RB:s krav på underrättelse till enskild. Frågan om ett sådant krav borde införas övervägdes i samband med att lagen infördes. Regeringen uttalade då, med hänvisning till SOU 2009:1, 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. Vidare uttalade regeringen att en sådan skyldighet därför skulle behöva förses med en rad undantag och det skulle 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. Det beaktades även att användningen av uppgifterna i en förundersökning förutsätter tillstånd av domstol till hemlig övervakning av elektronisk kommunikation. I dessa fall, där uppgifterna innebär en påtaglig integritetspåverkan för en enskild, skulle därmed bestämmelserna om underrättelseskyldighet i RB bli tillämpliga (prop. 2011/12:55 s. 107).

Det ska också noteras att i vissa fall är identiteten på den som omfattas av inhämtning enligt IHL inte känd på annat sätt än genom t.ex. ett smeknamn. I dessa fall är underrättelse omöjlig att lämna.

Som regeringen konstaterade vid införandet av IHL omfattas uppgifterna av sekretess – i många fall dessutom av sekretess som är särskilt viktig att bibehålla. Dessutom är den brottslighet som är aktuell vid inhämtning enligt IHL mycket angelägen att bekämpa effektivt. Det rör sig nämligen om grov brottslighet, antingen sett till de straff som kan utdömas (2 § IHL) eller sett till att brotten riktar sig mot centrala delar av samhället och staten (3 § IHL).

Som ovan anförs när det gäller hemlig övervakning av elektronisk kommunikation torde det finnas ett nationellt utrymme att underlåta underrättelse. Enligt utredningens bedömning täcker detta undantag

in ett system där information till de berörda över huvud taget inte föreskrivs vid inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet. Vid denna bedömning har även beaktats att det finns en möjlighet för den enskilde att vända sig till SIN med en begäran att nämnden ska kontrollera om vederbörande har utsatts för inhämtning enligt IHL och om inhämtningen och behandlingen av uppgifterna varit lagenlig, 3 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet) samt att SIN underrättas om beslut om inhämtning av uppgifter enligt IHL (6 §). Europadomstolen har godtagit att underrättelse inte lämnas till den berörde när liknande kontrollsystem funnits att tillgå (jfr Kennedy mot Förenade kungariket, 18 maj 2010, § 167 Roman Zakharov mot Ryssland, 4 december 2015, § 288). Enligt utredningens bedömning innebär det nu beskrivna regelsystemet således att det svenska regelverket lever upp till de krav som EU-rätten ställer enligt EU-domstolen.

2007 års preventivlag

Utredningens bedömning: Reglerna om information till de berörda när det gäller hemlig övervakning av elektronisk kommunikation enligt 2007 års preventivlag uppfyller de krav som EU-rätten ställer.

Som framgår ovan gäller att den som varit utsatt för övervakning enligt 2007 års preventivlag avseende vissa brott som huvudsakligen utreds av Polismyndigheten ska underrättas om tvångsmedelsanvändningen (avsnitt 6.4.2). Underrättelseskyldigheten gäller alltså inte för de brott som huvudsakligen utreds av Säkerhetspolisen.

Underrättelse kan skjutas upp om det gäller sekretess för uppgifterna. Underrättelse får även underlåtas helt i vissa fall. Reglerna kring detta är utformade på motsvarande sätt som för underrättelse vid hemlig övervakning av elektronisk kommunikation enligt RB. De skäl som redovisas till stöd för utredningens uppfattning att underrättelsereglerna i RB är förenliga med EU-rätten har giltighet även vid bedömningen av underrättelseskyldigheten enligt 2007 års preventivlag. Utredningens bedömning är därför att underrättelseskyldigheten enligt 2007 års preventivlag är förenlig med EU-rätten.

LSU

Utredningens bedömning: Avsaknaden av regler om information till de berörda vid särskild utlänningskontroll är inte i strid med EU-rätten.

Som redovisas ovan finns det ingen underrättelseskyldighet till enskild när hemlig övervakning av elektronisk kommunikation sker som ett led i en särskild utlänningskontroll. Det som kan bli aktuellt inom ramen för en särskild utlänningskontroll är utredning om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för planlägger eller förbereder terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott. Sådana brott är riktade mot statens centrala och vitala intressen och tillhör Säkerhetspolisens verksamhetsområde. Det finns därför starka sekretesskäl att vara restriktiv med underrättelser till enskild.

Som framgår ovan får EU-rätten anses vara mer tillåtande för undantag när det gäller så vitala statsintressen som det nu är fråga om, i synnerhet när dessa hotas av terrorism. Utredningen gör därför bedömningen att en underlåten underrättelseskyldighet vid tvångsmedelsanvändningen vid särskild utlänningskontroll är förenlig med EU-rätten.

I sammanhanget kan nämnas att hemlig övervakning av elektronisk kommunikation i samband med särskild utlänningskontroll är en mycket begränsad företeelse. Redovisningsperioden den 1 juli 2015–30 juni 2016 förordnades endast om tre fall av sådan övervakning (skr. 2016/17:72 s. 4).

12.8.6 Tillgången ska avse även uppgifter som lagras för operatörernas egna ändamål

Utredningens bedömning: De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation ska alltjämt avse inte bara de uppgifter som sparas enligt datalagringsreglerna utan också den information som sparas för operatörernas egna ändamål, t.ex. uppgifter som behövs för fakturering.

Enligt direktiv 2002/58 gäller att operatörerna ska utplåna uppgifter när de inte längre behövs för sitt syfte att överföra kommunikation (artikel 6). Av samma artikel framgår att operatörerna, trots denna utplåningsskyldighet, får spara uppgifter i vissa fall. Utöver dessa uppgifter som enligt direktivet får sparas för egna ändamål finns det ett regelverk för lagring av uppgifter för brottsbekämpande ändamål. Man skulle alltså kunna uttrycka det som att operatörerna har två uppgiftsmängder: en för egna ändamål (som t.ex. fakturering) och en som de är ålagda att lagra enligt datalagringsreglerna (uppgifter som sparas för brottsbekämpande ändamål).

Tudelningen av de lagrade uppgifterna framgår för svenskt vidkommande genom 6 kap. 16 a och 16 c §§ LEK. Av dessa bestämmelser kan utläsas att de trafikuppgifter som lagras för brottsbekämpande ändamål endast får behandlas vid tillämpning av reglerna om hemliga tvångsmedel. Detta innebär att om Polismyndigheten efterforskar en försvunnen person (utan misstanke om brott) eller Skatteverket behöver uppgifter i ett ärende om kontroll av skatt så får myndigheten inte tillgång till de uppgifter som är lagrade för brottsbekämpande ändamål, men däremot de uppgifter som finns lagrade för operatörens eget behov (6 kap. 22 § LEK jämförd med 16 a och 16 c §§ samma kapitel).

Det står alltså klart att endast de brottsbekämpande myndigheterna har rätt att få tillgång till de uppgifter som är föremål för lagring enligt de speciella datalagringsreglerna. Vid det omvända förhållandet – alltså att de brottsbekämpande myndigheterna vill få åtkomst till uppgifter som lagras av operatörerna för eget behov – så finns inga begränsningar. De brottsbekämpande myndigheterna är alltså inte avskurna från tillgång till de uppgifter som en operatör lagrar för egna ändamål. En annan sak är att en sådan tillgång förutsätter tillämpning av ett annat regelverk, t.ex. hemlig övervakning av elektronisk kommunikation med de begränsningar som följer av det regelverket (detta gäller självklart även vid tillgång till uppgifter som omfattas av lagringsskyldigheten).

Från det ovanstående måste skiljas de uppgifter som operatörerna behandlar på grund av sina åligganden att medverka till att förmedla meddelanden som är av vikt för allmänheten vid en olycka eller en annan allvarlig händelse (5 kap. 7 d § LEK). Dessa uppgifter får användas endast för att förmedla sådana meddelanden och får således

inte tillgängliggöras för de brottsbekämpande myndigheterna (5 kap. 10 b § LEK).

Det ska i detta sammanhang nämnas att regleringen i 6 kap. 16 e § LEK innebär att operatörernas prissättning för att lämna ut uppgifter som inte omfattas av lagringsskyldigheten inte omfattas av PTS normgivningsbemyndigande. Det innebär att ett utlämnande av mycket likartade uppgifter kan skilja sig åt väsentligt i pris för de brottsbekämpande myndigheterna. Det är enligt utredningen en otillfredsställande ordning. Utredningen har dock inte inom ramen för sitt uppdrag haft möjlighet att lämna något förslag i denna del.

12.9 Tillgången till abonnemangsuppgifter

Utredningens bedömning: Regleringen kring abonnemangsuppgifter är förenlig med Sveriges internationella åtaganden.

Som tidigare nämnts omfattar inte Tele2-domen abonnemangsuppgifter (avsnitt 12.2). Som framhålls där går det dock inte att i detta sammanhang underlåta att anlysera regleringen kring dessa uppgifter. Det ska inledningsvis konstateras att tillgång till abonnemangsuppgifter inte utgör ett hemligt tvångsmedel (prop. 2013/14:237 s. 134) och sådana uppgifter har i sig inte ansetts vara särskilt integritetskänsliga, eftersom de endast ger uppgift om att personen är registrerad abonnent eller användare av ett visst abonnemang eller en ip-adress vid en viss tidpunkt (avsnitt 6.2.2). Det bör emellertid poängteras att abonnemangsuppgifter utgör kopplingen mellan annars relativt anonyma uppgifter och en fysisk person. I den egenskapen är abonnemangsuppgifter både skyddsvärda och integritetskänsliga, ungefär på samma sätt som en krypteringsnyckel. De kan dock inte likställas med trafik- och lokaliseringsuppgifter, av vilka man kan dra betydligt mer precisa slutsatser om personers privatliv (p. 99 i Tele2-domen). Det är därmed inte heller möjligt att analogt tillämpa EU-domstolens resonemang om de brottsbekämpande myndigheternas tillgång till lagrade trafik- och lokaliseringsuppgifter. I stället måste utgångspunkt tas ur mer generella regler kring behandling av personuppgifter. I sammanhanget ska även poängteras att den begränsningen av tillgång till lagrade uppgifter som EU-domstolen uppställer i Tele2-domen, till att endast omfatta bekämpning

av grov brottslighet, har sin utgångspunkt i artikel 15.1, som inte är relevant för abonnemangsuppgifter (p. 115 i Tele2-domen). Däremot bör det även för abonnemangsuppgifter gälla att syftet med tillgångsbestämmelsen ska stå i proportion till hur allvarligt ingrepp i de grundläggande rättigheterna det innebär att ge tillgång till de lagrade uppgifterna.

På liknande sätt blir inte heller de höga krav som Europakonvention ställer på hemliga tvångsmedel tillämpbara (jfr hänvisningarna i avsnitt 3.1.3 till Europadomstolens domar i målen Uzun mot Tyskland samt P.G. och J.H. mot Förenade kungariket, båda målen avsåg dessutom hemliga övervakningsåtgärder). Med den breda omfattning som skyddet för privatliv har (Europadomstolens dom den 16 februari 2000 i målet Amann mot Schweiz, § 65) får tillgången till abonnemangsuppgifter ändå anses innebära ett visst ingrepp i skyddet enligt artikel 8 i Europakonventionen och artikel 8 i rättighetsstadgan. Det krävs därför att tillgången är begränsad till vad som är strängt nödvändigt och proportionerligt i ett demokratiskt samhälle (artikel 8.2 i Europakonventionen och artikel 52.1 i rättighetsstadgan, Tele2-domen p. 96 och p. 122–124 i EU-domstolens yttrande 1/15 den 26 juli 2017).

Utifrån Europadomstolens praxis följer att Europakonventionen betraktar abonnemangsuppgifter som ett viktigt verktyg för att skydda brottsoffers rätt till upprättelse. Europadomstolen har nämligen i ett avgörande tolkat konventionen på så sätt att den innebär en förpliktelse för staterna att ha en lagstiftning som möjliggör åtkomst till abonnemangsuppgifter. Omständigheterna i avgörandet var i korthet följande. En okänd person hade gjort sig skyldig till förtal eller möjligen sexuellt ofredande av ett 12-årigt barn i Finland genom att lägga ut en påhittad kontaktannons av sexuell natur i 12-åringens namn. Gärningsmannen kunde inte identifieras på grund av att den nationella lagstiftningen inte möjliggjorde att uppgiften om förövarens identitet kunde inhämtas från operatören. I det aktuella fallet uttalade domstolen särskilt att konfidentialitet för kommunikation och yttrandefrihet ibland måste få vika för brottsbekämpande ändamål. Domstolen ansåg att Finland inte hade levt upp till sina skyldigheter enligt konventionen då det saknades lagstiftning som möjliggjorde för polisen att komma åt abonnemangsuppgifterna. (Europadomstolens dom den 2 december 2008 i målet K.U. mot Finland, särskilt § 49).

Det kan alltså sägas att Europakonventionen inte bara tillåter en rättsordning där de brottsbekämpande myndigheterna i någon form ges tillgång till abonnemangsuppgifter, den påbjuder en sådan ordning. Utrymmet för Sverige att ha ett regelverk som över huvud taget inte tillåter de brottsbekämpande myndigheterna att komma åt abonnemangsuppgifter är således tämligen begränsat.

Eftersom det inte är fråga om en hemlig övervakningsåtgärd och ingreppet i privatlivet är begränsat i jämförelse med tillgång till trafik- och lokaliseringsuppgifter, finns det inte heller något krav på förhandskontroll av domstol eller annan oberoende myndighet, eller på underrättelse till de berörda (angående förhandskontroll jfr även analysen i Ds 2014:23 s. 23–24 och avseende underrättelse, se SOU 2015:31 s. 192–194 och prop. 2011/12:55 s. 108). Vid en jämförelse med t.ex. husrannsakan, som normalt får beslutas av undersökningsledaren, är inhämtning av abonnemangsuppgifter betydligt mindre integritetskränkande, både i utförande och med beaktande av vilken information som kan fås fram. I någon mån kan också en jämförelse göras med inhämtande av annan identitetsinformation som omfattas av tystnadsplikt, såsom uppgift om innehavaraen av ett visst bankkort eller ännu mer integritetskänslig information, såsom hur bankkortet har använts, 1 kap. 10 och 11 §§ lagen (2004:297) om bank- och finansieringsrörelse.

Enligt utredningens bedömning behöver myndigheternas tillgång till abonnemangsuppgifter inte heller begränsas till misstanke om grov brottslighet. Ett intrång i skyddet för privatlivet torde normalt vara godtagbart om uppgifterna är nödvändiga för att det över huvud taget ska finnas förutsättningar för myndigheterna att utreda brottet, även om brottet har ett förhållandevis lågt straffvärde (Ds 2014:23 s. 68). När tillgångsbestämmelserna i 6 kap. 22 § första stycket 2 LEK utökades till att avse alla slags brott gjordes övervägandena bl.a. utifrån att trakasserier över internet och vuxnas kontakter med barn i sexuellt syfte blivit allt vanligare fenomen. Vid bedömningen av integritetsintrånget avseende utlämnande av abonnemangsinformation om ip-adresser beaktades att privatpersoner ofta använder dynamiska ip-adresser. Det gjordes en avvägning mellan det integritetsintrång som ett utlämnande av abonnemangsuppgifter innefattar och den stora betydelse uppgifterna ofta kan ha för polisens möjlighet att över huvud taget utreda brott som begås på internet. (prop. 2011/12:55 s. 102–103) Som framgår i avsnitt 7.3 fortsätter

användandet av internet och telekommunikation att växa och det finns ingenting som talar för att it- och telekombrottsligheten avtar eller att de brottsbekämpande myndigheternas behov av abonnemangsuppgifter minskat. Avvägandena framstår därmed fortfarande som giltiga. Mot bakgrund av detta framstår de brottsbekämpande myndigheternas tillgång till abonnemangsuppgifter som både strängt nödvändig och proportionell (se även avsnitt 12.6.4). Det gäller oavsett om det gäller uppgifter som operatörerna lagrar för egna ändamål eller endast i brottsbekämpande syfte.

Sammantaget är det utredningens bedömning att varken EU-domstolens dom eller Sveriges internationella åtaganden ger anledning att förändra förutsättningarna för de brottsbekämpande myndigheternas tillgång till uppgifter om abonnemang.

Utredningen noterar att Datalagringsutredningen har kommit med motiverade förslag på bl.a. beslutsbehörighet inom myndigheten och dokumentationskrav samt att dessa förslag alltjämt bereds inom Regeringskansliet (SOU 2015:31 avsnitt 7.5). Utredningen kan konstatera att en reformerad beslutsordning kan leda till ökad rättssäkerhet, ökade möjligheter att ta fram tillförlitlig statistik och att förfrågningarna till operatörerna blir mer enhetligt utformade.

12.10 Skydds- och säkerhetsnivåer, lagring inom Sverige och utplåning

Utredningens förslag: Uppgifterna som omfattas av lagringsskyldigheten får inte lagras utanför Sverige.

Utredningens bedömning: Reglerna om skydds- och säkerhetsnivå uppfyller de krav som EU-rätten ställer. Reglerna om utplåning uppfyller de krav som EU-rätten ställer.

12.10.1 Skydds- och säkerhetsnivåer

Som framgår ovan måste leverantörerna av elektroniska kommunikationstjänster enligt EU-domstolen garantera en särskilt hög skydds- och säkerhetsnivå för trafik- och lokaliseringsuppgifter genom lämpliga tekniska och organisatoriska åtgärder (avsnitt 9.9).

Artikel 4 i direktiv 2002/58, som avser säkerhet i samband med behandling av uppgifter, berör personuppgifter generellt. EU-domstolens uttalanden om skydd och säkerhet för uppgifterna kan därmed få viss betydelse även för regleringen kring abonnemangsuppgifter. Den särskilt höga skydds- och säkerhetsnivån som nämns i domen motiveras emellertid främst av att det är en stor mängd uppgifter av känslig natur, vilket inte får samma bäring för abonnemangsuppgifter.

I analysen i departementspromemorian Datalagring, EU-rätten och svensk rätt konstaterades att de svenska leverantörerna, genom regleringen i 6 kap. 3 a § LEK, som tar sikte 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. (Ds 2014:23 s. 90) Det saknas enligt utredningen anledning att göra någon annan bedömning nu. De svenska reglerna i detta avseende uppfyller alltså de krav EU-rätten uppställer.

När det gäller säkerhetsnivå konstaterades i analysen efter Digital Rights-domen att de svenska regler som ska säkerställa skyddet för de lagrade uppgifterna var tillräckligt strikta och precisa; bl.a. beaktades de krav som följer av PTS föreskrifter. Enligt föreskrifterna gäller bl.a. att den lagringsskyldige ska bedriva ett kontinuerligt och systematiskt säkerhetsarbete samt att rutiner och processer i detta avseende ska dokumenteras. Vidare ska endast personal med särskild behörighet ha tillgång till de lagrade uppgifterna och all behandling av uppgifterna ska loggas. (Post- och telestyrelsens föreskrifter och allmänna råd om skyddsåtgärder i samband med lagring och annan behandling av uppgifter för brottsbekämpande ändamål, PTSFS 2012:4).

EU-domstolen har inte gjort något uttalande i den nu aktuella domen som gör att analysen efter Digital Rights-domen behöver frångås. Enligt utredningens bedömning uppfyller således den svenska regleringen i detta hänseende EU-rättens krav.

12.10.2 Lagring inom Sverige

EU-domstolen anger att den nationella lagstiftningen måste föreskriva att datalagrade uppgifter inte ska få lagras utanför unionen (avsnitt 9.9). Vid den inledande analysen efter Digital Rights-domen föreslogs att frågan om ett förbud mot lagring utanför EU/EES borde utredas vidare (Ds 2014:23 s. 101). I den efterföljande analysen gjordes bedömningen att det inte bör införas något uttryckligt förbud mot att uppgifter som lagras enligt de svenska datalagringsreglerna förs över till tredje land (SOU 2015:31 s. 178). Genom EU-domstolens tydliga ställningstagande blir den nu nämnda bedömningen inte längre hållbar. Enligt utredningen bör det därför i vart fall införas ett förbud mot att lagra de nu aktuella uppgifterna utanför EU. För att regleringen ska bli enhetlig bör detsamma gälla abonnemangsuppgifter.

Som nämnts ovan (avsnitt 8.4.2) menade Datalagringsutredningen att lagring utomlands inte minskar möjligheterna att bedriva en aktiv och ändamålsenlig tillsynsverksamhet (se även prop. 2010/11:46 s. 58–60 och bet. 2010/11:JuU14 s. 13–14). Datalagringsutredningen noterade i och för sig att PTS befogenhet att få tillträde till områden, lokaler och andra utrymmen i praktiken endast kan utövas i Sverige. Däremot påverkades enligt samma utredning inte möjligheterna att utöva de övriga befogenheter myndigheten har till sitt förfogande, t.ex. att begära upplysningar eller att meddela förelägganden och förbud, av var leverantören väljer att lagra uppgifterna. Mot den bakgrunden kom Datalagringsutredningen till slutsatsen att PTS har möjlighet att bedriva en aktiv och ändamålsenlig tillsynsverksamhet även gentemot leverantörer som väljer att lagra uppgifter utanför unionen.

Även om man kan instämma i Datalagringsutredningens bedömning är det ofrånkomligt att en skyldighet för operatörerna att lagra uppgifterna i Sverige skulle göra PTS tillsyn ännu mer potent. När nu regelsystemet måste förändras vore det enligt utredningen värdefullt om den ytterligare förstärkning av tillsynen, som det skulle innebära med ett lagringskrav i Sverige, skulle tas till vara (se även p. 241 i generaladvokatens förslag till avgörande i Tele2-målet). Härutöver finns det skäl att tro att konfidentialiteten skyddas på ett bättre sätt om uppgifter endast lagras i Sverige.

Vidare blir det inte möjligt att i lagstiftningsarbetet göra en rättvis proportionalitetsbedömning, om det inte är möjligt att avgränsa vilka myndigheter (eller andra) som kan beredas tillgång till uppgifterna och för vilket syfte. Någon närmare harmonisering av lagrings- och tillgångsbestämmelser avseende uppgifter om elektronisk kommunikation mellan staterna finns nämligen inte. Om uppgifterna lagras i ett annat land, som har en snävare lagringsskyldighet men generösare tillgångsbestämmelser, kan användningsområdet för uppgifterna bli oproportionerligt stort. En bestämmelse om att lagring inte får ske utanför Sverige kan således motiveras utifrån flera syften.

En nackdel med en begränsning till Sverige är att operatörer som har verksamhet i flera EU-länder inte kan centralisera sin lagring och på så sätt kostnadseffektivisera processen. Motsvarande nackdel gäller för operatörer som verkar både i och utanför EU.

Vid bedömningen av om det nu diskuterade lagringskravet ska införas är frågan om Sveriges åtaganden enligt dataskyddskonventionen hindrar det. Som beskrivs ovan förbjuder nämligen dataskyddskonventionen en nationell lagstiftning som endast av integritetsskyddsskäl (”for the sole purpose of the protection of privacy”, artikel 12.2) hindrar att personuppgifter förs över till en annan konventionsstat för att behandlas där (avsnitt 3.2.3).

Datalagringsutredningen synes närmast ha kommit till slutsatsen att en lagstiftning som påbjuder lagring endast inom EU inte skulle vara förenlig med Sveriges åtaganden enligt dataskyddskonventionen (SOU 2015:31 s. 181–182). Det finns dock skäl att numera ifrågasätta den slutsatsen eftersom EU-domstolen i Tele2-domen har föreskrivit att lagring måste ske inom unionen och att lagring i konventionsstater utanför EU alltså inte är tillåten. Vid ett första påseende kan EU-domstolens slutsats synas svårförenlig med dataskyddskonventionen, men EU-domstolen har uppenbarligen inte ansett att konventionen hindrar en sådan ordning. (I sammanhanget bör påpekas att samtliga EU-medlemsstater har ratificerat konventionen). Förklaringen till EU-domstolens resonemang måste sökas i domskälen. Domstolen lyfter här fram inte bara integritetsaspekter utan även t.ex. konfidentialitet (p. 122). I resonemanget pekar även EU-domstolen på vikten av en effektiv tillsyn (p. 123) och hänvisar till Digital Rights-domen p. 68, i vilken myndighetskontrollen anförs som det bärande skälet för att förbjuda lagring

utanför unionen (se även generaladvokatens förslag till avgörande i Tele2-målet p. 241). Det kan visserligen argumenteras för att även tillsyn omfattas av ”protection of privacy”. Med beaktande av att bestämmelserna om tillsyn infördes först genom tilläggsprotokollet till dataskyddskonventionen och att detta inte har ratificerats av alla konventionsstater framstår emellertid inte det ha varit syftet. I förslaget till en ny dataskyddskonvention är kapitlet om tillsyn också placerat efter den motsvarande bestämmelsen om fri rörlighet för personuppgifter. Det framgår alltså att även om integritetsintresset har vägts in i EU-domstolens resonemang så har det inte varit ensamt avgörande (således inte ”the sole purpose”). Vid en sådan bedömning hindrar inte dataskyddskonventionen en ordning där lagring inte tillåts i andra konventionsstater.

Dataskyddskonventionen är för närvarande under reform men det finns inget som tyder på att nu aktuell bestämmelse i dataskyddskonventionen skulle få ett så annorlunda innehåll att bedömningen skulle bli annorlunda när den nya konventionen börjar tillämpas.

I sammanhanget ska noteras att direktiv 95/46 innehåller en reglering som i detta hänseende i stora drag motsvarar konventionens (skäl 9 och artikel 1.2) och som skulle kunna utgöra ett hinder mot att förbjuda att lagring sker i andra unionsländer. Detsamma gäller den kommande dataskyddsreformen (avsnitt 3.2.2). Det är inte möjligt att inom ramen för detta betänkande göra en tillräckligt djup analys av dataskyddsregleringen för att kunna bedöma om det utifrån ett EU-rättligt perspektiv är möjligt att förbjuda lagring i andra EU-länder.

Oavsett hur det dataskyddsrättsliga regelverket förhåller sig till olika former av geografiska begränsningar för lagringen måste beaktas att sektorn för elektronisk kommunikation i Sverige omfattas av säkerhetsskydd, dvs. skydd mot brott som riktar sig mot totalförsvaret eller rikets säkerhet i övrigt, säkerhetsskyddslagen (1996:627). PTS har tillsynsansvar över säkerhetsskyddet för bolag som verkar inom området för elektronisk kommunikation, 40 § säkerhetsskyddsförordningen (1996:633).

Av det nu sagda följer alltså att området för elektronisk kommunikation är av vikt för rikets säkerhet och att PTS har ett tillsynsuppdrag att fullfölja på området. Även om det som är mest skyddsvärt i telekomsektorn är själva driftsäkerheten i de allmänna näten så är utformningen av lagringsystemen en så integrerad del av

driften att även den får anses vara en del av det som är skyddsvärt för rikets säkerhet. För att PTS ska kunna fullgöra sitt tillsynsansvar på säkerhetsskyddsområdet på ett effektivt sätt fordras att lagringen görs i Sverige. (Hur tillsynen enligt säkerhetsskyddslagen ska vara utformad är för närvarande föremål för överväganden, dir. 2017:32). Eftersom de centrala intressena för staten inte omfattas av EU-rätten utgör inte heller EU-rätten något hinder mot en sådan ordning.

Enligt utredningen bör det således införas ett förbud för operatörerna att lagra uppgifterna utanför Sverige. Det ska i sammanhanget nämnas att lagring utanför Sverige inte torde förekomma alls eller endast i mycket liten utsträckning.

12.10.3 Utplåning

EU-domstolen har fastslagit att EU-rätten kräver att uppgifter som är föremål för datalagring oåterkalleligen ska förstöras när deras lagringstid har gått ut.

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.

Den svenska regleringen är således i överensstämmelse med EU-rättens krav.

12.11 Tillsyn

Utredningens bedömning: Reglerna om tillsyn uppfyller de krav som EU-rätten ställer.

Som beskrivs ovan måste medlemsstaterna enligt EU-domstolen garantera att en oberoende myndighet kontrollerar att den skyddsnivå som säkerställs i unionsrätten iakttas vad gäller skyddet för fysiska personer vid behandlingen av personuppgifter (avsnitt 9.10).

I Sverige är tillsyn över personuppgiftsbehandling delvis uppdelad. När det gäller tillsynen över personuppgiftsbehandling generellt är Datainspektionen tillsynsmyndighet. När det gäller den personuppgiftsbehandling som utförs i brottsbekämpande verksamhet

har även SIN en roll. Härtill kommer att PTS har tillsynsansvar över operatörerna. Att dessa tre myndigheter har tillräcklig grad av oberoende i en europeisk kontext är uppenbart (12 kap. 2 § RF).

Enligt utredningen finns tillräcklig grad av oberoende tillsyn för att det svenska regelverket ska vara förenligt med EU-rätten.

13 Konsekvenser och genomförande

13.1 Konsekvenser

Utredningens bedömning: Förslagen om en ändrad lagringsskyldighet, förbud mot lagring utanför Sverige och förhandsprövning vid beslut enligt IHL kommer att stärka integritets- och personuppgiftsskyddet. Förslaget om en ändrad lagringsskyldighet kommer möjligen att innebära att de brottsbekämpande myndigheternas förmåga att bekämpa brottslighet försämras i någon mån men torde inte innebära att brottsligheten kommer att öka. Åklagarmyndigheten kommer att behöva ytterligare resurser. Miljön kommer inte att påverkas av förslagen.

Utredningens förslag: Förslaget om förhandsprövning av beslut enligt IHL innebär att Åklagarmyndigheten kommer att behöva ett större årligt anslag (1 miljon kronor) och ett engångsbelopp (3 miljoner kronor) som bör finansieras med neddragning av anslagen för Polismyndigheten (500 000 kronor för den löpande ramhöjningen och 1,5 miljoner kronor för engångsbeloppet), Säkerhetspolisen (200 000 kronor för den löpande ramhöjningen och 600 000 kronor för engångsbeloppet) och Tullverket (300 000 kronor för den löpande ramhöjningen och 900 000 kronor för engångsbeloppet). Den kostnadsökning som drabbar operatörerna för lagring, säkerhet och anpassning ska de själva stå för.

13.1.1 Beskrivning av branschen

De företag som är relevanta för förslagen i detta betänkande utgör tillsammans en mycket heterogen grupp bestående av cirka 500 företag. De erbjuder olika tjänster i segmentet och har en mycket varierande marknadsandel. Dessutom varierar deras storlek mätt i omsättning kraftigt.

Bland mobiloperatörerna märks en tydlig fokusering kring fyra stora företag som tillsammans har en marknadsandel på cirka 95 procent. Den årliga omsättningen för det företag med störst marknadsandel ligger på 13 miljarder kronor samtidigt som ett av de företag med minst marknadsandel har en omsättning på 8 miljoner kronor. Av naturliga skäl varierar resultatet och balansomslutningen kraftigt mellan företagen. Även antalet abonnemang varierar kraftigt. Vissa av de små företagen räknar sina kunder i hundratal samtidigt som de största företagen har miljontals kunder.

I segmentet fast telefoni (inklusive ip-telefoni) finns ett företag med nästan 60 procent av marknaden. Det näst största har en marknadsandel som är på knappt 10 procent. Den årliga omsättningen för det största företaget uppgår till 92 miljarder kronor samtidigt som ett av de minsta omsätter 14 miljoner kronor. Även i denna del av segmentet varierar resultatet och balansomslutningen kraftigt mellan företagen. Några redovisar sina kunder i hundratal, de flesta i tusental och några i hundratusental. Endast ett företag har över en miljon kunder.

Även i det segment som erbjuder internetabonnemang finns en fokusering kring några stora företag. De tre största har en marknadsandel på drygt 70 procent. Det närmast därefter har en andel på drygt 5 procent av marknaden. Därutöver finns det en stor mängd företag med en marknadsandel som understiger en procent. Det största företaget omsätter 92 miljarder kronor och ett av de minsta 12 miljoner kronor. På samma sätt som för övriga segment varierar resultat och balansomslutning kraftigt. Antalet abonnemang redovisas för de flesta företagen i hundra- eller tusental. Fem av företagen räknar sina kunder i hundratusental och endast fyra i miljontal.

13.1.2 Samhällsekonomiska konsekvenser

Stärkt integritets- och personuppgiftsskydd för medborgarna

Genom förslaget på en mindre omfattande lagring stärks skyddet för den enskildes privatliv och kommunikation; såväl intrånget som risken för intrång minskar. Färre uppgifter kommer att lagras om människors kommunikationer och rörelser och därmed lagras mindre information som gör det möjligt att dra slutsatser om individers vanor och företeelser. En mindre omfattande lagring och även begränsningen i sig torde också innebära att folks eventuella känsla av att vara konstant övervakade minskar.

Utöver att antalet känsliga uppgifter minskar förstärks skyddet för uppgifterna genom förslaget på ett förbud att lagra uppgifterna utanför Sverige. Skyddet ökar också genom att det inte längre blir möjligt i något fall för myndigheterna att få tillgång till de lagrade trafik- och lokaliseringsuppgifterna utan en förhandsprövning av en åklagare eller oberoende myndighet. Härigenom omgärdas uppgifterna av ytterligare en rättssäkerhetsgaranti. Det kan därigenom antas att förtroendet för statens tvångsmedelsanvändning ökar.

En mindre omfattande lagring kan även få negativa följder för integritetsskyddet för den som är misstänkt för ett allvarligt brott. Ett sämre utbud av uppgifter och därmed en minskad nytta av hemlig övervakning av elektronisk kommunikation kan i något fall leda till att mer integritetskränkande tvångsmedel måste användas i stället. Sammantaget bedöms dock förslaget innebära integritetsvinster.

En minskad brottsuppklarning för narkotika- och våldsbrottslighet

Lagringsskyldigheten minskar tämligen kraftigt.[1] Effekten av hemlig övervakning av elektronisk kommunikation, som är beroende av tillgång till lagrade uppgifter, kommer därför att minska. Det kommer att påverka brottsuppklarningen på ett negativt sätt. I motsatt rikt-

[1] Denna analys utgår i sin helhet från en jämförelse med dagens lagstiftning. I vart fall delar av den nuvarande lagstiftningen har inte tillämpats efter Tele2-domen och Kammarrätten i Stockholms dom. En i sin helhet tillämpbar lagstiftning innebär självklart att bekämpningen av brott förstärks kraftigt i förhållande till en motsvarande lag som inte tillämpas.

ning verkar utredningens förslag att NAT-teknik nu inte längre kommer att hindra en meningsfull inhämtning av uppgifter.

För att bedöma hur stora effekter förslagen får på brottsuppklarningen är en rimlig utgångspunkt att ställa tvångsmedelsanvändningen i relation till den totala brottsutredande verksamheten. Därefter måste försöka skattas hur stor påverkan förändringarna har på den brottutredande verksamheten. Dessutom bör fastställas för vilka brottstyper detta får störst effekt.

En uppenbar svårighet med denna analys är att hitta något mått på den brottutredande verksamheten som är rimligt att jämföra med tvångsmedelsanvändningen. Ett mått som redovisas både för tvångsmedelansvändningen och för den brottsutredande verksamheten är antalet personer som varit föremål för hemliga tvångsmedel respektive lagföring. Detta mått är dock förenat med en viss svaghet eftersom uttrycket lagföring endast omfattar åklagarens beslut om åtal, strafföreläggande och åtalsunderlåtelse samt beslut om företagsbot som ersättning för straff, men alltså inte nedlagda förundersökningar. Dock kan det självklart ha förekommit hemlig övervakning av elektronisk kommunikation även i en nedlagd förundersökning. Oavsett vilket mått man väljer så kommer det vara behäftat med svagheter och det är svårt att se att något annat mått skulle vara särskilt mycket bättre.

Under år 2016 lagfördes drygt 100 000 misstänkta personer genom Åklagarmyndigheten. För Ekobrottsmyndigheten var motsvarande siffra knappt 2 000. Hemlig övervakning av elektronisk kommunikation användes mot drygt 2 000 personer. Säkerhetspolisen ingår inte i denna statistik. Myndigheterna använde alltså hemlig övervakning av elektronisk kommunikation mot cirka två procent av dem som var föremål för förundersökningar. Det är mot denna grupp utredningarna riskerar att försämras.

Nästa svårighet är att försöka skatta hur stor effekt förändringsförslagen har på den brottsutredande verksamheten. Även om viktiga uppgifter så som lokalisering och tid för kommunikationen fortfarande lagras så kommer en stor andel av uppgifterna inte längre att omfattas av lagringskravet. Dessutom ska lokaliseringsuppgifter bara lagras en tredjedel av tiden, jämfört med dagens lagstiftning. Det ska dock noteras att de brottsbekämpande myndigheterna fortfarande kommer att ha tillgång till den uppgiftsmängd som sparas för operatörernas egna ändamål. Därtill kan det antas att andra infor-

mationskällor kan komma att användas i högre utsträckning i vissa fall och därmed minska de negativa effekterna av en minskad lagring. Om andra informationskällor kommer att användas kan det innebära en omfördelning av resurser, som får till följd att t.ex. färre mindre allvarliga brott klaras upp. Till analysen hör också att NAT-teknik inte längre att vara ett hinder för meningsfull inhämtning. Att problemet med NAT-teknik betraktats som ett stort problem av myndigheterna framgår t.ex. av Säkerhetspolisens remissvar på Datalagringsutredningens betänkande. Däri lyfts farhågan att bestämmelserna om hemlig övervakning av elektronisk kommunikation i praktiken kan bli helt meningslösa på grund av NAT-tekniken. När nu detta problem åtgärdas torde det vara en tämligen verkningsfull förstärkning av de brottsbekämpande myndigheternas förmåga att klara upp brott, särskilt när den begåtts med hjälp av internet. Icke desto mindre gör utredningen bedömningen att brottsuppklarningen torde komma att påverkas negativt i viss omfattning. Det är i princip omöjligt att göra en bedömning av hur många ouppklarade brott som blir följden av detta, men det är rimligt att tro att ytterligare ett antal brottslingar kommer att gå fria på grund av förslaget om en förändrad lagringsskyldighet.

Den brottslighet som kan komma att påverkas mest är narkotika- och våldsbrottslighet eftersom det är i dessa förundersökningar som hemlig övervakning av elektronisk kommunikation används mest. Dessutom är dessa utredningar ofta tidsödande och därmed behovet av äldre uppgifter större där än i andra utredningar.

Den minskade brottsuppklarning som möjligen kan inträffa torde inte vara tillräcklig för att påverka brottsligheten i samhället.

Vad gäller förslaget om förhandskontroll vid inhämtning enligt IHL bedöms det inte påverka brottsbekämpningen alls. Datalagringsutredningen fann inga tecken på att lagen överanvänts eller på annat sätt missbrukats av de brottsbekämpande myndigheterna (SOU 2015:31 avsnitt 9.2.3.10, jfr dock om viss kritik av SIN mot hur lagen tillämpas av de brottsbekämpande myndigheterna i avsnitt 12.8.4). Det kan därför inte antas att ett krav på förhandsprövning av en åklagare, i sig skulle innebära att inhämtningarna skulle minska.

En försämrad underrättelseverksamhet

Underrättelseverksamheten kommer att påverkas av den förändrade lagringsskyldigheten. De lagar som ger de brottsbekämpande myndigheterna tillgång till uppgifter hos operatörerna i underrättelseverksamheten är IHL och 2007 års preventivlag. Även effektiviteten i dessa lagar påverkas av en minskad lagringsskyldighet. Men på samma sätt som i den brottsutredande verksamheten gynnas effektiviteten av att NAT-tekniken inte längre kommer att vara ett hinder för meningsfull inhämtning. Även denna aspekt har lyfts fram av Säkerhetspolisen i sitt remissvar över Datalagringsutredningens betänkande där myndigheten har pekat på att inhämtning enligt IHL kan bli helt meningslös på grund av NAT-tekniken.

Problemet med att kvantifiera påverkan på underrättelseverksamheten är att den innehåller ännu färre mått på sin omfattning än vad utredningsverksamheten gör. Även om man skulle kunna kvantifiera omfattningen är det möjligen än svårare att bedöma hur underrättelseverksamheten påverkas. Det som dock kan konstateras är att det i princip saknas straffprocessuella tvångsmedel som kan kompensera för sänkt effektivitet i de hemliga tvångsmedlen enligt IHL och 2007 års preventivlag. De försämringar i underrättelseverksamheten som blir följden av en minskad lagringsskyldighet kommer således inte att kunna kompenseras med andra åtgärder i någon större utsträckning. Påverkan på underrättelseverksamheten kommer därför sannolikt att bli större än på förundersökningsverksamheten.

Ingen påverkan på utlänningskontrollen

Antalet fall av användande av hemliga tvångsmedel vid LSU är mycket få, skr. 2016/17:72. Någon mätbar påverkan av en minskad lagringsskyldighet kommer därför inte att uppstå.

Kostnader för företagen

För de lagringsskyldiga inom it- och telekomområdet kommer det verka kostnadsdrivande att behöva anpassa sina datasystem till de nya förslagen. Operatörerna kommer även i vissa fall att behöva lagra många fler uppgifter än förut (om de använder NAT-teknik). Även

detta verkar kostnadsdrivande. Samtidigt innebär förslagen att många uppgifter som förut lagrades nu inte längre omfattas av lagringsskyldigheten. I sin helhet bedöms dock lagringsmassan öka och därmed operatörernas löpande kostnader. Det är svårt att ens uppskatta den ökade lagringsmassan som är hänförlig till NAT-tekniken. Olika beräkningar ger olika svar och om de ingående parametrarna varierar något så ger det stor påverkan på den slutliga produkten. Det finns uppskattningar på att en miljon kunder genrerar en NAT-relaterad lagring på 150 terabyte per månad.[2] En annan uppgift som förekommit är att NAT-relaterad lagring för samtliga svenska mobilabonnemang skulle uppgå till drygt 80 terabyte per månad.[3] Operatörerna själva har för utredningen uppgett att den extra lagringen för NAT skulle uppgå till 30 terabyte per månad för en normalstor internetleverantör. Oavsett vilken siffra som hamnar närmast verkligheten kan det konstateras att själva lagringskapaciteten inte kommer att medföra särskilt betungande investeringar även om man beaktar att särskilda krav ställs på stabilitet och säkerhet. Det ska anmärkas att datautrymme är billigare i dag än vad det var när datalagringsskyldigheten infördes.

I samband med att den nya regleringen införs kan det komma att behövas kostnadskrävande anpassningar för att datasystemen ska kunna klara av att hantera de potentiellt miljardtals uppgifter kopplade till NAT-teknik som kan bli nödvändiga att lagra. Operatörerna har å ena sidan för utredningen uppgett att ett sådant genomförande skulle medföra att kostnaderna skulle skjuta i höjden och hamna på helt orimliga nivåer, inte minst mot bakgrund av att operatörerna redan har gjort dyra investeringar i datalagringssystem grundat på den lagringsskyldighet som följer av dagens reglering. Å andra sidan har någon operatör uppgett att systemet i princip redan finns på plats, eftersom NAT-tekniken infördes medan datalagringsdirektivet fortfarande var gällande.

Även om operatörerna inte har förmått att kvantifiera kostnaderna som kommer att uppstå på grund av utredningens förslag är det uppenbart att de kommer att öka – i vart fall för de operatörer

[2] The Internet Engineering Task Force, Network Working Group https://tools.ietf.org/id/draft-donley-behave-deterministic-cgn-01.html, 18 januari 2012.
[3] PTS rapport från ÅF: NAT i mobila nätverk, 23 november 2015.

som använder NAT-teknik. Frågan är hur dessa kostnader ska fördelas.

Den nuvarande modellen för kostnadsfördelning mellan det allmänna och operatörerna innebär att operatörerna står för kostnaderna för anpassning, drift och underhåll och de brottsbekämpande myndigheterna betalar en ersättning till operatörerna vid varje utlämnande av uppgifter. Denna ordning har sin utgångspunkt i ställningstagandet att det finns verksamhetsområden där samhället, som en förutsättning för att tillåta ett företag att driva näringsverksamhet, kräver att vissa samhälleliga intressen beaktas (prop. 2010/11:46 s. 67). Förutom att vila på detta principiella ställningstagande har en sådan modell för kostnadsfördelning även samhällsekonomiska fördelar. Den part som har möjlighet att påverka kostnaden har nämligen också ett ansvar för den. Operatörernas tekniska och administrativa kompetens på området utnyttjas härigenom, samtidigt som de har ett tydligt incitament att hålla kostnaderna för anpassning och drift nere. Med denna modell får de brottsbekämpande myndigheterna dessutom ett incitament att inhämta trafik- och lokaliseringsuppgifter bara då de anser det vara en effektiv metod som kan förväntas föra utredningsarbetet framåt. En sådan modell har tidigare bedömts som samhällsekonomiskt kostnadseffektiv (prop. 2010/11:46 s. 68). Utredningen delar denna bedömning. Eftersom ingen av de författningsändringar som utredningen föreslår rubbar den ovan redovisade utgångspunkten eller de ovan redovisade fördelarna bör den gällande modellen för kostnadsfördelning inte frångås. Det innebär att operatörerna alltjämt ska stå för kostnader för anpassning (och drift och underhåll) samtidigt som det allmänna ska ersätta operatörerna för de kostnader som hänför sig till utlämnande av uppgifter i enskilda ärenden.

Som redovisas ovan är operatörsbranschen mycket heterogen och består av en mängd olika företag sett till t.ex. verksamhetsnisch, omsättning och marknadsandel (avsnitt 13.1.1). Det skulle därför kunna antas att de har olika förutsättningar för att kunna anpassa sig till de förändrade reglerna. Det ska emellertid vägas in att datasystem kontinuerligt behöver översyn och uppdateringar, varför de förändringar som behövs med anledning av förslagen inte nödvändigtvis driver kostnaderna särskilt mycket utöver vad som annars skulle blivit fallet.

Utredningens bedömning är att både små och stora företag kommer att ha liknande förutsättningar att kunna anpassa sig till ett förändrat regelverk. Utredningen bedömer alltså att förslagen inte kommer att få någon betydande konkurrenspåverkan inom gruppen av operatörer och nätägare.

Det ska framhållas att verksamheter som enbart erbjuder tjänster inom fast telefoni helt kommer att undantas från lagringsskyldighet. Dessa företag måste genomföra systemanpassningar för att upphöra med lagringen samtidigt som de nu föreslagna ändringarna medför en viss besparing i längden. Någon större sammantagen påverkan på dessa operatörer förväntas därför inte.

13.1.3 Offentligfinansiella effekter

Ingen förändrad kostnad för inhämtningen

Den nuvarande regleringen för inhämtning av uppgifter från operatörerna innehåller regler om ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut (6 kap. 16 e § LEK). Hur stor denna ersättning är bestäms av PTS (46 § FEK).

Det kan å ena sidan antas att förändringarna gör att myndigheterna i något enstaka fall avstår ifrån att ställa en fråga till en operatör om den uppgift de eftersöker inte längre lagras. Å andra sidan kan det antas att myndigheterna i vissa andra fall kommer att behöva ställa fler frågor för att få den fullständiga bilden eftersom svaret på varje fråga nu blir något mindre informationsrik. Sammantaget gör utredningen bedömningen att kostnaderna som uppstår för myndigheterna när lagrade uppgifter begärs ut inte kommer att påverkas på något märkbart sätt.

Ökade kostnader för Åklagarmyndigheten

Åklagare föreslås få en roll vid beslutsfattande enligt IHL. Förslaget innebär att Åklagarmyndigheten kommer att få ökade kostnader, dels i form av ökade löpande kostnader för personal, dels i form av engångskostnader för it-anpassningar och utbildningar.

Totalt sett meddelades det 855 beslut enligt IHL under år 2016. Det vill säga cirka 16 beslut i veckan. Även om kostnaden för den

personalförstärkning som behövs för detta inte fullt ut motsvarar en heltidsarbetskraft måste det tas med i beräkningen att vissa beslut kommer att behöva fattas under obekväm arbetstid; i vart fall måste det finnas en beredskap för att kunna fatta sådana beslut. Åklagarmyndigheten bör därför få ett årligt tillskott om 1 miljon kronor.

Härutöver måste Åklagarmyndigheten anpassa sina it-system, ta fram nya beslutsmallar och utöka kompetensen på området. I viss utsträckning kan anpassningen av it-systemen göras inom ramen för sedvanlig uppdatering och utveckling. Det är emellertid nu fråga om att införa ett system som skiljer sig från vad som används i förundersökningsverksamheten och som möjligen kommer att kräva en högre grad av säkerhet. Kostnaden för systemanpassning kommer därför inte helt att kunna tas inom ramen för den sedvanliga it-utvecklingen.

Det är svårt att närmare uppskatta de framtida kostnaderna för Åklagarmyndigheten för att anpassa sina it-system och utbilda sin personal. Som en jämförelse kan nämnas att när Ekobrottsmyndigheten ålades att utföra statens talan i fråga om skattetillägg så uppskattades kostnaden för it-anpassning och utbildning till en engångskostnad om 4 miljoner kronor (prop. 2014/15:131 s. 239). I sammanhanget bör dock beaktas att arbetsuppgiften att föra talan om skattetillägg ligger något längre ifrån Ekobrottsmyndighetens kärnområde än vad beslut enligt IHL ligger jämfört med Åklagarmyndighetens kärnområde. Det får antas att en verksamhetsanpassning blir billigare ju närmare den nya arbetsuppgiften ligger den verksamhet som redan bedrivs inom myndigheten.

Mot den ovan tecknade bakgrunden gör utredningen bedömningen att Åklagarmyndigheten kommer att behöva 3 miljoner kronor extra för de initiala kostnaderna i form av utbildning och it-anpassningar.

Även om det nu inte är fråga om en verksamhetsflytt i den meningen att saken ska underställas riksdagens prövning enligt budgetregelverket så innebär den nya beslutsordningen enligt IHL vissa besparingar för Polismyndigheten, Säkerhetspolisen och Tullverket, men förmodligen inte fullt ut i samma utsträckning som kostnader uppstår för Åklagarmyndigheten. Trots detta föreslår utredningen att de resurser som Åklagarmyndigheten ska tillföras tillgängliggörs genom en höjning av Åklagarmyndighetes ramanslag och motsvarande minskning hos de nämnda myndigheterna. Med

beaktande av myndigheternas relativa användning av IHL finner utredningen att 50 procent bör belasta Polismyndigheten (1,5 miljoner kronor för engångssumman och 500 000 kronor för den löpande ramhöjningen), 30 procent Tullverket (900 000 kronor för engångssumman och 300 000 kronor för den löpande ramhöjningen) och 20 procent Säkerhetspolisen (600 000 kronor för engångssumman och 200 000 kronor för den löpande ramhöjningen).

13.1.4 Inga konsekvenser för miljön

En miljökonsekvensanalys har gjorts utifrån de riktlinjer som upp-ställts av Regeringskansliet. Utredningen bedömer att förslagen inte får någon miljöpåverkan.

13.1.5 Inga övriga konsekvenser

Förslagen bedöms inte få några ytterligare sådana konsekvenser som anges i kommittéförordningen (1998:1474).

13.1.6 Ingen anmälningsskyldighet för tekniska föreskrifter

Enligt Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster har medlemsstater en skyldighet att offentligt tillkännage om en ny nationell teknisk föreskrift har antagits. Det nu nämnda direktivet är dock inte tillämpligt på teletjänster, artikel 1.3 och Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv). Någon anmälningsskyldighet kommer således inte att uppkomma med anledning av de föreslag utredningen lämnar.

13.2 Ikraftträdande

Utredningens förslag: Den föreslagna regleringen ska träda i kraft den 1 december 2018. Det ska införas en övergångsbestämmelse för lagringsskyldigheten för annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare vid internetåtkomst. Den bestämmelsen ska inte behöva tillämpas förrän den 1 april 2019.

Med beaktande av Tele2-domen och den osäkerhet som till följd av domen råder kring gällande rätt är det viktigt att författningsförslagen genomförs så snart som möjligt. Samtidigt måste det beaktas att förslagen rör komplexa frågor inom ett viktigt område och att den efterföljande beredningen därför måste tillåtas ta viss tid. Det ska även beaktas att vissa operatörer kan behöva göra tidskrävande förändringar i sina datalagringssystem. Vid en avvägning mellan dessa intressen föreslår utredningen att förslagen ska träda i kraft den 1 december 2018.

Reglerna ska börja tillämpas genast vid ikraftträdandet. Några särskilda övergångsbestämmelser är inte nödvändiga förutom såvitt avser lagringsskyldigheten för annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare (del av 39 § första stycket 1 FEK). Detta led av bestämmelsen bedöms kräva mest omfattande systemanpassningar hos de lagringsskyldiga. Det bör därför inte finnas någon skyldighet att tillämpa den delen av bestämmelsen före den 1 april 2019.

14 Författningskommentar

14.1 Förslaget till lag om ändring lagen (2003:389) om elektronisk kommunikation

6 kap.

16 d §

Uppgifter som avses i 16 a § ska lagras *den tid regeringen föreskriver dock som längst i tio* månader räknat från den dag kommunikationen avslutades. Vid utgången av denna tid ska den lagringsskyldige genast utplåna dem, om annat inte följer av andra stycket.

Om uppgifter som avses i första stycket begärts utlämnade före utgången av den föreskrivna lagringstiden men uppgifterna inte har hunnit lämnas ut, ska den lagringsskyldige lagra uppgifterna till dess så har skett och därefter genast utplåna de lagrade uppgifterna.

Första stycket är ändrat. Ändringen är föranledd av att lagringstiderna för uppgifterna differentieras. Övervägandena finns i avsnitt 12.7.1.

Regeringen bestämmer hur långa lagringstiderna ska vara, 41 § FEK. Den angivna lagringstiden om tio månader utgör en längsta tillåtna tid för hur länge uppgifterna får lagras. Lagringstiderna ska bestämmas efter vad som är proportionerligt och får inte vara längre än vad som är strängt nödvändigt. Hänsyn ska tas till de brottsbekämpande myndigheternas behov och nytta av uppgiften samt till hur integritetskänslig den är.

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

4 §

Beslut om inhämtning av uppgifter fattas av *åklagare efter ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket*.

Ändringen innebär att åklagare pekas ut som ansvariga för att fatta beslut enligt IHL. Det klargörs också att ansökan ska komma från respektive myndighet. Övervägandena finns i avsnitt 12.8.4.

Som framgår av avsnitt 12.8.4 har åklagare som utgångspunkt generell befogenhet att utöva sitt ämbete, 6 § åklagarförordningen (2004:1265). Det finns dock skäl att för de nu aktuella ärendena begränsa kretsen av behöriga åklagare genom myndighetsinterna föreskrifter. Den skulle t.ex. kunna begränsas till åklagare vid Riksenheten för säkerhetsmål, någon funktion på huvudkontoret eller på något annat sätt. Det ankommer på Åklagarmyndigheten att tillse att lämpliga sådana förskrifter beslutas. Det bör för tydlighets skull nämnas att det inte nu är fråga om att anförtro beslutanderätten till s.k. tullåklagare vid Tullverket.

5 §

I ett beslut om inhämtning av uppgifter ska det anges vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet avser. Tiden får inte bestämmas längre än nödvändigt och får, när det gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.

Om det inte längre finns skäl för ett beslut om inhämtning av uppgifter, ska beslutet omedelbart hävas *av den ansökande myndigheten*.

Paragrafen ändras som en följd av att åklagare blir behöriga att fatta beslut enligt IHL. Övervägandena finns i avsnitt 12.8.4.

I andra stycket anges att det fortfarande är Polismyndigheten, Säkerhetspolisen och Tullverket som har en rätt och en skyldighet

att bevaka behovet av inhämtningen och att beslutet omedelbart ska hävas om det inte längre finns behov av åtgärden.

6 §

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.

Underrättelse enligt första stycket ska fullgöras av den ansökande myndigheten.

Andra stycket är nytt. Ändringen innebär att det alltjämt är de ansökande myndigheterna (Polismyndigheten, Säkerhetspolisen och Tullverket) som har ansvar för att SIN underrättas om ett beslut om inhämtning. Övervägandena finns i avsnitt 12.8.4.

14.3 Förslaget till förordning om ändring i förordningen (2003:396) om elektronisk kommunikation

37 §

Den som är skyldig att lagra uppgifter enligt 6 kap. 16 a § lagen (2003:389) om elektronisk kommunikation ska vidta de åtgärder som krävs 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.

Den lagringsskyldige ska vidta de åtgärder som krävs för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring. Sådana åtgärder ska även vidtas för att förhindra otillåten lagring, behandling av eller tillgång till och otillåtet avslöjande av uppgifterna. Uppgifterna får göras tillgängliga endast för personal med särskild behörighet.

Uppgifterna får inte lagras utanför Sverige.

Post- och telestyrelsen får, efter att ha hört Polismyndigheten, Säkerhetspolisen och Datainspektionen, meddela närmare föreskrifter om de åtgärder som ska vidtas enligt första och andra styckena.

Tredje stycket är nytt. Övervägandena finns i avsnitt 12.10.2. Ändringen innebär att de uppgifter som lagras enligt 6 kap. 16 a § LEK inte får lagras utanför Sverige.

38 §

För att fullgöra lagringsskyldigheten i 6 kap. 16 a § lagen (2003:389) om elektronisk kommunikation ska den lagringsskyldige lagra de uppgifter som anges i 39 *och 40* §§.

Paragrafen är ändrad till följd av att 39 § ersatt tidigare 43 § och 40 § ersatt tidigare 39–42 §§.

39 §

När det gäller *internetåtkomst* ska följande lagras:

1. användares ip-adress och annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare,

2. uppgifter om abonnent och registrerad användare,

3. datum och spårbar tid för på- och avloggning i tjänsten som ger internetåtkomst, och

4. uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten.

Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten är någon som inte omfattas av 6 kap. 16 a § lagen (2003:389) om elektronisk kommunikation, ska första stycket 4 gälla för den som avskiljer kommunikationen till den som slutligt avskiljer kommunikationen till den enskilda abonnenten.

Paragrafen reglerar vilka uppgifter som ska lagras för internetåtkomst. Den ersätter tidigare 43 §. Övervägandena finns i avsnitt 12.6.4.

De uppgifter som ska lagras regleras i *första stycket* och är med något undantag desamma som i nuvarande 43 §, även om någon språklig ändring gjorts. En betydande ändring har emellertid gjorts av styckets första punkt.

Enligt *första punkten* ska användarens ip-adress lagras. Till skillnad från vad som gäller i dag, ska även uppgift som är nödvändig för att identifiera abonnent och registrerad användare lagras. Ändringen är föranledd av att många operatörer använder sig av NAT-teknik där

flera abonnenter använder samma publika ip-adress. För att kunna identifiera rätt abonnent eller registrerad användare krävs därför i vissa fall att även flera ip-adresser och andra uppgifter lagras. Vilka uppgifter som ska lagras är beroende av vilken teknik som operatören använder men det kan t.ex. vara publik och lokal ip-adress (dvs. den som används mellan abonnent och internetleverantör) och port. Innehållet i kommunikation, destinations-ip (t.ex. vilka webbsidor en person besökt) eller annan information om hur användaren trafikerat internet får inte lagras med stöd av denna bestämmelse. Detsamma gäller uppgifter som kan härleda hur trafiken gått efter att den avskilts till abonnenten eller den registrerade användaren, t.ex. den ip-adress som tilldelas en enhet inom ett hemmanätverk. Tidsuppgifter torde däremot vara nödvändiga att lagra. Om ip-adress eller annan uppgift som omfattas av bestämmelsen ändras under pågående uppkoppling ska även de nya uppgifterna lagras. Att både ip-adress och uppgift står i singular utesluter inte att flera ip-adresser eller att flera andra uppgifter kan behöva lagras för att uppfylla kravet på att uppgifterna ska möjliggöra identifikation av abonnenten eller den registrerade användaren. Bestämmelsen innebär inte att uppgifter ska lagras om anonymiseringstjänster som aktiveras först efter internetåtkomst, t.ex. VPN (Virtual Private Network). PTS bör i enlighet med 44 § utfärda närmare föreskrifter om vilka närmare uppgifter som enligt denna bestämmelse ska lagras.

Av *andra punkten* följer att uppgifter om abonnent och registrerad användare ska lagras. De uppgifter som avses är t.ex. namn, adress och person- eller organisationsnummer. Att ”i förekommande fall” inte längre anges för registrerad användare beror på att alla uppgifter ska lagras endast i förekommande fall. Någon ändring i sak är alltså inte avsedd. Finns det flera abonnenter eller registrerade användare ska uppgifter om samtliga dessa lagras.

I *tredje punkten* regleras vilka tidsuppgifter som ska lagras. Med spårbartid avses tidsangivelse där förhållandet till UTC (SP) (den tillämpning av den internationella tidsskalan UTC som används i Sverige) framgår. Uppgiften ska vara så precis som möjligt.

Fjärde punkten innebär att uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ska lagras. Den utrustning som avses är den sista utrustningen inom den lagringsskyldiges kontroll. Vid fast internetåtkomst innebär det t.ex. fibermodem eller telefonjack och

vid mobil internetåtkomst utrustning i baststationen, oftast en cell, eller en router vid ett allmänt trådlöst nätverk. Uppgift som kan identifiera utrustningen kan vara ett unikt identitetsnummer, t.ex. MAC-adress, eller annan uppgift om utrustningens identitet som genereras eller behandlas av den lagringsskyldige i samband med internetåtkomsten. Vid mobil internetåtkomst motsvarar uppgifterna i princip lokaliseringsuppgifter vid telefonitjänst.

Av *andra stycket* framgår att om den som slutligt avskiljer kommunikationen till den enskilda abonnenten är någon som inte omfattas av 6 kap. 16 a § (dvs. inte omfattas av lagringsskyldigheten) ska det lagras uppgifter som identifierar utrustningen vid den punkt där kommunikationen avskiljs till den som slutligt avskiljer kommunikationen till den enskilda abonnenten, i stället för vid den punkt där kommunikationen avskiljs till den enskilda abonnenten. Bestämmelsen gäller alltså punkten mellan å ena sidan det sista i kedjan av nät som ägs av någon som omfattas av lagringsskyldigheten och å andra sidan ett nät som inte omfattas av lagringsskyldigheten.

40 §

När det gäller telefonitjänst *och meddelandehantering* via en mobil nätanslutningspunkt ska följande lagras:

1. uppringande och uppringt nummer eller motsvarande adress,

2. såvitt avser telefonitjänst uppringandes och uppringds abonnemangsidentitet och utrustningsidentitet,

3. uppgifter om abonnent och registrerad användare som uppgifterna i 1 och 2 kan hänföras till,

4. datum och spårbar tid då kommunikationen påbörjades och avslutades eller ett meddelande skickades och mottogs,

5. såvitt avser telefonitjänst lokaliseringsuppgifter då kommunikationen påbörjades och avslutades, och

6. datum, spårbar tid och lokaliseringsuppgifter för den första aktiveringen av en förbetald anonym tjänst.

Paragrafen reglerar vilka uppgifter som ska lagras för telefoni- och meddelandetjänster. Den ersätter nuvarande 39–42 §§. Övervägandena finns i avsnitt 12.6.3.

Av paragrafens inledning framgår att endast kommunikation via en mobil nätanslutningspunkt omfattas av lagringsskyldigheten. Med mobil nätanslutningspunkt avses t.ex. en mobiltelefon som kopplar

upp mot en mobilmast eller ett mot wifi som tillhandahålls av någon som omfattas av lagringsskyldigheten, men inte när en mobiltelefon ansluter till ett privat trådlöst nätverk. Om endast en av parterna kommunicerar mobilt (t.ex. med en mobiltelefon eller en dator med mobilt bredband) ska den partens operatör lagra uppgifterna, men inte operatören för den part som kommunicerar via fast anslutning. Det torde i vissa fall kunna uppstå situationer när den lagringsskyldige inte har all information som krävs för att avgöra om lagringsskyldighet har inträtt för en viss kommunikation. Det kan t.ex. vara så att det saknas information om huruvida ett meddelande har skickats från en mobil eller fast nätanslutning. Ett sådant exempel kan, beroende på teknisk lösning, vara att en operatörs e-posttjänst används av någon som är uppkopplad mobilt genom en annan operatör. I dessa fall ska inte uppgifterna lagras.

Flera uppgifter omfattas inte längre av lagringsskyldigheten. De uppgifter som fortfarande ska lagras motsvarar respektive uppgift enligt nuvarande lydelser, även om någon språklig ändring gjorts.

Första punkten innebär att det nummer eller annan adress som har använts för att inleda kommunikationen och som är målet för kommunikationen ska lagras. Oftast är uppringande och uppringd adressen av samma slag. Uppringt nummer eller motsvarande adress avser den adress som användaren anger för att initiera en kommunikation med motparten. För telefonitjänst är det ett telefonnummer (E.164-nummer) och för meddelandehantering kan det t.ex. vara ett telefonnummer, användarnamn eller en e-postadress. Lagringsskyldigheten innefattar även icke fullständiga nummer som slagits och s.k. skräppost (som hamnar direkt i mottagarens mapp för skräppost eller borttagna meddelanden). Däremot omfattas inte meddelanden som filtreras bort av tjänsteleverantören och därmed aldrig når mottagaren. Kommunikation via telefoni- och meddelandetjänster som tillhandadahålls av någon som inte omfattas av 6 kap. 16 a § LEK, t.ex. via Whatsapp eller Hotmail, omfattas inte av lagringsskyldigheten.

Av *andra punkten* följer att abonnemangs- och utrustningsidentitet ska lagras vid telefonitjänst. En vanligt förekommande abonnemangsidentitet för mobiltelefoner är IMSI-nummer. Utrustningsidentitet kan vara t.ex. IMEI-nummer och MAC-adress.

Enligt *tredje punkten* ska uppgifter om abonnent och registrerad användare lagras. De uppgifter som avses är t.ex. namn, adress och

person- eller organisationsnummer. Att ”i förekommande fall” inte längre anges för registrerad användare beror på att alla uppgifter ska lagras endast i förekommande fall. Någon ändring i sak är alltså inte avsedd. Finns det flera abonnenter eller registrerade användare ska uppgifter om samtliga dessa lagras.

I *fjärde punkten* regleras vilka tidsuppgifter som ska lagras. Med spårbar tid avses tidsangivelse där förhållandet till UTC (SP) (den tillämpning av den internationella tidsskalan UTC som används i Sverige), framgår. Uppgiften ska vara så precis som möjligt.

Av *femte punkten* framgår att lokaliseringsuppgifter ska lagras, men bara vid telefonitjänst. Så precis uppgift som möjligt ska lagras, vilket för närvarande oftast torde vara kommunicerande cell tillsammans med cellens position och riktning, dvs. det geografiska område som cellen täcker. Även vid t.ex. publika trådlösa nätverk, som tillhandahålls av en lagringsskyldig, ska motsvarande uppgifter lagras.

Enligt *sjätte punkten* ska uppgifter som genereras vid den första aktiveringen av en förbetald anonym tjänst (oregistrerat kontantkort) lagras. Uppgifterna ska fortsätta lagras hela lagringstiden även om den förbetalda tjänsten registreras efter aktiveringen.

41 §

Med stöd av 6 kap. 16 d § lagen (2003:389) om elektronisk kommunikation förordnas att:

1. uppgifter som avses i 39 § första stycket 1–3 ska lagras i tio månader,

2. uppgifter som avses 39 § första stycket 4 och andra stycket samt 40 § 1–4 och 6 ska lagras i sex månader, och

3. uppgifter som avses i 40 § 5 ska lagras i två månader.

Paragrafen reglerar lagringstiderna för uppgifterna som ska lagras enligt 39 och 40 §§. Övervägandena finns i avsnitt 12.7.2.

44 §

Post- och telestyrelsen får meddela närmare föreskrifter *som rör* de uppgifter som ska lagras enligt 39 *och 40* §§. *Post- och telestyrelsen får också meddela föreskrifter om vilka närmare uppgifter som ska lagras enligt 39 och 40 §§.*

Övervägandena finns i avsnitt 12.6.6.

Paragrafen är ändrad till följd av att 39 § ersatt tidigare 43 § och 40 § ersatt tidigare 39–42 §§.

Ändringen i *första meningen* till formuleringen ”som rör” är endast för paragrafen ska bli mer lättläst med den nya andra meningen. PTS behörighet har förtydligats i *andra meningen*. PTS har enligt bestämmelsen behörighet att föreskriva vilka exakta uppgifter som ska lagras för att lagringsskyldigheten enligt respektive paragraf och punkt ska vara uppfylld. Bestämmelsen blir främst relevant för 39 § första stycket 1, se ovan kommentar till den bestämmelsen. Man kan dock tänka sig att teknikutveckling eller andra omständigheter nödvändiggör föreskrifter även för andra delar av lagringsskyldigheten. Som framgår av avsnitt 12.6.6 ska lagringsskyldighetens ramar framgå i lag. PTS kan alltså inte utvidga lagringsskyldigheten med stöd av denna bestämmelse, varken i förhållande till lag eller förordning.

1. Denna förordning träder i kraft den 1 december 2018.

2. Lagringsskyldigheten enligt 39 § första stycket 1 om annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare behöver inte tillämpas förrän den 1 april 2019.

Övervägandena kring övergångsbestämmelserna finns i avsnitt 13.2.

Övergångsbestämmelserna innebär att förordningen träder i kraft den 1 december 2018. Den del av 39 § första stycket 1 FEK som innebär att de lagringsskyldiga ska lagra annan uppgift som är nödvändig för att identifiera abonnent och registerad användare behöver inte tillämpas före den 1 april 2019. Det innebär att de övriga uppgifter som avses i 39 § första stycket 1 (t.ex. portnummer) omfattas av lagringsskyldigheten först från och med den 1 april 2019. Det finns dock inget hinder för en lagringsskyldig, som är klar med sin systemanpassning, att påbörja lagringen dessförinnan.

Källförteckning

Offentligt tryck

Direktiv

Dir. 2014:101 Översyn av vissa bestämmelser om elektronisk kommunikation i brottsbekämpningen.

Dir. 2016:21 Genomförande av EU:s direktiv om skydd av personuppgifter vid brottsbekämpning, brottmålshantering och straffverkställighet.

Dir. 2016:36 Hemlig dataavläsning.

Dir. 2017:32 Utkontraktering av säkerhetskänslig verksamhet, sanktioner och tillsyn – tre frågor om säkerhetsskydd.

Utredningsbetänkanden och promemorior

SOU 1984:54 Tvångsmedel – Anonymitet – Integritet.

SOU 2005:38 Tillgång till elektronisk kommunikation i brottsutredningar m.m.

SOU 2007:22 Skyddet för den personliga integriteten – kartläggning och analys.

SOU 2007:76 Lagring av trafikuppgifter för brottsbekämpning.

SOU 2009:1 En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen.

SOU 2009:70 Utvärdering av buggning och preventiva tvångsmedel.

SOU 2010:103 Särskilda spaningsmetoder.

SOU 2012:44 Hemliga tvångsmedel mot allvarliga brott.

SOU 2013:39 Europarådets konvention om it-relaterad brottslighet.

Ds 2014:23 Datalagring, EU-rätten och svensk rätt.

SOU 2015:31 Datalagring och integritet.

SOU 2016:65 Ett samlat ansvar för tillsyn över den personliga integriteten.

SOU 2017:29 Brottsdatalag.

SOU 2017:57 Lag om flygpassageraruppgifter i brottsbekämpningen.

SOU 2017:52 Så stärker vi den personliga integriteten.

Propositioner och regeringens skrivelser

Prop. 1988/89:124 Om vissa tvångsmedelsfrågor.

Prop. 1990/91:118 Förslag till lag om särskild kontroll av vissa utlänningar, m.m.

Prop. 2002/03:74 Hemliga tvångsmedel – offentliga ombud och en mer ändamålsenlig reglering.

Prop. 2002/03:110 Lagen om elektronisk kommunikation, m.m.

Prop. 2005/06:173 Översyn av personuppgiftslagen.

Prop. 2005/06:177 Åtgärder för att förhindra vissa särskilt allvarliga brott.

Prop. 2006/07:63 En anpassad försvarsunderrättelseverksamhet.

Prop. 2006/07:133 Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m.

Prop. 2009/10:80 En reformerad grundlag.

Prop. 2009/10:85 Integritet och effektivitet i polisens brottsbekämpande verksamhet.

Prop. 2010/11:46 Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG.

Prop. 2011/12:55 De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.

Prop. 2011/12:146 Skyddsåtgärder för trafikuppgifter lagrade för brottsbekämpande ändamål.

Skr. 2012/13:47 Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2011.

Prop. 2013/14:237 Hemliga tvångsmedel mot allvarliga brott.

Skr. 2016/17:69 Redovisning av användningen av hemliga tvångsmedel under år 2015.

Skr. 2016/17:72 2016 års redogörelse för tillämpningen av lagen om särskild utlänningskontroll.

Prop. 2016/17:113 Viktigt meddelande till allmänheten via telefon.

Prop. 2016/17:180 En modern och rättssäker förvaltning – ny förvaltningslag.

Prop. 2016/17:186 Fortsatt giltighet av en tidsbegränsad bestämmelse i inhämtningslagen.

Utskottsbetänkanden

Bet. 1981/82:JuU54 Om parlamentarisk kontroll i fråga om telefonavlyssning.

Bet. 2011/12:JuU8 De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.

Bet. 2011/12:JuU26 Skyddsåtgärder för trafikuppgifter lagrade för brottsbekämpande ändamål.

Bet. 2016/17:FöU12 Viktiga meddelanden till allmänheten via telefon.

Bet. 2017/18:KU2 En modern och rättssäker förvaltning – ny förvaltningslag.

Rättsfall

Högsta domstolen

NJA 2010 s. 122.

NJA 2015 s. 631.

Kammarrätten

RK 2010:1.

Tele2 Sverige AB mot Post- och telestyrelsen, mål 7380-14, 12 maj 2015.

Post- och telestyrelsen mot Bahnhof AB, mål 2699-16, 16 juni 2016.

Post- och telestyrelsen mot Bahnhof AB, mål 3256-17, 9 juni 2017.

Tele2 Sverige AB mot Post- och telestyrelsen, mål 7380-14, 22 december 2016.

Förvaltningsrätten

Tele2 Sverige AB mot Post- och telestyrelsen, mål 14891-14, 13 oktober 2014.

Bahnhof AB mot Post- och telestyrelsen, mål 6895-16, 7 april 2016.

Bahnhof AB mot Post- och telestyrelsen, mål 6895-16, 5 maj 2017.

EU-domstolen

Åkerberg Fransson, mål C-617/10, 26 februari 2013.

Digital Rights Ireland Ltd, mål C-293/12, och *Kärntner Landesregierung m.fl.*, C-594/12, 8 april 2014.

Maximillian Schrems, mål C-362/14, 6 oktober 2015.

Tele2 Sverige AB, mål C-203/15, och *Tom Watson m.fl.* mål C-698/15, 21 december 2016.

Tele2 Sverige AB, mål C-203/15, och *Tom Watson m.fl.* mål C-698/15, förslag till avgörande av generaladvokaten Henrik Saugmandsgaard Øe, 19 juli 2016.

EU-domstolens yttrande 1/15, 26 juli 2017.

Europadomstolen

Klass m.fl. mot Tyskland, mål 5029/71, 6 september 1978.

Leander mot Sverige, mål 9248/81, 26 mars 1987.

Kopp mot Schweiz, mål 23224/94, 25 mars 1998.

Osman mot Förenade kungariket, mål 23452/94, 28 oktober 1998.

Amann mot Schweiz, mål 27798/95, 16 februari 2000.

Rotaru mot Rumänien, mål 28341/95, 4 maj 2000.

P.G. och J.H. mot Förenade kungariket, mål 44787/98, 25 september 2001.

Greuter mot Nederländerna, mål 40045/98, beslut den 19 mars 2002.
von Hannover mot Tyskland, mål 59320/00, 24 juni 2004.
Segerstedt-Wiberg m.fl. mot Sverige, mål 62332/00, 6 juni 2006.
Weber och Saravia mot Tyskland, mål 54934/00, 29 juni 2006.
Dumitru Popescu mot Rumänien, (nr 2), mål 71525/01, 26 april 2007.
Liberty m.fl. mot Förenade Kungariket, mål 58243/00, 1 juli 2008.
K.U. mot Finland, mål 2872/02, 2 december 2008.
S. och Marper mot Förenade kungariket, mål 30562/04 och 30566/04, 4 december 2008.
Iordachi m.fl. mot Modaliven, mål 25198/02, 10 februari 2009.
Natunen mot Finland, mål 21022/04, 31 mars 2009.
Janatuinen mot Finland, mål 28552/05, 8 december 2009.
Kennedy mot Förenade kungariket, mål 26839/05, 18 maj 2010.
Uzun mot Tyskland, mål 35623/05, 2 september 2010.
Gillberg mot Sverige, mål 41723/06, 2 november 2010.
Söderman mot Sverige, mål 5786/08, 12 november 2013.
Dragojević mot Kroatien, mål 68955/11, 15 januari 2015.
Roman Zakharov mot Ryssland, mål 47143/06, 4 december 2015.
Szabó och Vissy mot Ungern, mål 37138/14, 12 januari 2016.

Övriga domstolar

Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Tyskland), mål 13 B 238/17, interimistiskt beslut, 22 juni 2017.
Acordam na 1.ª Secção do Tribunal Constitucional (Portugal), dom 420/2017, 13 juli 2017.

Myndighetspraxis

Säkerhets- och integritetsskyddsnämnden uttalande, dnr 169-2015, 18 november 2015.
Säkerhets- och integritetsskyddsnämnden uttalande, dnr 206-2015, 16 mars 2016.

Säkerhets- och integritetsskyddsnämnden uttalande, dnr 130-2016, 14 september 2016.

Litteratur

Danelius, Hans (2015) Mänskliga rättigheter i europeisk praxis, 5:e uppl.

Lindberg, Gunnel (2012) Straffprocessuella tvångsmedel, 3:e uppl.

Lindberg, Håkan (2009) Introduktion till IP – Internet Protocol, version 2.0.

Naarttijärvi, Markus (2013), För din och andras säkerhet, Konstitutionella proportionalitetskrav och Säkerhetspolisens preventiva tvångsmedel.

Naarttijärvi, Markus (2016), Övervakning av metadata som spelplan för rättsliga principkonflikter, ingår i antologin Övervakning och integritet : teknik, skydd och aktörer i det nya kontrollandskapet.

Övrigt

Article 29 data protection working party WP 220, 1 augusti 2014.

Article 29 data protection working party WP 237, 13 april 2016.

Cameron, Iain Balancing data protection and law enforcement needs: Tele2 Sverige and Watson, Common Market Law Review, kommande artikel 2017.

Europarådet resolution 1970, 29 januari 2014.

Europarådet rekommendationer 2033, 29 januari 2014.

Europarådet Report on European standards as regards the independence of the judicial system: Part II – The prosecution service adopted by the Venice commission, 17–18 december 2010.

Europarådet www.coe.int/en/web/portal/28-january-data-protection-day-factsheet

European Police Office (Europol) IOCTA 2016 Internet Organised Crime Threat Assessment, 2016.

Europeiska kommissionen Commission Staff Working Document, bilaga till det förslag till direktiv som ledde fram till antagandet av

direktiv 2006/24, SEK(2005) 1131, 21 september 2005, celexnummer: 52005SC1131.

Europeiska kommissionen Utvärderingsrapport av direktiv 2006/24, celexnummer: 52011DC0225.

Europeiska unionens råd Rådets slutsatser om vägen till ett förbättrat informationsutbyte och säkerställande av interoperabiliteten mellan EU:s informationssystem, 10151/17, 8 juni 2017.

Finska Kommunikationsministeriet Rapporter och utredningar 9/2017.

Förenta nationerna Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, A/HRC/27/37, 30 juni 2014.

The Internet Engineering Task Force Network Working Group https://tools.ietf.org/id/draft-donley-behave-deterministic-cgn-01.html, 18 januari 2012.

Internetstiftelsen i Sverige Svenskarna och internet 2016.

Leswing, Kif Apple says people send as many as 200,000 iMessages per second, Business insider, 12 februari 2016.

Necessary and Proportionate https://necessaryandproportionate.org

OECD OECD Digital Economy Outlook 2015, december 2015.

Polismyndigheten och *Tullverket* Drogsituationen i Sverige, 2016.

Post- och telestyrelsen skrivelse till Ekobrottsmyndigheten, dnr 15-1185, 26 februari 2015.

Post- och telestyrelsen NAT i mobila nätverk, 23 november 2015.

Post- och telestyrelsen Svenskarnas användning av telefoni och internet 2015, PTS-ER-2015:29, 10 december 2015.

Post- och telestyrelsen Svensk Telekommarknad 2016, PTS-ER-2017:10, 22 maj 2017.

Privacy International National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, september 2017.

Säkerhets- och integritetsskyddsnämnden årsredovisning 2015.

Säkerhets- och integritetsskyddsnämnden årsredovisning 2016.

Åklagarmyndigheten Redovisning av användningen av vissa hemliga tvångsmedel under 2016, 31 maj 2017.

Särskilda yttranden

Särskilt yttrande av Jonas Agnvall

Sammanfattning

Jag kan inte stå bakom utredningens förslag till lagring av information om användares kommunikation eftersom jag anser att en sådan lagringsskyldighet går utöver vad som är strängt nödvändigt och kan anses motiverat i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i direktiv 2002/58 jämfört med artiklarna 7, 8, 11 och 52.1 i EU:s rättighetsstadga. Därtill anser jag att utredningen, i större utsträckning, bort analysera räckvidden av EU-domstolens dom i Tele2-målet[1] och dess påverkan på hanteringen av s.k. abonnemangsuppgifter. I de följande två avsnitten utvecklar jag mina synpunkter.

Lagring av information om användares kommunikation

En mycket viktig fråga sedan EU-domstolen meddelade sin dom är vilket utrymme som den nationella lagstiftaren har att föreskriva att operatörerna ska lagra information om användarnas kommunikation. EU-domstolen har tydligt uttryckt att lagringen av information inte får, med hänsyn till artikel 15.1 i direktiv 2002/58, vara en huvudregel[2]. Den s.k. artikel 29-gruppen har också, redan före domen, uttalat att masslagring av data inte kan anses som proportionellt[3]. Datainspektionen har också i ett tidigare remissvar över utredningen

[1] Dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15.
[2] Se skäl 104 i Tele2-målet.
[3] WP 237 s. 12 ”…recalls that it has consistently considered that massive and indiscriminate collection of data (non-targeted bulk collection) in any case cannot considered as proportionate”.

Datalagring och integritet (SOU 2015:31) hänvisat till 29-gruppens uttalande med anledning av Digital Rights-domen[4], i vilken det framhålls särskilt att datalagringsreglerna 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[5].

Enligt min mening innebär utredningens förslag till ändrade bestämmelser att lagringen av information om kommunikationen fortfarande kommer att vara en huvudregel, vilket i enlighet med vad EU-domstolen uttalat i Tele2-målet går utöver vad som är acceptabelt enligt direktiv 2002/58 och EU:s rättighetsstadga. Den differentiering som utredningen föreslår är långt ifrån tillräcklig. Vad lagringsskyldigheten kallas är inte väsentligt, det är dess effekter som är avgörande. Jag kan konstatera att det fortfarande är fråga om en generell och till stor del odifferentierad lagring som omfattar väldigt stora mängder trafikuppgifter och lokaliseringsuppgifter för samtliga abonnenter och nästan alla elektroniska kommunikationsmedel. De nya begränsningar som föreslås av utredningen, t.ex. att fast telefoni inte ska omfattas, är närmast att betrakta som marginella i sammanhanget i förhållande till den tekniska utvecklingen och användarmönster. Lagringen berör fortfarande på ett allomfattande sätt personer som använder elektroniska kommunikationstjänster utan att dessa personer ens indirekt befinner sig i en situation som kan föranleda lagföring. Det går inte ihop med EU-domstolens tolkning vilken bland annat uttalar att de materiella villkoren i den nationella lagstiftningen måste vara sådana att den klart avgränsar åtgärdens omfattning och följaktligen den berörda personkretsen[6].

Vilka möjligheter finns då för fortsatt lagring av information? I skälen för EU-domstolen ett resonemang kring riktad lagring. Utredningen har dock avfärdat en riktad lagring som en framkomlig lösning.

För det första anser utredningen att EU-domstolens argumentation kring riktad lagring är att närmast betrakta som obiter dictum dvs. uttalande som inte är relevant för rättsfrågan som prövas. Utredningens resonemang framstår här som forcerat, där syftet med

[4] Domstolens dom den 8 april 2014 i de förenade målen C-293/12 och C-594/12.
[5] Se Datainspektionens remissyttrande daterat den 28 augusti 2015, dnr 902-2015.
[6] Se skäl 110.

att EU-domstolen för en argumentation kring riktad lagring inte har analyserats tillräckligt. Utredningen har även bort analysera argument *för* att domen innebär ett krav på riktad lagring och inte fokuserat på argument *mot*.

För det andra anser utredningen att en riktad lagring inte möter behovet från de brottsbekämpande myndigheterna. Experterna från de brottsbekämpande myndigheterna har i utredningen med stor tyngd visat på ett starkt behov av att uppgifter lagras i minst samma omfattning som före EU-domstolens dom. En riktad lagring kräver ett aktivt beslut att ”slå på” lagringen och det framhålls, utifrån ett verksamhetsperspektiv, som ett stort problem. Skälet är att det är svårt att i förväg veta hur man ska rikta lagringen. Jag delar utredningens bedömning att ett verksamhetsperspektiv starkt talar mot en riktad lagring men konstaterar samtidigt att lagringen måste rymmas inom de juridiska ramar som EU-domstolen och lagstiftningen satt upp.

Vad talar då för att EU-domstolen förespråkar en riktad lagring?

För det första bygger hela domstolens resonemang på att det måste finnas en begränsning i lagringsskyldigheten och att begränsningen måste vara så pass omfattande att huvudregeln inte kan anses vara att uppgifter ska lagras. En riktad lagring har alla förutsättningar att uppfylla detta.

För det andra framför EU-domstolen i skäl 108 att en nationell lagstiftning inte hindrar en riktad lagring, som differentieras utifrån personkrets, tidsperiod och situation. Även i skäl 105-106 och i skäl 108-111 argumenterar EU-domstolen kring en riktad lagring.

För det tredje måste det finnas en koppling, om än indirekt, mellan lagringskyldigheten och grov brottslighet. Här konstaterar EU-domstolen i skäl 105 och 111 bl.a. att den nationella lagstiftningen i målet är tillämplig på personer beträffande vilka de inte föreligger något indicium som ger anledning att tro att deras beteende ens kan ha ett indirekt eller avlägset samband med grov brottslighet. Det ligger i sakens natur att en generell lagring aldrig kan uppfylla detta kriterium medan en riktad lagring kan göra det.

Jämfört med de argument som utredningen presenterar och de faktorer som enligt min uppfattning talar för en riktad lagring, väger

de förstnämnda lätt. Min tolkning av EU-domstolens dom är således att det utrymme som finns för nationell lagstiftning är begränsat till en riktad lagring.

Särskilt om abonnemangsuppgifter och räckvidden av EU-domstolens dom

EU-domstolen konstaterar i domen att de uppgifter som leverantörer av elektroniska kommunikationstjänster är skyldiga att lagra gör det möjligt att få kännedom om med vilken person en abonnent eller registrerad användare har kommunicerat med och på vilket sätt, hur länge kommunikationen varat och från vilken plats kommunikationen skett[7]. Enligt EU-domstolen gör uppgifterna det möjligt att kartlägga de berörda personerna på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationen[8]. Det är noterbart att bland uppgifterna som räknas upp av domstolen så finns ip-adresser med[9].

Det sagda väcker frågan i vilken omfattning som utredningens slutsats att abonnemangsuppgifter inte omfattas av EU-domstolens dom är korrekt. Det är också den slutsatsen som ligger till grund för att utredningen inte föreslår några förändringar i den svenska hanteringen av abonnemangsuppgifter. Enligt utredningen omfattas endast trafikuppgifter och lokaliseringsuppgifter av domen.

Jag anser att utredningen inte problematiserar tillräckligt kring förhållandet hur framförallt ip-adresser och andra abonnemangsuppgifter ska betraktas enligt EU-rätten och inte heller analyserar detta tillräckligt. För att analysen ska bli fullständig krävs t.ex. att den behandlar de argument som talar för att ip-adresser omfattas av domen. Det finns enligt min bedömning skäl som talar för att ip-adresser, som lagras i trafikloggar, är trafikuppgifter och att lagringen därför omfattas av domen.

Det som idag omfattas av det svenska begreppet abonnemangsuppgift, där ip-adresser med tiden kommit att ingå, är en rest från telelagen. Som utredningen konstaterar har abonnemangsuppgifter ibland kallats för kataloguppgifter eftersom informationen som kan

[7] Se skäl 98.
[8] Se skäl 99.
[9] Se skäl 98.

erhållas närmast motsvarar vad som finns i telefonkataloger[10]. Begreppet kataloguppgifter är, såsom utredningen konstaterat, missvisande eftersom det även omfattar andra uppgifter än traditionella kataloguppgifter.

I sammanhanget ska också påpekas att de brottsbekämpande myndigheterna har rätt att få tillgång till abonnemangsuppgifter utan domstolsprövning. Ett tungt skäl som framförts är att uppgifter om abonnemang historiskt inte har ansetts lika integritetskänsliga. Mot bakgrund av EU-domstolens dom kan denna bedömning ifrågasättas.

[10] Se avsnitt 4.3 i betänkandet.

Särskilt yttrande av Anders Ahlqvist, Anna Olander Selldén, Katarina Bigovic Apitzsch, Carin Ewald Möller och Hans Harding

Inledning

Grova brott orsakar stora skador för enskilda och samhället. Samhället ansvarar för medborgarnas trygghet och rättssäkerhet. Både för medborgarna i allmänhet och för brottsoffren är det angeläget att förutsättningarna för att klara upp grova brott och för att kunna förhindra brott redan på planeringsstadiet är så goda som möjligt.

Att de brottsbekämpande myndigheterna har tillgång till trafik- och lokaliseringsuppgifter är avgörande för en effektiv bekämpning av grov brottslighet, inklusive sådan som är kopplad till nationell säkerhet. Utredaren anger att om de brottsbekämpande myndigheterna inte skulle ha tillgång till adekvata utredningsverktyg i den elektroniska miljön så skulle grova brott i vissa fall vara omöjliga att klara upp och brottsoffer i motsvarande omfattning vara skyddslösa (avsnitt 12.3). Vissa brott skulle i praktiken bli straffria och många målsägande skulle aldrig kunna få upprättelse. Utredaren konstaterar också att staten har en skyldighet att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda och, om intrång görs, se till att brotten utreds. Enligt utredaren skulle det inte vara förenligt med Sveriges internationella åtaganden att inte ge de brottsbekämpande myndigheterna möjlighet att effektivt utreda brott i den elektroniska miljön. Dessa utgångspunkter bör vara fundamentala för lagstiftarens syn på frågan om datalagring.

Lagringsskyldigheten infördes för att säkerställa att uppgifterna kommer brottsbekämpningen till del genom de aktuella tvångsmedlen. I de delar lagringsskyldigheten begränsas kommer den garantin inte att finnas kvar. Resultatet blir att myndigheterna vid bekämpning av den grova brottsligheten får hoppas på turen att operatörerna ändå har sparat uppgifterna, t.ex. för fakturering. Detta kommer i många fall att få allvarliga följder, inte minst eftersom lagringsskyldigheten redan idag innebär att enbart ett minimum av strängt nödvändiga uppgifter ska lagras.

Trafik- och lokaliseringsuppgifter har med tiden blivit ett allt viktigare verktyg i brottsbekämpningen. I nuläget, där en stor del av brottsligheten lämnar digitala spår i någon form, är uppgifterna

oumbärliga. Det gäller i såväl underrättelse- som förundersökningsverksamhet. Uppgifterna används i stort sett i varje utredning av grov brottslighet. Ofta är uppgifterna dessutom den första och enda ingången i utredningarna och ger nyckeln till det vidare arbetet. Utan denna nyckel kommer dörren till framgång många gånger att förbli stängd.

Lagringsskyldigheten i Sverige är redan begränsad

Utredarens uppdrag har varit att anpassa det svenska regelverket till EU-rätten såsom den uttolkas i EU-domstolens förhandsavgörande den 21 december 2016 i de förenade målen C-203/15 och C-698/15. EU-domstolen har i sin tur tolkat EU-rätten i skenet av den beskrivning av den svenska lagstiftningen som Kammarrätten i Stockholm har presenterat i sin begäran om förhandsavgörande.

Kammarrätten har i sin beskrivning av de svenska bestämmelserna om lagring av uppgifter om elektroniska kommunikation olyckligtvis gett EU-domstolen intrycket att den svenska lagringsskyldigheten omfattar ”samtliga personer, samtliga kommunikationsmedel och samtliga trafikuppgifter”. EU-domstolen konstaterar utifrån detta att den svenska lagstiftningen avser samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter. Den slutsatsen kan dock ifrågasättas. Sanningen är att lagringsskyldigheten omfattar endast en del därav. Det kan inte uteslutas att kammarrättens beskrivning har lett EU-domstolen fel, då domstolen i sina domskäl kommer fram till att den svenska lagstiftningen har gjort undantaget (från principen att säkerställa konfidentialiteten för kommunikation) till huvudregel (se domskäl 89 och 97–104).

Man måste därför, som utredaren anger (avsnitt 12.4.2), tolka EU-domstolens slutsatser i ljuset av hur kammarrätten ställde sina frågor.

Många av de kommunikationsmedel som den moderna människan idag använder och många av de trafik- och lokaliseringsuppgifter som operatörerna behandlar omfattas inte av den svenska lagringsskyldigheten.

Exempelvis omfattas inte följande uppgifter av lagringsskyldigheten (se avsnitt 12.4.2):

- position när ett meddelande skickades och när det mottogs,
- position under ett mobilsamtal,
- position vid fast telefoni,
- utrustningsidentitet vid skickade och mottagna meddelanden,
- utrustningsidentitet vid fast telefoni,
- abonnemangsidentitet vid skickade och mottagna meddelanden,
- abonnemangsidentitet vid internetåtkomst,
- uppgifter om samtal med annat än vanligt telefonnummer (däribland uppringande och uppringt nummer, tid och position),
- uppgift om port och lokal ip-adress (dvs. den som används mellan abonnent och internetleverantör) vid internetåtkomst,
- meddelandehantering och ip-telefoni,
- uppgifter om samtal som inte kopplas fram på grund av tekniskt fel eller dylikt (däribland uppringande och uppringt nummer, tid, utrustning och position) och
- rena lokaliseringsuppgifter (positioner som inte är kopplade till kommunikation eller internetåtkomst).

Lagringsskyldigheten omfattar inte heller

- web-surf (besök på hemsida),
- kommunikation mellan två ip-adresser som inte är telefoni (t.ex. Skype- och Vibersamtal),
- internetbaserad e-post såsom hotmail och g-mail,
- VPN-tjänst,
- FTP (filöverföring),
- chat (meddelandetjänst),
- sociala medietjänster (såsom Facebook, Twitter, Viber, Whatsapp m.fl.) och
- informationssamhällestjänster (såsom Blocket, E-bay m.fl.).

Som utredaren konstaterar (avsnitt 12.4.2) är det alltså långt ifrån samtliga trafik- och lokaliseringsuppgifter som omfattas av lagringsskyldigheten. Den är redan idag klart begränsad.

Lagringsskyldigheten innefattar i stället enbart en minimilista, som, redan när den kom till, uppfyllde bara de absolut mest grundläggande behoven vid utredning av grov brottslighet. Teknikutvecklingen för dessutom med sig att minimilistan relativt sett blir mindre och mindre i förhållande till samtliga de trafik- och lokaliseringsuppgifter som operatörerna behandlar och som brottsbekämpande myndigheter skulle kunna ha nytta av i sitt arbete. Sett ur denna synvinkel kan man därför ifrågasätta riktigheten av EU-domstolens beskrivning av den svenska lagstiftningen som att lagringen har gjorts till huvudregel i stället för att vara ett undantag (jfr domskäl 104). Enligt vår uppfattning är lagring redan idag ett undantag och inte en huvudregel.

EU-domstolens bedömning av vad som är en acceptabel omfattning av lagringsskyldigheten hade rimligen kunnat få ett annat utfall, om domstolen hade utgått från det riktiga förhållandet, att den svenska lagringsskyldigheten inte på långa vägar omfattar ”samtliga kommunikationsmedel och samtliga trafikuppgifter”.

Det som nu sagts innebär bl.a. att bedömningsutrymmet är stort i fråga om vad som är en acceptabel omfattning av lagringsskyldigheten. I avvägningen mellan samhällsnyttan och graden av intrång i enskildas skyddade rättigheter är vår uppfattning att det finns större utrymme för en lagringsskyldighet än vad utredarens förslag ger uttryck för.

EU-domstolen kräver en ändring av svensk rätt

Likväl går det nu inte att tolka EU-domstolens dom på ett annat vis än att den fordrar att den svenska lagstiftningen på datalagringsområdet reformeras och lagringen relativt sett begränsas. Utredarens uppdrag har således varit att utifrån tolkning av EU-domstolens dom finna en ny balans mellan tillvaratagandet av den personliga integriteten och en effektiv brottsbekämpning. Även om det förväntade resultatet av utredningen från vårt perspektiv var en försämring av datalagringen, vill vi likväl uttrycka vår uppskattning för utredarens arbete och hans ambition att bevara någon form av datalagring för

brottsbekämpningsändamål värd namnet. Utredningen vittnar om ett gediget arbete utfört inom en snävt begränsad tidsram.

Synpunkter på förslagen i utredningen

Vi kommer i det följande att lämna några synpunkter på förslagen i utredningen. Vi vill med detta särskilt belysa att varje form av nedskärning av datalagring för brottsbekämpningsändamål kommer att få allvarliga återverkningar på vår förmåga att förebygga, förhindra och utreda brott.

Minskad effektivitet i brottsbekämpningen

För brottsbekämpningen i Sverige är konsekvensen av EU-domstolens tolkning av EU-rätten att effektiviteten i arbetet minskar. Detta märktes redan kort tid efter EU-domstolens dom, då flera operatörer, som en följd av domen, slutade lagra trafik- och lokaliseringsuppgifter för brottsbekämpande ändamål. Detta har för brottsbekämpningen under innevarande år redan inneburit tillkommande svårigheter att utreda grova brott såsom mord, människorov och grov narkotikasmuggling, för att nämna några konkreta exempel.

Någon enstaka operatör har tolkat EU-domstolens dom som gällande även abonnemangsuppgifter och ip-adresser och har därför slutat att lagra även dessa uppgifter. Detta har fått till följd att vissa brottstyper blivit praktiskt taget omöjliga att utreda. Det har bl.a. lämnat dörren öppen för pedofiler att straffritt ladda ner och sprida övergreppsmaterial, med andra ord att begå grovt barnpornografibrott.

En forskningsstudie som tagits fram av barnrättsorganisationen ECPAT Sverige visar att det finns ett starkt samband mellan barnpornografibrott och sexuella övergrepp på barn. Forskningen omfattade en granskning av drygt 100 avgöranden från tingsrätt och hovrätt, mellan åren 2014 och 2016. Av dessa visade det sig att de personer som dömdes för barnpornografibrott i omkring hälften av fallen (48 %) även dömdes för sexualbrott mot barn. Detta gör det än mer angeläget att säkerställa möjligheter att bekämpa denna brottstyp.

Frågan om vad som ska omfattas av begreppet abonnemangsuppgifter, och särskilt om ip-adresser omfattas av detta, har redan tidigare varit föremål för delade meningar, eftersom lagstiftningen har varit otydlig på den punkten.

Viktigt om abonnemangsuppgifter

Vi instämmer i utredarens bedömning att EU-domstolens avgörande inte rör abonnemangsuppgifter utan enbart trafik- och lokaliseringsuppgifter, och vi delar till fullo hans bedömning av vilka uppgifter som ska anses omfattas av begreppet abonnemangsuppgifter, däribland återfinns IMSI-nummer och ip-adresser. Vi välkomnar särskilt att utredaren på ett tydligt sätt slår fast att ip-adresser är abonnemangsuppgifter. Det är välgörande att utredaren tar tydlig ställning i frågan och inte lämnar fältet öppet för operatörer att tolka sin lagringsskyldighet på ett sätt som underlättar för deras kunder att ostraffat begå brott på internet. Det är ur principiell synvinkel viktigt att möjligheten för kunderna att komma undan straffansvar inte får bli en konkurrensfördel bland operatörerna.

I detta sammanhang vill vi framhålla utredarens förslag att möjliggöra identifiering av slutanvändare vid internetåtkomst genom s.k. NAT-teknik, dvs. en teknik som låter flera användare dela på en och samma publika ip-adress. Utredaren har här identifierat en betydande inkonsekvens i nuvarande lagstiftning som är en följd av senare teknikutveckling. Enbart en skyldighet för operatörerna att lagra uppgifter för att kunna identifiera användaren av en viss ip-adress är alltså inte tillräcklig vid användning av denna teknik. NAT-tekniken innebär i nuläget att alla slutanvändare (kunder) förblir omöjliga för brottsbekämpande myndigheter att identifiera. Denna inkonsekvens har påtalats i tidigare betänkanden utan att leda fram till lagändring. För att främja teknikneutraliteten beträffande identifiering av slutanvändare vid internetåtkomst har utredaren därför föreslagit att det ska lagras uppgifter för att kunna identifiera en slutanvändare även då operatören använder NAT-teknik (se avsnitt 12.6.4). Vi är eniga med utredaren i denna del. Det är helt nödvändigt att motverka den anonymisering som användandet av NAT-tekniken innebär för slutanvändarna. Operatörens val av teknik bör rimligen inte möjlig-

göra för dess kunder att i skydd av anonymitet begå brott på internet.

En begränsad lagringsskyldighet är lösningen – alternativ saknas

Vi står bakom utredarens bedömning att det är möjligt att lösa uppdraget genom att föreslå en begränsad lagringsskyldighet i förhållande till idag. Vi har inte funnit något alternativ till sådan lagring som ger möjligheter att förutsättningslöst utreda brott som redan inträffat eller skaffa sig underrättelser om brottslighet som kan vara å färde. Därför har vi avfärdat möjligheten att införa någon form av sådan riktad lagring, som EU-domstolen i ett *obiter dictum* framställt som ett tänkbart alternativ till generell lagring (domskäl 108 och 111 tredje meningen). Anledningen är, som också framgår av utredningen, att en riktad lagring kräver att man redan på förhand vet var eller av vem som brott ska begås, vilket mycket sällan är fallet.

Att, som EU-domstolen föreslår (jfr domskäl 111), på förhand peka ut brottsbenägna personer eller brottsbelastade områden för en riktad lagring skulle enligt vår mening vara förenat med praktiska svårigheter och bl.a. innebära en dubbel diskriminering, där alla personer i vissa områden (dit lagringen riktas) pekas ut som mer brottsbenägna än andra (där lagring inte förekommer) samtidigt som alla personer i områden där lagring inte förekommer skulle nedprioriteras från ett brottsbekämpningsperspektiv (där skulle grova brott inte kunna utredas lika effektivt).

Enligt vår kännedom tillämpar inte något annat land inom EU riktad lagring i likhet med EU-domstolens förslag. En plausibel anledning till detta är att en sådan form av riktad lagring helt enkelt inte anses utgöra ett effektivt brottsbekämpningsverktyg.

Det av utredaren framförda förslaget innebär, vilket han själv påpekar, att lagringsskyldigheten minskar tämligen kraftigt (avsnitt 13.1.2). Det för med sig att möjligheterna att förebygga, förhindra och utreda brott försämras. Begränsningen kommer enligt vår bedömning att få klart negativa effekter på det brottsbekämpande arbetet i Sverige. I många fall kan konsekvenserna beskrivas som mycket allvarliga.

En av orsakerna till att trafik- och lokaliseringsuppgifter har så stor betydelse vid utredningar av grov brottslighet är att den infor-

mation som uppgifterna ger är unik, dvs. den kan i praktiken sällan inhämtas genom andra metoder. De brottsbekämpande myndigheterna har ingen möjlighet att t.ex. börja arbeta på annat sätt för att kompensera för ett bortfall.

Visst kan fysisk spaning vid något tillfälle användas i stället för att lokaliseringsuppgifter inhämtas i realtid från operatörer, men det är inget alternativ till inhämtning av uppgifter från förfluten tid. Den fysiska spaningen är en mycket begränsad och även resurskrävande metod som knappast kan kallas ett alternativ till information från operatörerna. Snarare är spaningen ibland ett komplement. Utredaren anger också i avsnitt 7.2 att det i princip inte går att ersätta inhämtning av trafik- och lokaliseringsuppgifter med fysisk spaning.

Det sägs ibland att kriminaltekniska undersökningar av telefoner och datorer skulle vara ett alternativt sätt för de brottsbekämpande myndigheterna att få information. Det är en sanning med modifikation. För det första kräver en sådan undersökning att telefonen eller datorn finns tillgänglig för undersökning – att den är i beslag. Beslag är dock ett tvångsmedel som enbart får användas under förundersökning, alltså inte i underrättelseverksamhet. För det andra är det inte alls säkert att de telefoner eller datorer som kan kopplas till brottsligheten påträffas och kan tas i beslag. För det tredje är beslag inte hemligt för den som innehar föremålet. För det fjärde är trafik- och lokaliseringsuppgifter ofta en förutsättning för att över huvud taget rättsligt och praktiskt kunna genomföra husrannsakan, ta föremål såsom telefoner och datorer i beslag och andra åtgärder med lyckat resultat. För det femte kan det inträffa att informationen i telefonen eller datorn inte är helt identisk med den som ges från operatörerna och således inte är tillförlitlig utan kanske rent missvisande. För det sjätte kan en telefon eller dator vara krypterad så att det inte går att komma åt informationen.

Risker med att bryta kommunikationskedjan

Tillhandahållandet av elektroniska kommunikationstjänster sker idag på annat sätt än när telefonitjänst tillhandahölls av Televerket som enda operatör på marknaden. Idag kan många operatörer vara involverade i en och samma kommunikation. Till exempel kan en person ha abonnemang på fiberanslutning från en operatör, internet-

åtkomsten kan komma från annan och ip-telefonin från en tredje. Alla operatörerna behandlar enbart uppgifter om sin egen del i kommunikationskedjan. För att de brottsbekämpande myndigheterna ska kunna kartlägga kommunikationen krävs att de får uppgifter från respektive operatör som gör det möjligt att gå vidare till nästa operatör i kedjan. Uppgifterna fungerar således som länkar som myndigheterna behöver i arbetet. Om lagringsskyldighet för en typ av uppgift tas bort kan den brygga mellan operatörerna som gör det möjligt att nå framgång försvinna. Detta påtalades också av företrädare för operatörerna i Trafikuppgiftsutredningen som en förutsättning för att kunna spåra deltagare i en kommunikation (SOU 2007:76). Den nuvarande minimilistan bygger också på den förutsättningen att kommunikationskedjan ska kunna följas.

Som exempel innebär utredarens förslag att ip-adresser ska lagras vid internetåtkomst men inte vid telefonitjänst och meddelandehantering. Om myndigheterna t.ex. har tillgång till en ip-adress som används av en viss person för internetåtkomst blir det i stort sett omöjligt att sedan knyta den adressen till telefoni- eller meddelandetjänster hos en annan operatör. Det innebär att vem personen kommunicerat med samt när, var och hur kommunikationen skedde inte kan klarläggas. Nackdelarna för brottsbekämpningen kan alltså bli mer omfattande än man vid en första anblick kan tro när lagringsskyldigheten försvinner för vissa typer av uppgifter. Det är nödvändigt att beakta sådana negativa effekter.

Utredaren föreslår att uppgifter om vem som kommunicerade med vem inte längre ska lagras när det gäller fast telefoni (inklusive fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator).

Uppgifter om vem som har haft kontakt med vem är fundamentala i de brottsbekämpande myndigheternas arbete med kartläggning av brottslighet, oavsett om det är fråga om förundersökning eller underrättelseverksamhet och oavsett kommunikationsmedel. Saknas de uppgifterna finns en stor risk att bevisning missas eller att den vidare analysen och bedömningen får stora svagheter. Många gånger kommer det inte ens att finns skäl att begära trafik- och lokaliseringsuppgifter från operatörerna, eftersom det vidare arbetet med uppgifterna bedöms som meningslöst.

Fast ip-telefoni kommer, till skillnad mot den ”vanliga” fasta telefonin, inte att försvinna inom några år. Vi vill understryka att fast ip-

telefoni är en modern tjänst som till stor del kan jämföras med mobil telefoni. Utvecklingen går mot att all telefoni blir ip-baserad och därmed mobil i olika avseenden. Ett och samma ip-telefoniabonnemang kan utnyttjas såväl från en fast telefon som från en mobil.

Sannolikt kommer också gränsen mellan fast och mobil nätanslutningspunkt att suddas ut eller bli diffus och medföra tolkningssvårigheter. Med en utökad anslutning av optofiber till både hem och företag med möjlighet att använda samma ip-telefonitjänst både hemma och på jobbet kan det redan idag konstateras att exempelvis telefonitjänster blir mer frikopplade från både geografisk plats och fysisk utrustning. Det skulle innebära allvarliga förluster av information för brottsbekämpningen om inte lagringsskyldigheten skulle omfatta den mest moderna typen av telefoni.

Det är bl.a. på grund av det sagda förenat med en stor risk för brottsbekämpningen att göra en differentiering mellan fast och mobil telefoni, eller fast och mobil nätanslutningspunkt. Det blir svårt att överblicka följderna framöver av en sådan gränsdragning, i synnerhet på ett område som elektronisk kommunikation där den tekniska utvecklingen går mycket fort.

I detta sammanhang vill vi framhålla att det är positivt att utredaren föreslår att utrustningsidentitet, som är en abonnemangsuppgift, ska lagras även i fortsättningen vid mobil telefoni. IMEI-nummer och MAC-adress är mycket viktiga för att identifiera hårdvaran som används vid en kommunikation. De uppgifterna ger, på samma sätt som uppringande eller uppringt nummer, information om vem som kommunicerat med vem.

Utredaren föreslår att uppgifter om när kommunikation skett inte längre ska lagras när det gäller fast telefoni (inklusive fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator).

Att få uppgift om vem som kommunicerat med vem är, som nyss framgick, fundamentalt i brottsbekämpningen. Den kunskapen riskerar att få liten betydelse om inte kontakten kan knytas till en viss tidpunkt genom datum och spårbar tid då kommunikationen påbörjades och avslutades eller ett meddelande skickades och mottogs.

Det är alltså många gånger avgörande att veta tidpunkterna för en kommunikation. Uppgifterna är viktiga pusselbitar i arbetet med att klarlägga personers kontakter, relationer och beteenden, och kan visa ”närheten” mellan personer och deras ageranden vid olika händelser.

Utredaren föreslår att uppgifter om var kommunikation skedde, dvs. lokaliseringsuppgifter, inte längre ska lagras när det gäller fast telefoni (inklusive fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator). Även uppgifter om var en viss utrustning befann sig när kommunikation skedde är fundamentala uppgifter i brottsbekämpningen. De är ofta avgörande i både förundersökning och underrättelseverksamhet och kan i vissa fall vara av större värde än uppgifter om vilka som har kommunicerat med varandra. Utan dessa uppgifter blir det mycket svårare att lokalisera brottsplatser, mötesplatser, gärningsmän, vapen- och narkotikagömmor.

Lokaliseringsuppgifter är alltså strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet.

Som utredaren påpekar omfattar lagringsskyldigheten enligt nuvarande lagstiftning (förordningen om elektronisk kommunikation) inte lokaliseringsuppgifter vid meddelandehantering såsom sms (avsnitt 12.6.3). Detta måste bero på ett förbiseende hos lagstiftaren. Hittills har operatörerna lagrat och lämnat ut dessa uppgifter till brottsbekämpande myndigheter. Dessa uppgifter är lika viktiga som motsvarande uppgifter vid telefonitjänster (telefonsamtal). I många brottsutredningar har det visat sig att kommunikationen mellan gärningsmännen skett nästan uteslutande via sms, och utan tillgång till lokaliseringsuppgifter vid sms-kontakter hade utredningarna inte nått framgång. Vi har förståelse för att utredaren i sitt uppdrag ansett sig förhindrad att föreslå en utökning av lagringsskyldigheten i denna del, även om han anser att denna uppgift är strängt nödvändig. Om operatörerna i framtiden inte lämnar ut denna uppgift kommer dock behovet av en lagringsskyldighet för den att bli akut.

Differentierad lagringstid

Utredarens förslag innebär att lagringstiderna differentieras utifrån hur gamla uppgifter det finns ett påtagligt behov av. Han föreslår att lokaliseringsuppgifter vid samtal ska lagras i två månader. Uppgifter om internetåtkomst, förutom uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs, ska lagras i tio månader och övriga uppgifter i sex månader.

Vi har ingen invändning i sig mot principen att lagringstiderna differentieras men kan konstatera att kortare lagringstider får negativa konsekvenser för tidskrävande utredningar av svårutredda brott.

Vi ser positivt på att utredaren föreslår att lagringstiden för vissa uppgifter ska förlängas från sex till tio månader. Detta kommer att innebära att fler ärenden kommer att kunna knytas till en misstänkt person, inte minst i barnpornografiärenden.

Ny beslutsordning i IHL-ärenden

Vi accepterar utredarens förslag till ny beslutsordning i IHL-ärenden, där åklagare ges behörighet att fatta beslut på ansökan av de brottsbekämpande myndigheterna. Vi är dock, liksom utredaren, bekymrade över att detta bryter mot principen att åklagare endast ska bedriva förundersökning och efterföljande lagföring och inte ska blanda sig i underrättelseverksamheten. Vi vill därför gärna se den föreslagna lösningen som provisorisk.

Övrigt

Vi ser det som mycket positivt att de brottsbekämpande myndigheternas tillgång till lagrade uppgifter även fortsättningsvis ska avse uppgifter som operatörerna sparar för egna ändamål och att lagringen inte får ske utanför Sverige.

Särskilt yttrande av Staffan Lindmark

Inledning

Inledningsvis vill jag framhålla att utredningen är väl genomförd, särskilt med hänsyn till den snäva tidsramen för denna del av uppdraget. Jag delar flertalet av utredningens slutsatser men har i några frågor en avvikande uppfattning.

Utredningens förslag innebär att lagring av uppgifter förblir huvudregel

Utredningen har föreslagit en modell för lagring av uppgifter om elektronisk kommunikation som enligt utredningen innebär en kraftig reformering av de hittillsvarande lagringskraven och som medför att lagringsskyldigheten inte längre blir generell utan anpassad till vad som är strängt nödvändigt utifrån nytta, behov och proportionalitet. Jag ställer mig dock tveksam till att de förändringar av lagringsskyldigheten som utredningen föreslår är tillräckligt långtgående för att leva upp till de EU-rättsliga krav som EU-domstolen gett uttryck för i sin dom av den 21 december 2016 i de förenade målen C-203/15 och C-698/15. Även om förslaget innebär att vissa uppgiftstyper och vissa kommunikationsslag inte längre ska omfattas av kravet på lagring, så måste ändå den föreslagna lagringen anses vara generell, i det att den gäller samtliga användare av de berörda kommunikationstjänsterna utan avgränsning till vissa tidpunkter, platser eller andra faktorer som kan relateras till risken för grov brottslig verksamhet. Liksom enligt hittillsvarande reglering kommer lagring av uppgifter enligt utredningens förslag att vara huvudregel, snarare än undantag.

Jag ifrågasätter inte att en mer generell lagring ger betydligt större nytta för de brottsbekämpande myndigheterna än en mer avgränsad och riktad lagring. Det är trots detta en brist att utredningen inte närmare har analyserat och lagt fram förslag till hur en riktad lagring skulle kunna utformas. EU-domstolen har slagit fast att EU-rätten tillåter just en riktad lagring i syfte att bekämpa grov brottslighet, under förutsättning att lagringen också begränsas till vad som är strängt nödvändigt. I domen utvecklas vidare vilka krav som måste

vara uppfyllda för att en sådan riktad lagring ska anses förenlig med EU-rätten.[11]

Utredningen har avfärdat EU-domstolens resonemang om riktad lagring som uttalanden *obiter dicta*. Jag menar dock att ett förhandsavgörande till sin natur utgör ett abstrakt besked om rättsläget utan stark koppling till sakomständigheterna i de enskilda nationella målen. Det gäller särskilt när domen, som i förevarande fall, har meddelats i stor avdelning. Samtidigt har EU-domstolen relativt specifikt och detaljerat angett vilka brister den nuvarande svenska regleringen lider av samt hur regleringen istället bör utformas, vilket ytterligare talar för att domstolens uttalanden bör anses vara bindande.[12]

Reglerna om lagring och inhämtning av uppgifter om IP-adresser behöver utredas ytterligare

EU-domstolen har i sin dom slagit fast ett antal kriterier som måste vara uppfyllda för att regler om lagring respektive inhämtning av uppgifter om elektronisk kommunikation ska kunna anses leva upp till EU-rättens krav på respekt för grundläggande rättigheter. Utredningen har dock kommit till slutsatsen att domen inte ens indirekt påverkar den svenska regleringen om lagring respektive tillgång till s.k. uppgifter om abonnemang. Jag delar inte den uppfattningen. Utredningens slutsats förefaller vila på det felaktiga antagandet att uppgifter om abonnemang utgör en kategori uppgifter som ur ett EU-rättsligt perspektiv kan skiljas från kategorierna trafik- och lokaliseringsuppgifter.

I själva verket har begreppet uppgift om abonnemang – som idag återfinns i bestämmelsen om tystnadsplikt i 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation (LEK) – sitt ursprung i sekretessregler som gällde för den verksamhet som bedrevs av det dåvarande statliga Telegrafverket, sedermera Televerket. Regleringen av brottsbekämpande myndigheters möjlighet att inhämta uppgifter om abonnemang från operatörerna har på motsvarande sätt sin grund i regler om undantag från sekretess. Dessa undantag vilade på

[11] Se skäl 108-111 i EU-domstolens dom av den 21 december 2016.
[12] Se Hettne, J. och Otken Eriksson, I., *EU-rättslig metod – Teori och genomslag i svensk rättstillämpning* (2011), 2 uppl., s. 53 samt även Munck, J. *Rättskällor förr och nu, Juridisk Publikation jubileumsnummer 2014* (2014), s 206f, Dickson, J. och Eleftheriadis, P., *Philosophical Foundations of European Union Law* (2012), s. 314 f.

en avvägning mellan intresset av brottsbekämpning och intresset av sekretess för de uppgifter som vid denna tid ansågs utgöra uppgifter om abonnemang.[13] Enligt förarbetena till den dåvarande regleringen skulle begreppet omfatta vissa uppgifter rörande enskilda abonnenters affärsangelägenheter och personliga angelägenheter, i fråga om telefoni främst uppgift om namn, titel, adress och telefonnummer. Från dessa uppgifter skulle skiljas innehållet i meddelanden samt andra uppgifter som angick särskilda meddelanden.[14]

Begreppet uppgifter om abonnemang härrör således från en tid långt före utvecklingen av de elektroniska kommunikationstjänster – såsom mobiltelefoni och internetåtkomst – som idag dominerar marknaden. När det s.k. e-dataskyddsdirektivet (2002/58/EG) införlivades i svensk rätt tillfördes den svenska regleringen nya begrepp för att beskriva de olika uppgifter som förekommer i samband med tillhandahållande av elektroniska kommunikationstjänster. Samtidigt bibehölls de äldre reglerna och de äldre begrepp som där används. I förarbetena uttalade regeringen att det nytillkomna begreppet ”trafikuppgift” i princip torde avse samma slag av uppgifter som i den befintliga nationella regleringen kallades för ”uppgifter som angår särskilda meddelanden”. Detta uttalande implicerar att trafikuppgifter skulle utgöra en kategori uppgifter som är distinkt skild från kategorin uppgift om abonnemang.[15]

I takt med den tekniska utvecklingen och tillkomsten av nya elektroniska kommunikationstjänster har emellertid allt fler uppgifter kommit att hänföras till kategorin uppgift om abonnemang. T.ex. kan nämnas s.k. IMSI-nummer för mobiltelefoni och IP-adresser för internetåtkomst. I praxis har bestämmelsen i 6 kap. 22 § första stycket 2 om inhämtning av uppgifter om abonnemang ansetts omfatta sådana uppgifter som kan leda till att en abonnent kan identifieras eller kontaktas. Denna utveckling har medfört att bedömningen av vilka uppgifter som anses utgöra uppgifter om abonnemang har kommit att utgå från syftet med inhämtningen och värdet för brottsbekämpningen av uppgifterna snarare än uppgifternas karaktär. Många av de uppgifter som idag anses höra till kategorin

[13] Se prop. 1983/84:142 s. 29.
[14] Se prop. 1979/80:2 del A s. 272 och prop. 1992/93:200 s. 310.
[15] Se prop. 2002/03:100 s. 389 f.

uppgift om abonnemang är av en helt annan natur än de som ursprungligen avsågs med begreppet.[16]

Någon motsvarighet till begreppet uppgift om abonnemang återfinns inte i e-dataskyddsdirektivet och den utveckling av begreppets omfattning som skett i Sverige under senare år kan inte heller hänföras till någon motsvarande förändring inom EU-rätten. Det rör sig alltså om två parallella begreppsfloror och det går inte att med säkerhet säga vilka av de uppgifter som i Sverige anses utgöra uppgifter om abonnemang som omfattas av de EU-rättsliga reglerna i bl.a. e dataskyddsdirektivet.

Enligt min mening är frågan om lagring och inhämtning av uppgifter om internetåtkomst, såsom IP-adresser och andra uppgifter som kan vara nödvändiga för att möjliggöra spårning av källan till internetbaserad kommunikation, särskilt problematisk. Det finns numera sällan en beständig koppling mellan en viss IP-adress och en viss abonnent. Ett stort antal abonnenter kan samtidigt nyttja samma IP-adress och kopplingen mellan en viss abonnent och en viss IP-adress kan i vissa fall förändras på sekundbasis. För att kunna spåra källan till en viss kommunikation över internet så krävs ofta att uppgifter om flera olika IP-adresser och andra tekniska data kombineras, och relationen mellan abonnent och IP-adress är i dessa fall mycket flyktig. Samtidigt kan de uppgifter som således måste behandlas sammantaget lämna mycket exakt information om abonnenternas internetkommunikation.

I EU-domstolens dom anges uttryckligen att IP-adressen för internettjänster är en av de uppgifter som kan bidra till att dra mycket precisa slutsatser om privatlivet för berörda personer och att regler om lagring av dessa uppgifter utgör ett långtgående ingrepp i grundläggande rättigheter.[17] Att EU-domstolen senare i domen använder begreppen trafik- och lokaliseringsuppgifter för att beskriva de uppgifter, vars lagring och inhämtning måste leva upp till de krav som följer av EU-stadgan och e-dataskyddsdirektivet, kan inte tolkas som att t.ex. IP-adresser inte skulle omfattas. Denna uppfattning stärks av att kammarrätten i sin dom i mål nr 7380-14 har dragit slutsatsen att de svenska reglerna om lagring av uppgifter för brottsbekäm-

[16] Se bl.a. uttalanden i SOU 2005:38 s. 131, Kammarrättens i Stockholm dom i mål 3138-09 och prop. 2011/12:55 s. 101 ff.
[17] Se skäl 98-100 i EU-domstolens dom den 21 december 2016 i de förenade målen C-203/15 och C-698/15.

pande ändamål, dvs. även de regler som avser lagring av uppgifter om abonnemang, står i strid med unionsrätten och därför inte får tillämpas. Att nuvarande reglering avseende IP-adresser inte är helt oproblematisk stärks även av att förvaltningsrätten den 5 maj 2017 i mål nr 6895-16, med hänvisning till EU-domstolens dom, har beslutat att inhibera Post- och telestyrelsens föreläggande om skyldighet att lämna ut uppgifter om IP-adresser till brottsbekämpande myndighet.[18]

Mot denna bakgrund kan jag inte ställa mig bakom utredningens slutsats att de svenska reglerna om lagring respektive inhämtning av lagrade uppgifter om abonnemang, i synnerhet IP-adresser och relaterade uppgifter avseende internetåtkomst, inte behöver leva upp till de EU-rättsliga krav som EU-domstolen gett uttryck för. Reglerna om inhämtning av uppgifter om abonnemang för brottsbekämpande ändamål uppställer idag inga krav på att den aktuella brottsligheten ska vara av en viss svårhetsgrad. Det krävs inte heller någon förhandsprövning av beslut om sådan inhämtning och det finns inte någon myndighet med uppdrag att bedriva tillsyn över de brottsbekämpande myndigheternas tillämpning av reglerna. Jag menar att ytterligare utredning av dessa reglers förenlighet med EU-rätten är nödvändig.

[18] Kammarrätten har den 9 juni 2017 beslutat att inte meddela prövningstillstånd varför förvaltningsrättens beslut om inhibition står fast.

Särskilt yttrande av Kurt Alavaara och Per Lagerud

Allmänt om förslagen

Inledning

Lagringsskyldigheten och samtliga uppgifter som den omfattar enligt förordningen om elektronisk kommunikation är strängt nödvändiga för brottsbekämpningen. Enligt utredarens förslag ska lagringsskyldigheten minska tämligen kraftigt. Det kommer att få till följd att möjligheterna att förebygga, förhindra och utreda brott försämras avsevärt. I många fall kan konsekvenserna betecknas som mycket allvarliga. Med det särskilda yttrandet vill vi göra tydligt i den fortsatta beredningen vilka effekterna blir om lagringsskyldigheten minskas. Vi vill också framhålla att det är synnerligen angeläget att Sverige inom EU verkar för en lagringsskyldighet som svarar mot de behov som staten har av en både effektiv och rättssäker brottsbekämpning.

Syftet med lagringsskyldigheten

Allvarliga brott orsakar stora skador för enskilda och samhället. Det finns ett stort värde i att brotten kan förhindras eller klaras upp, kanske redan på planeringsstadiet. För samhället i stort, för medborgarna i allmänhet och för brottsoffren är det därför angeläget att förutsättningarna för att klara upp brotten är så goda som möjligt.

Att de brottsbekämpande myndigheterna har tillgång till trafik- och lokaliseringsuppgifter är avgörande för en effektiv bekämpning av grov brottslighet, inklusive sådan som är kopplad till nationell säkerhet. Utredaren anger att om de brottsbekämpande myndigheterna inte skulle ha tillgång till adekvata utredningsverktyg i den elektroniska miljön så skulle grova brott i vissa fall vara omöjliga att klara upp och brottsoffer i motsvarande omfattning vara skyddslösa. Vissa brott skulle i praktiken bli straffria och många målsägande skulle aldrig kunna få upprättelse. Utredaren konstaterar också att staten har en skyldighet att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda och, om intrång görs, se till att brotten utreds. Enligt utredaren skulle det inte vara förenligt med Sveriges internationella åtaganden att inte ge de brotts-

bekämpande myndigheterna möjlighet att effektivt utreda brott i den elektroniska miljön.

Trafik- och lokaliseringsuppgifter har med tiden blivit ett allt viktigare verktyg i brottsbekämpningen. I nuläget, där en stor del av brottsligheten lämnar digitala spår i någon form, är uppgifterna fundamentala. Det gäller i såväl underrättelse- som förundersökningsverksamhet. Uppgifterna används i stort sett i varje utredning av grov brottslighet. Ofta är uppgifterna dessutom den första och enda ingången i utredningarna och ger nyckeln till det vidare arbetet. Utan de nycklarna kommer dörren till framgång många gånger att vara stängd.

Bestämmelserna i bl.a. rättegångsbalken om tillgången till trafik- och lokaliseringsuppgifter syftar till att ge de brottsbekämpande myndigheterna information som kan klarlägga

– *vem* som kommunicerade med vem (dvs. källan och slutmålet). Det framgår av uppgifter om telefonnummer och ip-adresser (vid telefoni), e-postadresser, ip-adresser, SMS-nummer och MMS-nummer (vid meddelandehantering) och ip-adresser (vid internetåtkomst).
– *när* kommunikationen skedde. Det framgår av uppgifter om datum, spårbar tid vid start och slut (vid telefoni och meddelandehantering) och tid för på- och avloggning (vid internetåtkomst).
– *var* kommunikationen skedde. Det framgår främst av uppgifter om lokalisering (vid telefoni, meddelandehantering [indirekt genom ip-adress], internetåtkomst och tillhandahållande av kapacitet för internetåtkomst).
– *hur* kommunikationen skedde. Exempelvis om det är frågan om fast telefoni (inkl. fast ip-telefoni), mobil telefoni (inkl. mobil ip-telefoni), SMS, MMS, e-post eller om tjänsten vidarekoppling har använts.

Lagringsskyldigheten infördes för att säkerställa att uppgifterna kommer brottsbekämpningen till del genom de aktuella tvångsmedlen. I de delar lagringsskyldigheten begränsas kommer den garantin inte att finnas kvar. Resultatet blir att myndigheterna vid bekämpning av den grova brottsligheten får hoppas på turen att operatörerna ändå har sparat uppgifterna, t.ex. för fakturering. Detta

kommer i många fall att få allvarliga följder, inte minst eftersom lagringsskyldigheten redan idag innebär att enbart ett minimum av strängt nödvändiga uppgifter ska lagras.

Lagringsskyldigheten behöver inte begränsas

EU-domstolen bygger sitt avgörande på att den svenska regleringen ”… föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel...” (p. 97). Den beskrivningen är felaktig. Som utredaren konstaterar kan EU-domstolens uppfattning härledas från hur kammarrätten formulerade förfrågan till EU-domstolen (p. 51), och man måste därför, som utredaren anger, tolka EU-domstolens slutsatser i ljuset av hur kammarrätten ställde sina frågor.

Många av de kommunikationsmedel som ”den moderna människan” idag använder och många av de trafik- och lokaliseringsuppgifter som operatörerna behandlar omfattas inte av lagringsskyldigheten. Exempelvis omfattas inte

– web-surf (besök på hemsida),
– kommunikation mellan två ip-adresser som inte är telefoni (t.ex. Skype- och Vibersamtal),
– internetbaserad e-post såsom hotmail och g-mail,
– FTP (filöverföring),
– chat (meddelandetjänst),
– iMessage (meddelandetjänst),
– sociala medietjänster (såsom Facebook, Twitter, Viber, Whatsapp m.fl.) och
– informationssamhällestjänster (såsom Blocket, E-bay m.fl.). Inte heller omfattas följande uppgifter av lagringsskyldigheten.
– position när ett meddelande skickades och när det mottogs,
– position under ett mobilsamtal,
– position vid fast telefoni,

– utrustningsidentitet vid skickade och mottagna meddelanden,
– utrustningsidentitet vid fast telefoni,
– abonnemangsidentitet vid skickade och mottagna meddelanden,
– abonnemangsidentitet vid internetåtkomst,
– uppgifter om samtal med annat än vanligt telefonnummer (däribland uppringande och uppringt nummer, tid och position),
– uppgift om port och lokal ip-adress (dvs. den som används mellan abonnent och internetleverantör) vid internetåtkomst, meddelandehantering och ip-telefoni,
– uppgifter om samtal som inte kopplas fram på grund av tekniskt fel eller dylikt (däribland uppringande och uppringt nummer, tid, utrustning och position) och
– rena lokaliseringsuppgifter (positioner som inte är kopplade till kommunikation eller internetåtkomst).

Det är uppenbart att dagens lagringsskyldighet enbart innefattar en minimilista, som, redan när den kom till, bara uppfyllde de absolut mest grundläggande behoven vid utredning av grov brottslighet. Teknikutvecklingen för dessutom med sig att minimilistan relativt sett blir mindre och mindre i förhållanden till samtliga de trafik- och lokaliseringsuppgifter som operatörerna behandlar och de kommunikationsmedel som finns. Enligt vår uppfattning är lagring redan idag ett undantag och inte en huvudregel.

För oss står det klart att EU-domstolens avgörande bygger på felaktiga antaganden om hur den rättsliga regleringen förhåller sig till den tekniska verkligheten och den snabba utvecklingen på området. Lagringsskyldigheten omfattar inte på långa vägar samtliga uppgifter och kommunikationsmedel. Vi har förståelse för att utredaren valt att tolka avgörandet på det sätt han gjort. Samtidigt menar vi att det finns utrymme för att behålla dagens lagringsskyldighet oförändrad.

Att begränsa lagringsskyldigheten kan få mycket allvarliga konsekvenser

Efter EU-domstolens avgörande har operatörerna i stort slutat att lagra trafik- och lokaliseringsuppgifter för brottsbekämpande ändamål. I stället följer man huvudregeln i lagen om elektronisk kommunikation om att uppgifterna omedelbart ska raderas när de inte längre behövs i den egna verksamheten.

Tillgången till samtliga de uppgifter som lagringsskyldigheten omfattar är idag fundamental och strängt nödvändig för att Sveriges förmåga att bekämpa grov brottslighet och skydda nationella säkerhetsintressen inte ska urholkas. Tillgången fyller de absolut mest grundläggande behoven. Det kan i många fall få mycket allvarliga konsekvenser att begränsa den ytterligare.

Det är inte enbart förmågan att bekämpa brott i Sverige som kommer att påverkas negativt. Grov brottslighet är många gånger internationell till sin karaktär, vilket innebär att även det internationella brottsbekämpande arbetet påverkas negativt. Gärningsmän reser mellan länder eller har kontakter med, och kanske styrs av, personer i andra länder. Det internationella samarbetet inom brottsbekämpning är mycket omfattande och kommer att försvåras avsevärt när man t.ex. inte längre kan hitta svenska kopplingar till gränsöverskridande grov brottslighet eller, på samma sätt som tidigare, lämna biträde när utländska myndigheter skickar rättshjälpsbegäran till Sverige.

En av orsakerna till den mycket stora betydelse som trafik- och lokaliseringsuppgifter har vid utredningar av grov brottslighet är att den information som uppgifterna ger är unik, dvs. den kan inte ges genom andra metoder. De brottsbekämpande myndigheterna har ingen möjlighet att t.ex. börja arbeta på annat sätt för att kompensera för ett bortfall.

Visst kan fysisk spaning vid något tillfälle användas i stället för att lokaliseringsuppgifter inhämtas från operatörer. Den fysiska spaningen är dock vid jämförelse en mycket begränsad och även resurskrävande metod som knappast kan kallas ett alternativ till information från operatörerna. Snarare är spaningen ibland ett komplement. Utredaren anger också det självklara att det inte går att ersätta inhämtning av historiska trafik- och lokaliseringsuppgifter med fysisk spaning i realtid.

Det sägs också ibland att kriminaltekniska undersökningar av telefoner och datorer skulle vara ett alternativt sätt för de brottsbekämpande myndigheterna att få information. Det är en sanning med modifikation. För det första är beslag ett tvångsmedel som enbart får användas under förundersökning, alltså inte i underrättelseverksamhet. För det andra är det inte alls säkert att de telefoner eller datorer som kan kopplas till brottsligheten påträffas och kan tas i beslag. För det tredje är beslag inte hemligt för den som innehar föremålet. För det fjärde är trafik- och lokaliseringsuppgifter ofta en förutsättning för att över huvud taget rättsligt och praktiskt kunna genomföra husrannsakan, beslag och andra åtgärder med lyckat resultat. För det femte kan det inträffa att informationen i telefonen eller datorn inte är helt identisk med den som ges från operatörerna. För det sjätte kan en telefon eller dator vara krypterad så att det inte går att komma åt informationen.

Kedjan av uppgifter får inte brytas

Tillhandahållandet av elektroniska kommunikationstjänster sker idag på annat sätt än när telefonitjänst tillhandahölls av Televerket som enda operatör på marknaden. Idag kan många operatörer vara involverade i en och samma kommunikation. Till exempel kan en person ha abonnemang på fiberanslutning från en operatör, internetåtkomsten kan komma från annan och ip-telefonin från en tredje. Operatörerna behandlar enbart uppgifter om sin egen del i kommunikationskedjan. För att de brottsbekämpande myndigheterna ska kunna kartlägga kommunikationen krävs att myndigheterna får uppgifter från respektive operatör som gör det möjligt att gå vidare till nästa operatör i kedjan. Uppgifterna fungerar således som länkar som myndigheterna behöver i arbetet. Om lagringsskyldighet för en typ av uppgift tas bort kan den brygga mellan operatörerna som gör det möjligt att nå framgång försvinna. Detta påtalades också av företrädare för operatörerna i Trafikuppgiftsutredningen som en förutsättning för att kunna spåra deltagare i en kommunikation (SOU 2007:76). Den nuvarande minimilistan bygger också på den förutsättningen att kommunikationskedjan ska kunna följas.

Som exempel innebär utredarens förslag att ip-adresser ska lagras vid internetåtkomst men inte vid telefonitjänst och meddelande-

hantering. Om myndigheterna t.ex. har tillgång till en ip-adress som används av en viss person för internetåtkomst blir det i stort sett omöjligt att sedan knyta den adressen till telefoni- eller meddelandetjänster hos en annan operatör. Det innebär att vem personen kommunicerat med samt när, var och hur kommunikationen skedde inte kan klarläggas. Det logiska innehåll som minimilistan har bryts alltså om vissa uppgifter inte ska lagras i framtiden. Nackdelarna för brottsbekämpningen kan alltså bli än mer omfattande än man vid en första anblick kan tro när lagringsskyldigheten försvinner för vissa typer av uppgifter. Det är nödvändigt att beakta sådana negativa effekter.

Övrigt om några av förslagen

När det gäller frågan om riktad lagring är det, som utredaren anger, mycket svårt att i förväg veta när, var eller av vem ett allvarligt brott kommer att begås. Det är många gånger inte meningsfullt att i förväg rikta in lagringsskyldigheten mot vissa tider, områden eller personer. Vi instämmer med utredaren att det, vid en jämförelse, inte finns någon större nytta av en möjlighet till riktad lagring. Vi håller också med om att integritetsintrånget för de berörda personerna skulle vara påtagligt med en riktad lagring, och att sekretesskäl i princip skulle hindra att åtgärden genomförs. Orsaken till det sistnämnda är att både enskilda personer och myndigheternas verksamhet med stor sannolikhet skulle drabbas av skada om uppgifterna behöver lämnas till samtliga omkring 600 operatörer och deras anställda. En riktad lagring, enligt EU-domstolens tanke, skulle alltså föra med sig uppenbara begränsningar i det brottsbekämpande arbetet. Till det kommer att vi instämmer i utredarens tolkning av EU-domstolens yttrande den 26 juli 2017 (1/15) om PNR-uppgifter och möjligheter till generell lagring.

Vi instämmer även i utredarens bedömning att EU-domstolens avgörande inte rör abonnemangsuppgifter utan enbart trafik- och lokaliseringsuppgifter. Vi håller med om att det är åklagare som bör fatta beslut i IHL-ärenden, när beslutsordningen ska ändras. Det är också positivt att de brottsbekämpande myndigheternas tillgång till uppgifterna även fortsättningsvis ska avse uppgifter som opera-

törerna sparar för egna ändamål och att lagringen inte får ske utanför Sverige.

Vidare är det positivt att utredaren föreslår att operatörernas eget val av teknisk lösning, dvs. användning av NAT-teknik, inte längre ska vara ett hinder för att identifiera vilken ip-adress en användare har tilldelats. Säkerhetspolisen har erfarenhet av att det inte har gått att identifiera målsägande på grund av att deras ip-adresser inte har kunnat knytas till en identifierbar person. Det har varit mycket olyckligt.

Det är ytterst angeläget att bestämmelser om lagringsskyldighet träder ikraft så snart som möjligt; senast den 1 juli 2018.

Ytterligare om konsekvenserna för Säkerhetspolisens verksamhet

Säkerhetspolisen arbetar mot kvalificerade aktörer

I betänkandet nämner utredaren att lagringsskyldigheten redan idag är så pass begränsad att det är möjligt för en person med högt säkerhetsmedvetande att kommunicera på ett sätt som inte lämnar elektroniska spår som omfattas av skyldigheten, och att de begränsningar som föreslås av utredaren därför inte kommer att påverka möjligheterna att utreda brott där dessa personer är inblandade.

En mycket stor del av de utredningar som Säkerhetspolisen genomför, såväl i underrättelsearbetet som i förundersökningar, har en koppling till kvalificerade aktörer som är tränade och styrda av främmande makt eller av större organisationer, exempelvis terrororganisationer. Personerna har många gånger kvalificerad utbildning i att dölja elektroniska spår. Grunden i Säkerhetspolisens arbete i sådana fall är att hitta de mönster som aktörerna har i sin kommunikation och de avvikelser som finns eller de misstag som faktiskt görs, samt att analysera vilka slutsatser som kan dras av dessa. Sådana mönster, avvikelser och misstag ses ofta och kan bli avgörande för hur Säkerhetspolisen ska agera. Detta är kärnan i arbetet mot aktörer som är tränade och medvetna om att deras brottslighet är under bevakning och påverkas i hög grad av om möjligheten att få del av trafik- och lokaliseringsuppgifter skulle minska. Utredarens slutsats är alltså felaktig. Att begränsa Säkerhetspolisens åtkomst till trafik- och lokaliseringsuppgifter i arbetet mot kvalificerade, resursstarka,

uthålliga och systematiska aktörer kan därför få mycket allvarliga konsekvenser för Sveriges säkerhet.

Uppgifterna har avgörande betydelse även i underrättelseverksamheten

En förundersökning har ett bakåtblickande perspektiv, där de brottsutredande myndigheterna försöker klarlägga vad som hände vid ett visst tillfälle. Underrättelseverksamheten har främst ett framåtblickande perspektiv, där myndigheterna ska bedöma vad som kan komma att inträffa i framtiden, allt i syfte att förebygga och förhindra brott men också att upptäcka brott som myndigheterna hittills inte har kunskap om.

Till skillnad mot vad som gäller vid Polismyndigheten får Säkerhetspolisen sällan in anmälningar från allmänheten om redan begångna brott. I stället måste myndigheten själv genom underrättelsearbetet dels ”leta upp” intressanta personer och grupperingar samt företeelser, skeenden och modus som redan är eller som senare kan komma att utvecklas till brottslighet kopplad till nationell säkerhet, dels ta ställning till bl.a. tips och hot som myndigheten får del av. Därför är underrättelseverksamheten tyngdpunkten i Säkerhetspolisens bekämpning av t.ex. spionerи och terrorism. Arbetet innebär att Säkerhetspolisen hämtar in eller får information från många olika håll samt att myndigheten bearbetar och analyserar informationen och gör en bedömning av det som kommit fram. Om det finns skäl delges resultatet utomstående, främst till svenska eller utländska myndigheter. Arbetet syftar till att brottsligheten ska förebyggas, förhindras eller i vart fall upptäckas innan den fullbordas. Ytterst är det fråga om att bedöma hur reellt ett eventuellt hot är, alltså att bekräfta eller avfärda ett misstänkt hot. Inte sällan är den bedömning som ska göras tidskritisk.

För att ge en bild av detta s.k. underrättelseflöde, där trafik- och lokaliseringsuppgifter är fundamentala vid analys och bedömning, lämnas här några verkliga exempel på uppgifter som kommer till Säkerhetspolisen relativt frekvent, både från enskilda och från svenska och utländska myndigheter. I flera fall finns både en namngiven person i informationen och en utpekad plats. Uppgifterna har anonymiserats för att inte avslöja sekretessbelagd information.

– NN var med när en person fick erbjudande om att utföra attentat mot [viss plats i Sverige]
– NN har fått uppdrag att tillverka en bomb och detonera den mot [viss byggnad i Sverige]
– NN har lämnat uppgifter till IS:s attentatsplanerare
– NN planerar att utföra attentat på okänd plats i Sverige och har tillgång till vapen
– NN sympatiserar med IS och letar efter automatvapen
– NN har stridit för IS och bygger nu upp nätverk för att planera attack i Sverige
– NN vill få tag på en bomb och döda människor i Sverige
– NN ska placera ut en bomb i [en svensk stad]
– NN ska hämnas på [vissa personer] på [viss plats i Sverige]
– NN vill använda handgranater mot [vissa personer]
– NN är ansluten till IS, ligger bakom flera attentat och gömmer sig i Sverige
– NN kommer från [visst land] och ska vara redo för ”arbete” i Sverige
– NN har uppdrag från IS att genomföra attentat i Sverige
– NN vill placera ut bomber [på vissa platser i Sverige] och ta bort [vissa personer]

En central del av underrättelsearbetet innebär att personers kontakter och rörelsemönster kartläggs, alltså att aktörer, platser och tidpunkter kopplas samman. I det arbetet har trafik- och lokaliseringsuppgifter en mycket stor och ofta avgörande betydelse. Som Säkerhetspolisen tidigare angett är uppgifterna av ovärderlig vikt för myndighetens arbete (SOU 2015:31 s. 87). Även regeringen har uttryckt att Säkerhetspolisen har ett uppenbart behov av uppgifterna för att bedriva kontraspionageverksamhet och arbete mot terrorism (prop. 2016/17:186 s. 9). Resultatet av analysarbetet kan sedan ligga till grund för strategiska beslut eller operativa åtgärder från Säkerhetspolisens eller andras sida, bl.a. i syfte att reducera ett bekräftat

hot eller lagföra begångna brott. Skulle trafik- och lokaliseringsuppgifterna inte längre ges till Säkerhetspolisen kommer förmågan att exempelvis bedöma de attentatshot som ligger i uppgifterna ovan att försämras avsevärt och i värsta fall leda till att terroristbrott, som hade kunnat förhindras, fullbordas.

Det är mot den bakgrunden av stor vikt att underrättelseverksamheten, vars mål är att förebygga och förhindra att brott över huvud taget kommer att begås i framtiden, får lika stort fokus som förundersökningsverksamheten när omfattningen av lagringsskyldigheten diskuteras. Det gäller inte minst då utredaren själv konstaterar att de försämringar i underrättelseverksamheten som blir följden av en minskad lagringsskyldighet inte kommer att kunna kompenseras med andra åtgärder i någon större utsträckning. Utredaren menar också att förslagens påverkan på underrättelseverksamheten sannolikt kommer att bli större än på förundersökningsverksamheten. För Säkerhetspolisens del är det riktiga slutsatser.

Lagringsskyldigheten och tillgången till samtliga uppgifter är strängt nödvändiga

Säkerhetspolisen har visserligen under utredningsarbetet rangordnat trafik- och lokaliseringsuppgifterna, där vissa typer generellt sett har värderats högre respektive lägre än andra. Det måste dock understrykas att lagringsskyldigheten och samtliga uppgifter som den omfattar är strängt nödvändiga i Säkerhetspolisens arbete. Det gäller inte bara i underrättelseverksamheten utan även i de förundersökningar som bedrivs inom kontraspionaget och kontraterrorismen (inkl. författningsskyddet).

Det är visserligen en självklarhet, men för att undvika missförstånd ska dock sägas att samtliga typer av uppgifter inte samtidigt är strängt nödvändiga i varje utredning. Även om behovet varierar från ärende till ärende beroende bl.a. på vilken brottslighet det är fråga om och vilka personer som är inblandade, är lagringsskyldigheten och samtliga uppgifter den omfattar av avgörande betydelse i Säkerhetspolisens arbete med brottslighet som hotar Sveriges säkerhet.

Som framgick ovan har operatörerna efter EU-domstolens avgörande i stort slutat att lagra trafik- och lokaliseringsuppgifter för brottsbekämpande ändamål. I stället raderas uppgifterna när de inte längre behövs i respektive operatörs verksamhet. Det har lett till stora

problem för Säkerhetspolisen i arbetet med att skydda Sveriges säkerhet. Främmande makts illegala verksamhet mot Sverige har blivit svårare att bekämpa. Sverige har inte heller kunnat upprätthålla förmågan att upptäcka terroristnätverk och förhindra terroristattentat.

Nationell säkerhet

Den brottslighet som Säkerhetspolisen hanterar rör Sveriges säkerhet. I regeringens direktiv till utredaren (dir. 2017:16) anges att en särskild fråga är vilken effekt domen har på verksamhet som ligger inom Säkerhetspolisens ansvarsområde. Som utredaren konstaterar öppnar EU-domstolen för något mer tillåtande regler vad gäller nationell säkerhet.

Sedan EU-domstolens avgörande har terroristhotet mot Europa blivit än mer allvarligt, och Sverige har drabbats av ett fullbordat terroristattentat på Drottninggatan i Stockholm i april 2017. Det internationella samarbetet och utbytet av uppgifter mellan brottsbekämpande myndigheter är intensivt och ökar ständigt. I det arbetet är utbyte av information som har sin grund i elektroniska spår, dvs. trafik- och lokaliseringsuppgifter fundamental. Bl.a. genom sådana uppgifter har det gått att klarlägga svenska kopplingar till flera av de storskaliga terrorattacker som genomförts runt om i Europa under senare tid. Till det kommer att främmande makts verksamhet mot Sverige satts i fokus genom att frågor om kontraspionage och bristande säkerhetsskydd hos myndigheter och företag har uppmärksammats. Detta bör beaktas vid bedömningen av vilket utrymme som finns att reglera lagringsskyldigheten. För vår del saknar vi dock ett uttryckligt resonemang från utredarens sida om lagringsskyldighetens omfattning och betydelse när det gäller Sveriges säkerhet.

Närmare om innehållet i förslagen

Vem kommunicerade med vem?

Utredaren föreslår att uppgifter om *vem* som kommunicerade med vem inte längre ska lagras när det gäller fast telefoni (inkl. fast iptelefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator).

Uppgifter om vem som har haft kontakt med vem är fundamentala i de brottsbekämpande myndigheternas arbete med kartläggning av brottslighet, oavsett om det är fråga om förundersökning eller underrättelseverksamhet och oavsett kommunikationsmedel. Saknas de uppgifterna finns en stor risk att omständigheter missas och den vidare analysen och bedömningen får svagheter. Många gånger kommer det inte ens att finnas skäl att begära andra trafik- och lokaliseringsuppgifter från operatörerna, eftersom det fortsatta arbetet med uppgifterna blir meningslöst.

Fast ip-telefoni kommer, till skillnad från den ”vanliga” fasta telefonin, inte att försvinna inom några år. Säkerhetspolisen vill understryka att fast ip-telefoni är en modern tjänst som till stor del kan jämföras med mobil telefoni. Utvecklingen går mot att all telefoni blir ip-baserad och därmed mobil i olika avseenden. Ett och samma ip-telefoniabonnemang kan utnyttjas såväl från en fast telefon som från en mobil.

Sannolikt kommer också gränsen mellan fast och mobil nätanslutningspunkt att suddas ut eller bli diffus och medföra tolkningssvårigheter. Med en utökad anslutning av optofiber till både hem och företag med möjlighet att använda samma ip-telefonitjänst både hemma och på jobbet kan det redan idag konstateras att exempelvis telefonitjänster blir mer frikopplade från både geografisk plats och fysisk utrustning. Det skulle innebära allvarliga förluster av information för brottsbekämpningen om inte lagringsskyldigheten skulle omfatta den mest moderna typen av telefoni.

Det är bl.a. på grund av det sagda förenat med en stor risk för brottsbekämpningen att göra en differentiering mellan fast och mobil telefoni, eller fast och mobil nätanslutningspunkt. Det blir svårt att överblicka följderna framöver av en sådan gränsdragning, i synnerhet på ett område som elektronisk kommunikation där den tekniska utvecklingen går mycket fort.

Det kan vid en första anblick framstå som att, vid en jämförelse med andra uppgifter, borttagandet av lagringsskyldigheten för bl.a. fast telefoni inte skulle ge en särskilt stor skadlig effekt för brottsbekämpningen. Det måste dock framhållas att det inte är ovanligt att man inom spionage- och terrorismverksamhet använder fasta telefoner. Uppgifter kopplade till fast telefoni är fortfarande strängt nödvändiga i utredningarna och om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser. Inte minst kan man utgå

från att de kvalificerade aktörer som finns kommer att uppmärksamma en borttagen lagringsskyldighet och utnyttja den begränsningen i Sveriges förmåga att utifrån nationell säkerhet förhindra, försvåra, upptäcka och utreda brott mot Sveriges säkerhet. Att inhämta historiska uppgifter för att t.ex. identifiera de agenter som underrättelseofficerare har kontakt med kommer sannolikt att försvåras betydligt.

Avslutningsvis vill vi framålla att det är positivt att utredaren föreslår att utrustningsidentitet, som är en abonnemangsuppgift, ska lagras även i fortsättningen vid mobil telefoni. IMEI-nummer och MAC-adress är mycket viktiga för att identifiera hårdvaran som används vid en kommunikation. De uppgifterna ger, på samma sätt som uppringande eller uppringt nummer, information om vem som kommunicerat med vem.

När skedde kommunikationen?

Utredaren föreslår att uppgifter om *när* kommunikationen skedde inte längre ska lagras när det gäller fast telefoni (inkl. fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator).

Att få uppgift om vem som kommunicerat med vem är, som nyss framgick, fundamentalt i brottsbekämpningen. Den kunskapen riskerar att få liten betydelse om inte kontakten kan knytas till en viss tidpunkt genom datum och spårbar tid då kommunikationen påbörjades och avslutades eller ett meddelande skickades och mottogs.

Det är alltså många gånger avgörande att veta tidpunkterna för en kommunikation. Uppgifterna är viktiga pusselbitar i arbetet med att klarlägga personers kontakter, relationer och beteenden, och kan visa ”närheten” mellan personer och deras ageranden vid olika händelser.

Säkerhetspolisen arbetar med att kartlägga personer som ofta är mycket skickliga på att undvika att brottsligheten upptäcks. Som exempel kommunicerar spioner och terrorister ibland genom vissa samtalsmönster. Ett missat (ej besvarat) samtal kan betyda en sak, två uppringningar och ett kort samtal något annat osv. Ett kort eller missat samtal kan vara en kodad signal om att man ska prata på annat kommunikationsmedel, ett långt samtal kan indikera att man har en närmare relation och ett samtal som sker vid en viss tidpunkt kan

peka mot att det finns en medgärningsman etc. Avsaknad av denna information skulle försvåra bedömningarna betydligt och riskera att Säkerhetspolisen, även i akuta skeden, tappar förståelsen för spioners och terroristers avsikt och förmåga.

För att på ett effektivt sätt kunna lägga det pussel arbetet med Sveriges säkerhet innebär, krävs alltså tillgång till detaljerade tidsangivelser för kommunikation vid alla kommunikationsmedel. Uppgifterna är strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet, och om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser.

Allmänt ska också nämnas något om ärenden som rör elektroniska angrepp. Där är tidsuppgifter om en aktörs internetanvändning, tillsammans med tider då ”attacker” genomförts, avgörande pusselbitar för att kunna förebygga, förhindra och utreda sådana brott med kopplingar till nationell säkerhet. Cyberhot är ett prioriterat område och uppgifter om bl.a. spårbar tid är strängt nödvändiga för att bekämpa brottsligheten.

Var skedde kommunikationen?

Utredaren föreslår att uppgifter om *var* kommunikationen skedde, dvs. lokaliseringsuppgifter, inte längre ska lagras när det gäller fast telefoni (inkl. fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator). Eftersom utredaren även föreslår att uppringandes och uppringds ip-adress inte längre ska lagras, innebär det att uppgifter om var kommunikationen skedde inte heller kommer fram vid mobil ip-telefoni och vid meddelandehantering (t.ex. sms-, mms- och e-postmeddelanden) via mobil internetåtkomst.

Även uppgifter om var en viss utrustning befann sig när kommunikation skedde är fundamentala uppgifter i brottsbekämpningen. De är ofta avgörande i både förundersökning och underrättelseverksamhet och kan i vissa fall vara av större värde än uppgifter om vilka som har kommunicerat med varandra. Om Säkerhetspolisen inte längre genom lokaliseringsuppgifter kan placera en person på en viss plats vid en given tidpunkt, kan det i många fall få mycket allvarliga effekter i bekämpningen av brott kopplade till nationell säkerhet. Det blir mycket svårare att på olika sätt ingripa mot spioneri och

terrorism, t.ex. genom att lokalisera brottsplatser, gärningsmän, ”safehouses”, vapengömmor, provsprängningsplatser m.m. Det kommer inte längre att gå att kartlägga hur en person rört sig över tid för att t.ex. planera, rekognosera, träffa medgärningsmän, utföra brottet, gömma sig etc. Att vara hänvisad till basstationstömningar är inte tillräckligt, bl.a. eftersom det ofta är oklart vilket geografiskt område som är aktuellt.

Inte minst i spioneriutredningar, där kvalificerade aktörer agerar, är rörelsemönster hos underrättelseofficerare och deras agenter avgörande uppgifter. I många fall kan tillgång till lokaliseringsuppgifter vara det enda sättet för Säkerhetspolisen att knyta personer till en viss plats vid en viss tidpunkt. Om uppgifterna inte lagras, skulle det göra Säkerhetspolisen nästan blind i dessa ärenden. Den negativa påverkan på Säkerhetspolisens arbete mot främmande makts underrättelseverksamhet i Sverige skulle bli mycket stor. Inom Säkerhetspolisens kontraspionageverksamhet har effekterna beskrivits som närmast oöverblickbara.

I terrorutredningar händer det mycket ofta att Säkerhetspolisen får information som anger att ett visst telefonnummer eller liknande finns i Sverige och att den som använder adressen har för avsikt att, tillsammans med andra okända aktörer, genomföra attentat i Sverige eller närliggande länder. Skulle Säkerhetspolisen vid sådana tillfällen, ofta i tidskritiska skeden, inte få tillgång till historiska trafik- och lokaliseringsuppgifter för att klarlägga positioner och kontakter kan det finnas stor risk för att misstänkta hot inte kan bedömas och reduceras.

Lokaliseringsuppgifter är alltså strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet. I Ds 2014:23 (s. 52) anges att polisen bedömt att uppgifterna är extremt viktiga. Vi instämmer i det. Om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser.

För tydlighetens skull måste också sägas att lokaliseringsuppgifter för kommunikationens slut oftast är lika viktiga som uppgifter som rör kommunikationens början, vilket utredaren också tagit med i sitt förslag rörande telefoni via mobil nätanslutningspunkt. Om uppgifter rörande kommunikationens slut inte lagras kommer ett modus att bli att spioner och terrorister startar kommunikation med andra gärningsmän för att därefter låta samtalet vara uppkopplat under t.ex. rekognosering, bevakning av tilltänkta brottsoffer, resor,

möten eller andra ”konspirativa handlingar”, allt för att undgå att lämna uppgifter om positionen i samband med att brott begås eller vid ageranden som kan kopplas till brottsligheten.

Uppgifter om vilken typ av kapacitet som den enskilde abonnerar på för att få internetåtkomst är också av grundläggande betydelse i sammanhanget (t.ex. fast fiber, xDSL, GPRS eller UMTS). Uppgifterna ger nämligen indirekt tillgång till lokaliseringsinformation. Förmågan att bekämpa brottslighet kommer alltså att påverkas negativt, eftersom utredaren föreslår att dessa uppgifter inte längre ska omfattas av lagringsskyldigheten (se även nedan).

Hur skedde kommunikationen?

Utredaren föreslår att uppgifter om *hur* kommunikationen skedde inte längre ska lagras när det gäller fast telefoni (inkl. fast ip-telefoni) och meddelandehantering via fast nätanslutningspunkt (t.ex. meddelanden från en ”fast” dator). Sådana uppgifter kan röra att det är fråga om talkommunikation, att ett e-postkonto har använts, att vidarekoppling har använts, att flera operatörer har varit inblandade i kommunikationen, att det finns en röstbrevlåda kopplad till abonnemanget eller att samtal inte har besvarats. Vidare föreslår utredaren att uppgifter om kapacitet för att få internetåtkomst inte längre ska lagras.

Inom den brottslighet som Säkerhetspolisen bekämpar förekommer det ofta att personer vidarekopplar kommunikationen till andra adresser. Det är enkelt att vidarekoppla samtal till en fast telefon till en mobiltelefon eller liknande. En orsak kan vara att man vill dölja ageranden som har med brottsligheten att göra. Den enskilt största förlusten av en borttagen lagringsskyldighet skulle bli att möjligheten att spåra samtal som styrs till mobila telefoner upphör. Samtliga uppgifter om kommunikationen blir ”tvättade” genom de fasta telefonerna. Det skulle innebära stora nackdelar i arbetet med att spåra de nummer som faktiskt används i kommunikationen och skulle öppna en möjlighet att komma undan brottsbekämpningen genom att fasta telefoner används som bryggor som bryter spårbarheten i kommunikationskedjan. Det öppnas med andra ord en enkel möjlighet att dölja vem som är mottagare av ett samtal.

Främmande makt som bedriver olaglig verksamhet i Sverige använder ofta olika samtalsmönster för att kommunicera, i stället för att kommunicera i klartext (se ovan). Att vidarekoppla kommunikation kan vara del av det. Vidarekoppling kan också användas för att dölja positionen vid ett visst tillfälle. Det förekommer dessutom ofta att gärningsmän stänger av sin telefon inför någon aktivitet som kopplas till brottsligheten. Eventuella samtal går då vidare till annan person eller till röstbrevlådan i syfte att dölja det faktiska användandet av mobiltelefonen.

En annan tjänst som är viktig att få uppgifter om är om det finns abonnemang på röstbrevlåda och när den i så fall har varit inkopplad. Innehållet i röstbrevlådan omfattas inte av lagringsskyldigheten, men uppgiften är viktig för att bedöma om man ska gå vidare med bl.a. tillstånd till hemlig avlyssning av elektronisk kommunikation.

För Säkerhetspolisen är behovet av att veta vilken typ av kapacitet som den enskilde abonnerar på för att få internetåtkomst av grundläggande betydelse (t.ex. fast fiber, xDSL, GPRS eller UMTS). Uppgifterna ger information t.ex. om anslutningsformen är fast eller mobil, vilket i sig kan ge lokaliseringsinformation. När utredningen dessutom föreslår att lagringsskyldigheten för lokaliseringsuppgifter ska minska (se ovan), innebär borttagandet av de nu aktuella uppgifterna en dubbel negativ effekt för brottsbekämpningen. Uppgifterna kan också ge information om vem som är abonnent. Därutöver behövs uppgifterna vid verkställighet av hemlig avlyssning av elektronisk kommunikation så att rätt teknik används. Skulle hemlig dataavläsning bli tillåten i framtiden är uppgifter om kapacitet för internetåtkomst av stor betydelse för bedömningen av vilken teknik som ska användas i respektive fall.

Om lagringsskyldigheten skulle tas bort kommer det att bli mycket svårare att identifiera utländska hot som verkar i Sverige. Spioner och terrorister skulle få större möjligheter till säker kommunikation. Säkerhetspolisen kan med visshet säga att de möjligheter som öppnas kommer att utnyttjas av spioner och terrorister som är inblandade i brottlighet som rör Sveriges säkerhet. Uppgifterna är alltså strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet. Om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser.

Lagringstiden

Utredarens förslag innebär att lagringstiderna differentieras utifrån hur gamla uppgifter det finns ett påtagligt behov av. Han föreslår att lokaliseringsuppgifter vid samtal ska lagras i 2 månader. Uppgifter om internetåtkomst, förutom uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs, ska lagras i 10 månader och övriga uppgifter i 6 månader.

Vi har ingen invändning i sig mot principen att lagringstiderna differentieras men kan konstatera att utredaren inte berör Säkerhetspolisen i sina resonemang.

Brott mot nationell säkerhet, som spioneri och terrorism, är speciella till sin karaktär i den meningen att brottsligheten ofta pågår under mycket lång tid.

För främmande makt kan det ta flera år att värva en agent med tillgång till skyddsvärd information. Brottsligheten är utdragen i tiden och sker i flera steg med faser som karaktäriseras av analys, målsökning, kartläggning, närmande, vänskap, värvning och inhämtning av hemlig information.

Även terrorism präglas av att brottsligheten många gånger är utdragen i tiden och att den sker i samverkan mellan flera. En process där en person utvecklas till en ideologiskt motiverad aktör med terroravsikt kan ta lång tid. Dessutom måste personen skaffa sig förmåga att planera och fullborda brott. Det sistnämnda innefattar både kunskap och materiel.

Det är ofta inte möjligt att redan i ett inledningsskede av kartläggningsarbetet förutse vilka trafik- och lokaliseringsuppgifter som bör inhämtas. Utredaren anger att behovet av äldre uppgifter än fem månader inte är särskilt stort i underrättelseverksamhet. Som utredaren antyder gäller det inte för Säkerhetspolisen. Trafikuppgiftsutredningen nämnde att bl.a. terroristbrott är en typ av brottslighet där mer än två år gamla uppgifter behövs (SOU 2007:76 s. 173 ff.).

Vi ser positivt på att utredaren föreslår att lagringstiden för vissa uppgifter ska förlängas från sex till tio månader. Däremot ser vi, utifrån perspektivet Sveriges säkerhet, allvarligt på att tiden för lokaliseringsuppgifter vid samtal ska minskas från sex till två månader.

Vi beskrev ovan hur grundläggande uppgifter om var kommunikation skedde är i Säkerhetspolisens arbete. Uppgifterna är strängt nödvändiga i såväl förundersöknings- som underrättelsearbetet och

om lagringsskyldigheten begränsas kan det få mycket allvarliga konsekvenser. Om utredarens förslag blir verklighet kommer inte enbart lagringsskyldigheten för lokaliseringsuppgifter att minska utan även lagringstiden. Vi är kritiska till detta.

Kommittédirektiv 2017:16

Datalagring och EU-rätten

Beslut vid regeringssammanträde den 16 februari 2017

Sammanfattning

En särskild utredare ska se över bestämmelserna om skyldigheten att lagra uppgifter om elektronisk kommunikation som gäller för leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster, samt bestämmelserna om de brottsbekämpande myndigheternas tillgång till sådana uppgifter. Översynen ska ske i syfte att anpassa det svenska regelverket till EU-rätten såsom den uttolkats av EU-domstolen i förhandsavgörandet den 21 december 2016 i de förenade målen C-203/15 och C-698/15. Utredaren ska föreslå de förändringar som är nödvändiga för att det svenska regelverket ska vara proportionerligt och ha en ändamålsenlig balans mellan skyddet för enskildas personliga integritet och behovet av uppgifter för att kunna förebygga, förhindra, upptäcka, utreda och lagföra brott.

Utredaren ska också se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när hemliga tvångsmedel för särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet används.

Uppdraget ska redovisas senast den 16 augusti 2018. Den del av uppdraget som ges med anledning av EU-domstolens förhandsavgörande om datalagring ska delredovisas senast den 9 oktober 2017.

Reglerna om datalagring och om vissa hemliga tvångsmedel behöver ses över

Leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster (leverantörerna) ska enligt lagen (2003:389) om elektronisk kommunikation (LEK) lagra vissa uppgifter om bl.a. telefonsamtal, internettrafik och meddelandehantering för att uppgifterna ska kunna användas vid brottsbekämpning. Villkoren för de brottsbekämpande myndigheternas inhämtning av dessa uppgifter regleras närmare i LEK, rättegångsbalken och lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen).

EU-domstolen har, efter en begäran om ett förhandsavgörande från Kammarrätten i Stockholm, nyligen prövat om de svenska reglerna om datalagring och om tillgången till lagrade uppgifter stämmer överens med EU-rätten. Avgörandet klargör att svensk rätt inte stämmer överens med EU-rätten på ett flertal punkter. Lagstiftningen behöver därför ses över och ändras.

Den 1 januari 2015 permanentades ett antal bestämmelser om hemliga tvångsmedel som fram till dess varit tidsbegränsade. I samband med uppdraget att se över frågorna om datalagring och åtkomst till lagrade uppgifter finns det även skäl att se över hur rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten när man använder dessa hemliga tvångsmedel fungerar.

Uppdraget att se över den svenska datalagringsregleringen i ljuset av EU-domstolens förhandsavgörande om datalagring

Den svenska regleringen har prövats av EU-domstolen

EU-domstolen (förenade målen C 293/12 och C 594/12) ogiltigförklarade i april 2014 det s.k. datalagringsdirektivet (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). Syftet med direktivet var att harmonisera medlemsstaternas bestämmelser om skyldighet att lagra vissa uppgifter om elektronisk kommuni-

kation för att säkerställa att uppgifterna är tillgängliga för utredning, avslöjande och åtal av brott som medlemsstaterna anser vara allvarliga. Enligt domstolens bedömning överskred EU:s lagstiftande församlingar sina befogenheter när direktivet antogs, eftersom det inte levde upp till proportionalitetsprincipen när det gällde artiklarna 7, 8 och 52.1 i EU:s stadga om de grundläggande rättigheterna (EU-stadgan). Artikel 7 reglerar rätten till respekt för bl.a. privat- och familjelivet och artikel 8 rätten till skydd av personuppgifter. Enligt artikel 52.1 måste varje begränsning i utövandet av fri-och rättigheter som erkänns i EU-stadgan vara föreskriven i lag och vara förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors fri- och rättigheter.

Till följd av ogiltigförklaringen faller nu EU-rätten när det gäller datalagring för brottsbekämpning tillbaka på artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (direktiv 2002/58). Där anges närmare under vilka förutsättningar medlemsstaterna får vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i direktivet. Direktivet är inte tillämpligt på verksamheter som avser allmän säkerhet, försvar, statens säkerhet och statens verksamhet på straffrättens område (artikel 1.3).

Det ogiltigförklarade direktivet genomfördes i svensk rätt genom ändringar i framför allt LEK (prop. 2010/11:46, bet. 2011/12:JuU28, rskr. 2011/12:166). Enligt 6 kap. 16 a § i den lagen är leverantörerna skyldiga att lagra vissa uppgifter som genereras eller behandlas i samband med att tjänster tillhandahålls, för att uppgifterna ska kunna användas vid brottsbekämpning. Lagringsskyldigheten gäller i sex månader från den dag kommunikationen avslutades. Som huvudregel ska den lagringsskyldige sedan genast utplåna uppgifterna (6 kap. 16 d § LEK).

Skyldigheten att lagra data enligt de svenska bestämmelserna ifrågasattes efter EU-domstolens dom där datalagringsdirektivet ogiltigförklarades. Flera leverantörer meddelade att de tänkte sluta lagra uppgifter enligt de tvingande reglerna i LEK, och i vissa fall att

man tänkte radera redan lagrade uppgifter. Post- och telestyrelsen förelade därför flera leverantörer att fortsätta med sin lagring. Med anledning av ett överklagande av ett sådant föreläggande begärde Kammarrätten i Stockholm ett förhandsavgörande från EU-domstolen (mål nr 7380-14). Frågorna tog sikte på rättsläget enligt artikel 15.1 i direktiv 2002/58, i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG, och artiklarna 7, 8 och 52.1 i EU-stadgan.

EU-domstolen besvarade kammarrättens begäran om förhandsavgörande genom en dom den 21 december 2016 (förenade målen C-203/15 och C-698/15). EU-domstolens slutsats var bl.a. att en generell och odifferentierad lagring av uppgifter om elektronisk kommunikation inte är förenlig med EU-rätten. Domstolen framhöll bl.a. att dessa uppgifter sammantagna kan göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vars uppgifter har lagrats, och att kartlägga de berörda personerna på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationerna. Domstolen gjorde även vissa uttalanden om förutsättningarna för de brottsbekämpande myndigheternas åtkomst till lagrade uppgifter samt om säkerheten för uppgifterna.

Kammarrätten beslutade dagen därpå att Post- och telestyrelsens föreläggande om fortsatt lagring tills vidare inte ska gälla. Kammarrätten har inte slutligt avgjort målet.

Uppgifter som kan lagras

Den centrala bestämmelsen om lagringsskyldighetens omfattning finns i 6 kap. 16 a § LEK. Skyldigheten omfattar uppgifter som anges som nödvändiga för vissa bestämda syften.

Dessa är preciserade som uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för den, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut. Även uppgifter som genereras eller behandlas vid misslyckade uppringningar ska lagras. Innehållet i kommunikationen lagras däremot inte. Lagringsskyldigheten är närmare strukturerad i vissa tekniskslag. Dessa är angivna som telefonitjänst, meddelandehantering, internet-

åtkomst och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform). I 39–43 §§ förordningen (2003:396) om elektronisk kommunikation (FEK) finns ytterligare bestämmelser om vilka uppgifter som ska lagras.

EU-domstolen har i förhandsavgörandet slagit fast att lagringsskyldigheten enligt LEK överskrider gränserna för vad som är strängt nödvändigt och att den inte kan anses motiverad i ett demokratiskt samhälle i enlighet med artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i EU-stadgan. En generell och odifferentierad lagring av uppgifter – utan att det görs någon åtskillnad, begränsning eller undantag utifrån syftet att bekämpa brott – är alltså inte tillåten. I sammanhanget påpekas bl.a. att den omständigheten att lagringen och den senare användningen av uppgifterna sker utan att abonnenten är underrättad om det kan ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning. Det finns enligt EU-domstolen däremot inget hinder mot att i förebyggande syfte tillämpa en riktad lagring i syfte att bekämpa grov brottslighet. En sådan datalagring förutsätter dock att lagringen begränsas till vad som är strängt nödvändig när det gäller vilka slags uppgifter som ska lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske.

Att kunna få tillgång till lagrade uppgifter om elektronisk kommunikation är av mycket stort värde för rättsväsendets myndigheter i arbetet med att förebygga, förhindra, upptäcka, utreda och lagföra brott, inte minst när det gäller grov brottslighet. Genom att sådana uppgifter finns lagrade – och därmed kan hämtas in av de brottsbekämpande myndigheterna – går det att klarlägga händelser som anknyter till såväl själva brottstillfället som till t.ex. planläggning eller flykt. I många fall, t.ex. vid barnpornografibrott, kan uppgifter om elektronisk kommunikation vara avgörande för att man ska kunna identifiera en misstänkt gärningsman. Uppgifterna har även stor betydelse för att man ska kunna bekräfta brottsmisstankar.

Inom ramen för de riktlinjer EU-domstolen drar upp bör det även i fortsättningen, vid sidan av de uppgifter leverantörerna lagrar frivilligt, finnas ett utrymme för att i lagstiftningen kunna ha tvingande regler för leverantörernas lagring av uppgifter om elektronisk kommunikation. Hur stort detta utrymme är och vilket behov det finns av det måste dock utredas. Målsättningen är att upprätthålla ett starkt skydd för de grundläggande rättigheterna som står sig

väl vid en rättslig prövning, samtidigt som de brottsbekämpande myndigheternas möjligheter att upprätthålla sin förmåga att förebygga, förhindra, upptäcka, utreda och lagföra brott kan tillgodoses. En särskild fråga i sammanhanget är också vilken effekt domen har på verksamhet som avser Sveriges säkerhet, dvs. sådan verksamhet som ligger inom Säkerhetspolisens ansvarsområde.

Utredaren ska

- analysera hur reglerna om lagring av uppgifter enligt 6 kap. 16 a § LEK och 39–43 §§ FEK förhåller sig till EU-domstolens dom,
- med beaktande av skyddet för den personliga integriteten och yttrandefriheten, överväga olika alternativ till förändringar i de delar reglerna inte bedöms vara förenliga med domen och belysa fördelarna och nackdelarna med dessa alternativ, och
- föreslå de författningsändringar och andra åtgärder som behövs.

Tillgången till lagrade uppgifter

EU-domstolen uttalar sig i domen också om vilka villkor som ska gälla för att behöriga nationella myndigheter ska få tillgång till lagrade uppgifter. För att begränsa tillgången till vad som är strängt nödvändigt krävs, enligt EU-domstolen, i princip att uppgifterna rör personer som misstänks planera, begå eller ha begått ett allvarligt brott eller som på något annat sätt är inblandade i ett sådant brott. När vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism kan tillgång dock även ges till uppgifter om andra personer. Vidare ska tillgången normalt – utom i brådskande fall – kräva förhandskontroll av en domstol eller en oberoende myndighet. Den person som de inhämtade uppgifterna rör ska dessutom underrättas om åtgärden så snart en sådan upplysning inte riskerar att skada utredningen.

Bestämmelser om tillgången till uppgifter som ska lagras finns i flera olika regleringar. Regler om inhämtning av abonnemangsuppgifter finns i 6 kap. 22 § första stycket 2 LEK, regler om inhämtning av trafik- och lokaliseringsuppgifter under förundersökning i 27 kap. 19 § rättegångsbalken och regler om inhämtning av trafik- och lokaliseringsuppgifter i underrättelseverksamhet finns i inhämtningslagen.

Det stora flertalet av de brottstyper som omfattas av regleringen om hemlig övervakning av elektronisk kommunikation har ett straffminimum på sex månaders fängelse. Tvångsmedlet får dock även användas i vissa andra fall, t.ex. vid dataintrång, barnpornografibrott och samhällsfarliga brott inom Säkerhetspolisens verksamhetsområde. Det får dessutom i förekommande fall användas vid förundersökning om försök, förberedelse eller stämpling till sådan brottslighet. Det finns också vissa bestämmelser i andra lagar som utvidgar tillämpningsområdet för tvångsmedlet. Enligt lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott får exempelvis hemlig övervakning av elektronisk kommunikation användas för brott som inte uppfyller kraven på brottets svårhet enligt reglerna i rättegångsbalken.

Huvudregeln är att hemlig övervakning av elektronisk kommunikation bara får användas efter förhandsprövning och beslut av domstol. Tillstånd får under vissa förutsättningar dock även ges interimistiskt av åklagare i avvaktan på domstolens prövning. Enskilda som har utsatts för användning av tvångsmedlet ska enligt huvudregeln underrättas om åtgärden i efterhand.

I princip motsvarande uppgifter som kan hämtas in enligt reglerna om hemlig övervakning av elektronisk kommunikation kan i Polismyndighetens, Säkerhetspolisens och Tullverkets underrättelseverksamhet hämtas in enligt inhämtningslagen. Uppgifterna får under vissa förutsättningar hämtas in för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott med ett straffminimum på två års fängelse, eller som avser vissa särskilt angivna brott inom Säkerhetspolisens ansvarsområde. Till skillnad från regleringen om hemlig övervakning av elektronisk kommunikation är beslut om inhämtning av uppgifter enligt inhämtningslagen inte föremål för någon utomstående förhandsprövning utan fattas på egen hand av respektive myndighet. Lagen innehåller inte heller någon motsvarighet till rättegångsbalkens krav på underrättelse till enskilda.

Inte heller vid inhämtning av abonnemangsuppgifter enligt LEK finns det något krav på föregående kontroll av en oberoende instans. Uppgifterna får alltså hämtas in efter beslut av den brottsbekämpande myndigheten själv. Regleringen ställer inte heller några krav på underrättelse i efterhand eller att den brottslighet som uppgifterna lämnas ut för ska vara av en viss svårhetsgrad. De brottsbekämpande

myndigheterna har således rätt att få tillgång till uppgifter om abonnemang – t.ex. abonnentens nummer, namn och adress – vid alla typer av brott utom sådana brott där åtal enbart får väckas av målsäganden. Bestämmelsens utformning motiverades med att trakasserier via internet av olika slag, nätmobbning och förtal liksom vuxnas kontakter med barn i sexuella syften (grooming), hade blivit ett allt större problem och att möjligheten att ingripa mot sådana brott ofta var begränsade eftersom det saknades tillgång till abonnemangsuppgifter som kunde identifiera abonnenten (prop. 2011/12:55, s. 102). Abonnemangsuppgifter hämtas även in i underrättelseskedet (SOU 2015:31, s. 198 f.)

EU-domstolens dom innebär att regelverkens nuvarande utformning behöver ses över när det gäller de närmare förutsättningarna för myndigheternas tillgång till uppgifter. Det gäller t.ex. vilka krav som bör ställas på brottets allvar för att uppgifterna ska få hämtas in. En annan sådan fråga är vad som sägs i domen om krav på underrättelse till enskilda. Även beslutsordningen för att få hämta in lagrade uppgifter behöver ses över liksom frågan om det behövs ett särskilt skydd för uppgifter som omfattas av yrkesmässig tystnadsplikt.

Utredaren ska

- analysera hur dagens regler om tillgång till uppgifter som lagras förhåller sig till EU-domstolens dom,
- överväga olika alternativ till förändringar i de delar reglerna inte bedöms vara förenliga med domen och belysa fördelarna och nackdelarna med dessa alternativ, och
- föreslå de författningsändringar och andra åtgärder som behövs.

Vid utformningen av förslagen bör den gräns som i dag råder mellan underrättelseverksamhet och brottsutredande verksamhet inom ramen för en förundersökning beaktas så långt som möjligt.

Skyddet och säkerheten för de lagrade uppgifterna

Den som är skyldig att lagra uppgifter enligt reglerna i LEK är också ansvarig för att skydda uppgifterna. Den lagringsskyldige ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling (6 kap. 3 a § första

stycket LEK). Ytterligare föreskrifter om säkerheten för de lagrade uppgifterna finns i bl.a. 37 § FEK. Det finns inget krav i Sverige på att uppgifterna ska lagras inom ett visst område, t.ex. inom EU.

Uppgifterna ska vidare utplånas vid lagringstidens slut eller, om en begäran om utlämnande har inkommit men inte hunnit behandlas inom denna tid, så fort uppgifterna har lämnats ut (6 kap. 16 d § LEK). Att reglerna följs står under tillsyn av Post- och telestyrelsen.

EU-domstolen uttalar sig i förhandsavgörandet även i dessa frågor. Med hänsyn till att det bl.a. handlar om en stor mängd uppgifter av känslig natur måste leverantörerna av elektroniska kommunikationstjänster, för att säkerställa fullständig integritet och konfidentialitet för uppgifterna, garantera en särskilt hög skydds- och säkerhetsnivå. EU-domstolen konstaterar också att den nationella lagstiftningen i synnerhet måste föreskriva att lagringen sker inom unionen och att uppgifterna oåterkalleligen förstörs när deras lagringstid gått ut. I domen pekas även på vikten av kontroll av en oberoende myndighet.

Utredaren ska

- analysera hur nuvarande regler om skydd av och säkerhet för uppgifter som lagras förhåller sig till EU-domstolens dom,
- överväga olika alternativ till förändringar i de delar reglerna inte bedöms vara förenliga med domen och belysa fördelarna och nackdelarna med dessa alternativ, och
- föreslå de författningsändringar och andra åtgärder som behövs.

Internationell utblick

Utredaren ska redovisa gällande rätt och pågående arbete i Finland och Danmark och de övriga länder som bedöms vara relevanta för utredningsuppdraget, t.ex. Österrike, Tyskland och Nederländerna, och i övrigt göra de internationella jämförelser som utredaren bedömer befogade.

Utredaren ska även följa arbetet med EU-kommissionens förslag till förordning om integritet och elektronisk kommunikation (COM [2017], 10 final, 2017/0003 [COD]) och, i den mån det bedöms nödvändigt, eventuellt arbete på EU-nivå med anledning av EU-domstolens förhandsavgörande.

Målet i kammarrätten

Enligt EU-domstolen ankommer det på Kammarrätten i Stockholm att pröva om och i så fall i vilken utsträckning den svenska regleringen uppfyller kraven enligt artikel 15.1 i direktiv 2002/58 jämfört med artiklarna 7, 8, 11 och artikel 52.1 i EU-stadgan, såsom de preciseras i förhandsavgörandet, när det gäller behöriga nationella myndigheters tillgång till lagrade uppgifter och skyddet av och säkerheten för uppgifterna.

Utredaren ska vid utformningen av sina förslag, i den mån utredaren bedömer det relevant, beakta utfallet av kammarrättens prövning.

Närliggande frågor

Utredaren får ta upp sådana närliggande frågor som har samband med de frågeställningar som ska utredas, under förutsättning att uppdraget ändå bedöms kunna redovisas i tid. Exempel på sådana frågor är vilken efterhandskontroll som bör finnas samt om någon myndighet bör ha tillsyn över att uppgifter om elektronisk kommunikation lämnas ut på ett korrekt sätt.

Uppdraget att se över rättssäkerhetsgarantierna och mekanismerna som ska skydda den personliga integriteten vid användning av hemliga tvångsmedel för vissa allvarliga brott

Permanentningen av reglerna om hemliga tvångsmedel

Under senare år har kriminaliteten blivit alltmer komplex och svårutredd. Att information kan hämtas in är som nämnts centralt för att de brottsbekämpande myndigheterna på ett effektivt sätt ska kunna förebygga, förhindra och utreda brott. När det gäller särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet är inhämtning av information genom användning av hemliga tvångsmedel i många fall de enda verktyg som kan användas för att driva en brottsutredning framåt.

Regler om hemliga tvångsmedel för den typen av brottslighet finns framför allt i rättegångsbalken och i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott. Lagen, som regle-

rar möjligheten att använda hemliga tvångsmedel utan att en förundersökning pågår, var tidigare tidsbegränsad men gjordes permanent genom lagändringar som trädde i kraft den 1 januari 2015. Genom en överflyttning till rättegångsbalken permanentades samtidigt även bestämmelserna i två andra tidsbegränsade lagar med bestämmelser om hemliga tvångsmedel för särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet, nämligen lagen (2007:978) om hemlig rumsavlyssning och lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott (prop. 2013/14:237, bet. 2014/15:JuU2, rskr. 2014/15:22).

En avvägning mellan enskildas rätt till integritet och rättssäkerhet och behovet av en effektiv brottsbekämpning

Det är samtidigt av grundläggande betydelse i en rättsstat att rätten till skydd för privat- och familjelivet respekteras. De hemliga tvångsmedlen inskränker de rättigheter som var och en har enligt regeringsformen och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Varje befogenhet för staten att i hemlighet bereda sig tillgång till personlig information, och varje utnyttjande av denna befogenhet, leder till ingrepp i den personliga integriteten. Graden av integritetsintrång varierar med befogenhetens (tvångsmedlets) utformning och tillämpning. Regleringen om hemliga tvångsmedel bygger på en avvägning mellan å ena sidan samhällets behov av en effektiv brottsbekämpning till skydd för medborgarna och å andra sidan enskildas rätt till integritet och rättssäkerhet i förhållande till staten.

Rättssäkerhetsgarantier och mekanismer till skydd för den personliga integriteten

Avvägningen har resulterat i att regleringen omgärdas av ett antal rättssäkerhetsgarantier och mekanismer för att säkerställa att reglerna och deras tillämpning lever upp till högt ställda krav på rättssäkerhet och att intrånget i den personliga integriteten minimeras. De har tillkommit bl.a. för att möta de krav som regeringsformen och Europakonventionen ställer i dessa avseenden. För till-

stånd till hemliga tvångsmedel krävs det normalt prövning i domstol. Vid domstolsprövningen av flertalet av de hemliga tvångsmedlen ska ett offentligt ombud kallas att närvara för att bevaka enskildas integritetsintressen. Det offentliga ombudet ska ha tillgång till allt material som ligger till grund för domstolens prövning och har rätt att överklaga domstolens beslut. I samband med permanentningen av de tidsbegränsade reglerna togs möjligheten för domstolen att fatta beslut om hemliga tvångsmedel, utan att ett offentligt ombud har medverkat, bort. Till rättssäkerhetsgarantierna räknas också skyldigheten att i efterhand underrätta vissa personer om att hemliga tvångsmedel har använts. Även den tillsyn och kontroll som Säkerhets- och integritetsskyddsnämnden utövar över de brottsbekämpande myndigheterna räknas hit. Nämnden har som övergripande mål att bidra till att värna rättssäkerheten och skyddet för den personliga integriteten inom den brottsbekämpande verksamheten. Tillsynen ska särskilt syfta till att säkerställa att verksamheten bedrivs i enlighet med lag eller annan författning. Nämnden är också på begäran av en enskild skyldig att kontrollera om han eller hon har utsatts för hemliga tvångsmedel och om hanteringen i så fall har varit lagenlig. Den enskilde underrättas om att kontrollen har utförts men kan p.g.a. sekretess som regel inte informeras närmare om vad som har funnits vid kontrollen.

Även regleringen av användningen av överskottsinformation har tillkommit mot bakgrund av regeringsformens och Europakonventionens krav. Vidare finns det av integritetshänsyn ett förbud mot avlyssning av vissa samtal eller meddelanden. Utgångspunkten för förbudet – som utvidgades i samband med permanentningen av de tidsbegränsade bestämmelserna – är att uppgifter som inte får inhämtas genom vittnesförhör i domstol inte heller ska kunna inhämtas genom avlyssning.

Tidigare översyner

Rättssäkerhetsgarantierna och mekanismerna till skydd för den personliga integriteten har setts över i olika sammanhang. Utredningen om rättssäkerhet vid hemliga tvångsmedel gjorde t.ex. bedömningen att systemet med offentliga ombud fungerade väl och att inga förändringar behövdes (SOU 2006:98). Några år senare

konstaterade Utredningen om utvärdering av vissa hemliga tvångsmedel att befintliga rättssäkerhetsgarantier och kontrollmekanismer utgör ett tillräckligt gott skydd mot otillbörliga intrång i den personliga integriteten (SOU 2009:70). Även Utredningen om vissa hemliga tvångsmedel gjorde en översyn i samband med att man tog ställning till de tre tidsbegränsade lagarnas fortsatta giltighet och hur den framtida regleringen av hemliga tvångsmedel för särskilt allvarlig eller annars samhällsfarlig brottslighet borde utformas. Enligt utredningen lever rättssäkerhetsgarantierna upp till regeringsformens och Europakonventionens krav (SOU 2012:44).

Rättssäkerhetsgarantierna och mekanismerna till skydd för den personliga integriteten bör ses över på nytt

Det är viktigt att rättssäkerhetsgarantierna och mekanismerna till skydd för den personliga integriteten fungerar. Den senaste översynen sträcker sig till utgången av 2011. Det finns när det gäller de bestämmelser om hemliga tvångsmedel för särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet, som permanentades den 1 januari 2015, skäl att nu följa upp tillämpningen av befintliga rättssäkerhetsgarantier och mekanismer till skydd för enskildas personliga integritet. Syftet är att säkerställa att de tillämpas på ett sådant sätt att systemet lever upp till de krav som Europakonventionen och regeringsformen ställer på rättssäkerhet och skydd för den personliga integriteten. Det är i detta sammanhang särskilt angeläget att bedöma effekterna avseende skyddet för enskildas personliga integritet med anledning av permanentningen (prop. 2014/15:1, uo 4, s. 23). Bland annat bör utredaren göra en analys av om det sedan permanentningen har uppstått något behov av att justera rättssäkerhetsgarantierna och mekanismerna till skydd för enskildas personliga integritet. Vid genomförandet av uppdraget ska beaktas vad som tidigare har uttalats om att en sådan ingående undersökning som gjordes inför permanentningen av de tidsbegränsade reglerna inte kan förväntas ske löpande (se prop. 2013/14:237, s. 168).

Utredaren ska

- undersöka hur rättssäkerhetsgarantierna och mekanismerna till skydd för den personliga integriteten vid användning av hemliga

tvångsmedel för särskilt allvarlig eller på annat sätt samhällsfarlig brottslighet har tillämpats från och med den 1 januari 2012,

- analysera om regelverket är förenligt med de krav regeringsformen och Europakonventionen ställer, och
- föreslå de författningsändringar och andra åtgärder som behövs om regleringen enligt utredarens bedömning inte skulle vara förenlig med kraven.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och konsekvenserna i övrigt av förslagen, inklusive förslagens betydelse för möjligheten att förebygga, förhindra, upptäcka, utreda och lagföra brott. Om förslagen kan antas försämra möjligheten i dessa avseenden ska detta belysas. Om förslagen kan förväntas medföra kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras.

Samråd och redovisning av uppdraget

Utredaren ska föra dialog med och inhämta upplysningar från Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Post- och telestyrelsen, Säkerhets- och integritetsskyddsnämnden samt andra myndig-heter i den utsträckning utredaren finner lämpligt. Utredaren ska också hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet och utredningsväsendet.

Uppdraget ska redovisas senast den 16 augusti 2018. Den del av uppdraget som ges med anledning av EU-domstolens förhandsavgörande om datalagring ska delredovisas senast den 9 oktober 2017.

(Justitiedepartementet)

Rättsfallssamlingen

DOMSTOLENS DOM (stora avdelningen)

den 21 december 2016*

”Begäran om förhandsavgörande — Elektronisk kommunikation — Behandling av personuppgifter — Konfidentialitet vid elektronisk kommunikation — Skydd — Direktiv 2002/58/EG — Artiklarna 5, 6, 9 och 15.1 — Europeiska unionens stadga om de grundläggande rättigheterna — Artiklarna 7, 8, 11 och 52.1 — Nationell lagstiftning — Leverantörer av elektroniska kommunikationstjänster — Skyldighet som avser en generell och odifferentierad lagring av trafikuppgifter och lokaliseringsuppgifter — Nationella myndigheter — Tillgång till uppgifter — Ingen förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet — Fråga om förenlighet med unionsrätten”

I de förenade målen C-203/15 och C-698/15,

angående beslut att begära förhandsavgörande enligt artikel 267 FEUF, från Kammarrätten i Stockholm (Sverige) och Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål, Förenade kungariket) av den 29 april 2015 respektive den 9 december 2015 som inkom till domstolen den 4 maj 2015 respektive den 28 december 2015, i målen

Tele2 Sverige AB (C-203/15)

mot

Post- och telestyrelsen,

och

Secretary of State for the Home Department (C-698/15)

mot

Tom Watson,

Peter Brice,

Geoffrey Lewis,

ytterligare deltagare i rättegången:

Open Rights Group,

Privacy International,

The Law Society of England and Wales,

* Rättegångsspråk: svenska och engelska.

meddelar

DOMSTOLEN (stora avdelningen)

sammansatt av ordföranden K. Lenaerts, vice ordföranden A. Tizzano, avdelningsordförandena R. Silva de Lapuerta, T. von Danwitz (referent), J.L. da Cruz Vilaça, E. Juhász och M. Vilaras samt domarna A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen och C. Lycourgos,

generaladvokat: H. Saugmandsgaard Øe,

justitiesekreterare: handläggaren C. Strömholm,

med hänsyn till beslutet av domstolens ordförande av den 1 februari 2016 att handlägga mål C-698/15 skyndsamt i enlighet med artikel 105.1 i domstolens rättegångsregler,

efter det skriftliga förfarandet och förhandlingen den 12 april 2016,

med beaktande av de yttranden som avgetts av:

— Tele2 Sverige AB, genom M. Johansson och N. Torgerzon, advokater, samt E. Lagerlöf och S. Backman,

— Tom Watson, genom J. Welch och E. Norton, solicitors, I. Steele, advocate, B. Jaffey, barrister, samt D. Rose, QC,

— Peter Brice och Geoffrey Lewis, genom A. Suterwalla och R. de Mello, barristers, R. Drabble, QC, samt S. Luke, solicitor,

— Open Rights Group och Privacy International, genom D. Carey, solicitor, samt R. Mehta och J. Simor, barristers,

— The Law Society of England and Wales, genom T. Hickman, barrister, samt N. Turner,

— Sveriges regering, genom A. Falk, C. Meyer-Seitz, U. Persson, N. Otte Widgren och L. Swedenborg, samtliga i egenskap av ombud,

— Förenade kungarikets regering, genom S. Brandon, L. Christie och V. Kaye, samtliga i egenskap av ombud, biträdda av D. Beard, G. Facenna och J. Eadie, QC, samt S. Ford, barrister,

— Belgiens regering, genom J.-C. Halleux, S. Vanrie och C. Pochet, samtliga i egenskap av ombud,

— Tjeckiens regering, genom M. Smolek och J. Vláčíl, båda i egenskap av ombud,

— Danmarks regering, genom C. Thorning och M. Wolff, båda i egenskap av ombud,

— Tysklands regering, genom T. Henze, M. Hellmann och J. Kemper, samtliga i egenskap av ombud, biträdda av M. Kottmann och U. Karpenstein, Rechtsanwälte,

— Estlands regering, genom K. Kraavi-Käerdi, i egenskap av ombud,

— Irland, genom E. Creedon, L. Williams och A. Joyce, samtliga i egenskap av ombud, biträdda av D. Fennelly, BL,

— Spaniens regering, genom A. Rubio González, i egenskap av ombud,

— Frankrikes regering, genom G. de Bergues, D. Colas, F.-X. Bréchot och C. David, samtliga i egenskap av ombud,

— Cyperns regering, genom K. Kleanthous, i egenskap av ombud,

— Ungerns regering, genom M. Fehér och G. Koós, båda i egenskap av ombud,

— Nederländernas regering, genom M. Bulterman, M. Gijzen och J. Langer, samtliga i egenskap av ombud,

— Polens regering, genom B. Majczyna, i egenskap av ombud,

— Finlands regering, genom J. Heliskoski, i egenskap av ombud,

— Europeiska kommissionen, genom H. Krämer, K. Simonsson, H. Kranenborg, D. Nardi, P. Costa de Oliveira och J. Vondung, samtliga i egenskap av ombud,

och efter att den 19 juli 2016 ha hört generaladvokatens förslag till avgörande,

följande

Dom

1 Respektive begäran om förhandsavgörande avser tolkningen av artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 2002, s. 37), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 (EUT L 337, 2009, s. 11) (nedan kallat direktiv 2002/58), jämförd med artiklarna 7, 8 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan).

2 Den ena begäran har framställts i ett mål (C-203/15) mellan Tele2 Sverige AB och Post- och telestyrelsen (nedan kallad PTS), om ett föreläggande från PTS för Tele2 Sverige att lagra trafikuppgifter och lokaliseringsuppgifter avseende bolagets abonnenter och registrerade användare. Den andra begäran har framställts i ett mål (C-698/15) mellan Tom Watson, Peter Brice och Geoffrey Lewis, å ena sidan, och Secretary of State for the Home Department (inrikesministern i Förenade konungariket Storbritannien och Nordirland), å andra sidan, om huruvida section 1 i Data Retention and Investigatory Powers Act 2014 (2014 års lag om datalagring och utredningsbefogenheter, nedan kallad Dripa) är förenlig med unionsrätten.

Tillämpliga bestämmelser

Unionsrätt

Direktiv 2002/58

3 I skälen 2, 6, 7, 11, 21, 22, 26 och 30 i direktiv 2002/58 anges följande:

”(2) I detta direktiv eftersträvas respekt för de grundläggande rättigheterna och iakttagande av de principer som erkänns i synnerhet i [stadgan]. I synnerhet eftersträvas i detta direktiv att säkerställa full respekt för rättigheterna i artiklarna 7 och 8 i … stadgan.

…

(6) Internet bryter upp traditionella marknadsstrukturer genom att tillhandahålla en gemensam, global infrastruktur för leverans av en mängd olika elektroniska kommunikationstjänster. Allmänt tillgängliga kommunikationstjänster via Internet öppnar nya möjligheter för användarna, men för även med sig nya risker för deras personuppgifter och integritet.

(7) När det gäller allmänna kommunikationsnät bör särskilda rättsliga och tekniska bestämmelser antas för att skydda fysiska personers grundläggande fri- och rättigheter samt juridiska personers berättigade intressen, särskilt med hänsyn till den ökade kapaciteten för automatisk lagring och behandling av uppgifter om abonnenter och användare.

…

(11) I likhet med [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 (EGT L 281, 1995, s. 31)] omfattar det här direktivet inte sådana frågor om skydd av grundläggande fri- och rättigheter som rör verksamhet som inte regleras av gemenskapslagstiftningen. Det ändrar därför inte den befintliga jämvikten mellan den enskildes rätt till integritet och medlemsstaternas möjligheter att vidta sådana åtgärder, enligt artikel 15.1 i det här direktivet, som krävs för att skydda allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och brottsbekämpning. Det här direktivet påverkar följaktligen inte medlemsstaternas möjlighet att utföra laglig avlyssning av elektronisk kommunikation eller att vidta andra åtgärder om det är nödvändigt för något av dessa ändamål och sker i enlighet med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna i den tolkning dessa fått i rättspraxis från Europeiska domstolen för de mänskliga rättigheterna. Sådana åtgärder måste vara lämpliga, i strikt proportion till det avsedda ändamålet och nödvändiga i ett demokratiskt samhälle. De bör omfattas av lämpliga skyddsmekanismer i överensstämmelse med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.

…

(21) Åtgärder bör vidtas för att förhindra obehörig åtkomst av kommunikation, så att konfidentialiteten vid kommunikation via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster skyddas såväl i fråga om innehåll som uppgifter som har samband med sådan kommunikation. Den nationella lagstiftningen i vissa medlemsstater förbjuder endast obehörig åtkomst av kommunikation om detta sker avsiktligen.

(22) Förbudet mot lagring av kommunikationer och tillhörande trafikuppgifter av andra än användarna eller utan deras samtycke är inte avsett att förbjuda någon automatisk, mellanliggande och tillfällig lagring av denna information, i den mån lagringen enbart görs för att utföra överföringen i det elektroniska kommunikationsnätet och under förutsättning att informationen inte lagras längre än vad som är nödvändigt för överföringen och trafikstyrningen och att konfidentialiteten förblir garanterad under lagringsperioden. …

…

(26) De uppgifter om abonnenter som behandlas inom elektroniska kommunikationsnät i samband med uppkoppling och överföring av information innehåller upplysningar om fysiska personers privatliv och gäller rätten till skydd för deras korrespondens eller omsorgen om juridiska personers berättigade intressen. Sådana uppgifter får endast lagras i den utsträckning det är nödvändigt för att tillhandahålla tjänsten när det gäller fakturering och betalning av samtrafikavgifter, och endast under en begränsad tid. [Ytterligare behandling av sådana uppgifter får] endast ske om abonnenten givit sitt samtycke till detta efter att ha erhållit korrekt och uttömmande information av den berörda leverantören om vilka typer av ytterligare behandling som denne avser att företa och om abonnentens rätt att inte ge sitt samtycke eller att återkalla sitt samtycke till en sådan behandling. …

…

(30) Systemen för tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster bör utformas så att mängden nödvändiga personuppgifter begränsas till ett absolut minimum. …”

4 I artikel 1 i direktiv 2002/58, med rubriken ”Tillämpningsområde och syfte”, föreskrivs följande:

”1. Genom detta direktiv möjliggörs en harmonisering av nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, samt för att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom gemenskapen.

2. Bestämmelserna i detta direktiv skall precisera och komplettera direktiv [95/46] för de ändamål som avses i punkt 1. Bestämmelserna är vidare avsedda att skydda berättigade intressen för de abonnenter som är juridiska personer.

3. Detta direktiv skall inte tillämpas på verksamheter som faller utanför tillämpningsområdet för Fördraget om upprättandet av Europeiska gemenskapen, t.ex. de som omfattas av avdelningarna V och VI i Fördraget om Europeiska unionen, och inte i något fall på verksamheter som avser allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och statens verksamhet på straffrättens område.”

5 I artikel 2 i direktiv 2002/58, som har rubriken ”Definitioner”, anges följande:

”Om inte annat anges skall definitionerna i Europaparlamentets och rådets direktiv 95/46/EG och 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) [(EGT L 108, 2002, s. 33)] gälla i detta direktiv.

Dessutom skall följande definitioner gälla:

…

b) *trafikuppgifter*: alla uppgifter som behandlas i syfte att överföra en kommunikation via ett elektroniskt kommunikationsnät eller för att fakturera den.

c) *lokaliseringsuppgifter*: alla uppgifter som behandlas i ett elektroniskt kommunikationsnät eller av en elektronisk kommunikationstjänst och som visar den geografiska positionen för terminalutrustningen för en användare av en allmänt tillgänglig elektronisk kommunikationstjänst."

d) *kommunikation*: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst. Detta inbegriper inte information som överförs som del av en sändningstjänst för rundradio eller TV till allmänheten via ett elektroniskt kommunikationsnät utom i den mån informationen kan sättas i samband med den enskilde abonnenten eller användaren av informationen.

…"

6 I artikel 3 i direktiv 2002/58, med rubriken "Berörda tjänster", föreskrivs följande:

"Detta direktiv ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom gemenskapen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning."

7 Artikel 4 i detta direktiv, med rubriken "Säkerhet i samband med behandlingen av uppgifter", har följande lydelse:

"1. Leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst skall 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 skall säkerställa en säkerhetsnivå som är anpassad till den risk som föreligger, med beaktande av dagens tillgängliga teknik och kostnaderna för att genomföra åtgärderna.

1a. Utan att det påverkar tillämpningen av direktiv 95/46/EG ska de åtgärder som avses i punkt 1 minst

— säkerställa att endast auktoriserad personal, och endast i lagligen tillåtna syften, får tillgång till personuppgifter,

— skydda personuppgifter som lagrats eller överförts mot oavsiktlig eller olaglig förstörelse, oavsiktlig förlust eller ändring samt mot icke auktoriserad eller olaglig lagring och behandling eller icke auktoriserat eller olagligt tillträde eller offentliggörande, och

— säkerställa införandet av en säkerhetsstrategi för behandling av personuppgifter.

…"

8 I artikel 5 i direktiv 2002/58, som har rubriken "Konfidentialitet vid kommunikation", anges följande:

"1. Medlemsstaterna skall genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. De skall särskilt förbjuda avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller 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 artikel 15.1. Denna punkt får inte förhindra teknisk lagring som är nödvändig för överföring av kommunikationen utan att det påverkar principen om konfidentialitet.

…

3. Medlemsstaterna ska se till att lagring av information eller tillgång till information som redan är lagrad i en abonnents eller användares terminalutrustning endast är tillåten på villkor att abonnenten eller användaren i fråga har gett sitt samtycke efter att ha fått tillgång till tydlig och fullständig information, i enlighet med direktiv [95/46/], bland annat om ändamålen med behandlingen av uppgifterna. Detta får inte förhindra någon teknisk lagring eller åtkomst som endast sker för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller det som är absolut nödvändigt för att leverantören ska kunna tillhandahålla en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt.”

9 I artikel 6 i direktiv 2002/58, med rubriken ”Trafikuppgifter”, anges följande:

”1. Trafikuppgifter om abonnenter och användare som behandlas och lagras av leverantören av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst skall utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra en kommunikation, utan att det påverkar tillämpningen av punkterna 2, 3 och 5 i den här artikeln samt artikel 15.1.

2. Trafikuppgifter som krävs för abonnentfakturering och betalning av samtrafikavgifter får behandlas. Sådan behandling är tillåten endast fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning.

3. I syfte att saluföra elektroniska kommunikationstjänster eller i syfte att tillhandahålla mervärdestjänster får en leverantör av en allmänt tillgänglig elektronisk kommunikationstjänst behandla de uppgifter som avses i punkt 1 i den utsträckning och under den tidsperiod som är nödvändig för sådana tjänster eller sådan marknadsföring, om den abonnent eller användare som uppgifterna gäller i förväg har samtyckt till detta. Användare eller abonnenter skall ha möjlighet att när som helst dra tillbaka sitt samtycke till behandling av trafikuppgifter.

…

5. Behandlingen av trafikuppgifter skall, i enlighet med punkterna 1, 2, 3 och 4, begränsas till sådana personer som av leverantören av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster getts i uppdrag att sköta fakturering, trafikstyrning, kundförfrågningar, spårning av bedrägerier, marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av en mervärdestjänst, och behandlingen skall begränsas till sådant som är nödvändigt för dessa verksamheter.”

10 Artikel 9 i direktivet har rubriken ”Andra lokaliseringsuppgifter än trafikuppgifter”. Artikel 9.1 stadgar följande:

”Om andra lokaliseringsuppgifter än trafikuppgifter som rör användare eller abonnenter av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster kan behandlas, får dessa uppgifter endast behandlas sedan de har avidentifierats eller om användarna eller abonnenterna givit sitt samtycke, i den utsträckning och för den tid som krävs för tillhandahållandet av en mervärdestjänst. Innan användaren eller abonnenten ger sitt samtycke skall tjänsteleverantören informera denne om vilken typ av andra lokaliseringsuppgifter än trafikuppgifter som kommer att behandlas, behandlingens syfte och varaktighet samt om uppgifterna kommer att vidarebefordras till tredje part för tillhandahållande av mervärdestjänsten. …”

11 Artikel 15 i direktivet, med rubriken ”Tillämpningen av vissa bestämmelser i direktiv [95/46]”, har följande lydelse:

”1. Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv [95/46]. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i denna punkt. Alla åtgärder som avses i denna punkt skall vara i enlighet med de allmänna principerna i gemenskapslagstiftningen, inklusive principerna i artikel 6.1 och 6.2 i Fördraget om Europeiska unionen.

…

1b. Leverantörerna ska införa interna förfaranden för att besvara förfrågningar om tillgång till användarnas personuppgifter, på grundval av nationella bestämmelser som antagits i enlighet med punkt 1. De ska på begäran förse den behöriga nationella myndigheten med information om dessa förfaranden, antalet förfrågningar som mottagits, vilken juridisk motivering som framförts och vilket svar leverantören lämnat.

2. Bestämmelserna om rättslig prövning, ansvar och sanktioner i kapitel III i direktiv [95/46] skall gälla för de nationella bestämmelser som antas i enlighet med det här direktivet och för de individuella rättigheter som kan härledas från det här direktivet.

…”

Direktiv 95/46

12 Artikel 22 i direktiv 95/46, som ingår i direktivets kapitel III, har följande lydelse:

”Medlemsstaterna skall – utan att det påverkar möjligheten att utnyttja något administrativt förfarande, till exempel vid den tillsynsmyndighet som avses i artikel 28, som kan användas innan ett ärende anhängiggörs hos en rättslig instans – föreskriva att var och en har rätt att föra talan inför domstol om sådana kränkningar av rättigheter som skyddas av den nationella lagstiftning som är tillämplig på ifrågavarande behandling.”

Direktiv 2006/24/EG

13 Artikel 1 i Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 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 (EUT L 105, 2006, s. 54), med rubriken ”Syfte och tillämpningsområde”, föreskrev följande i punkt 2:

”Detta direktiv skall gälla trafik- och lokaliseringsuppgifter om såväl fysiska som juridiska personer och enheter, samt de uppgifter som är nödvändiga för att kunna identifiera abonnenten eller den registrerade användaren. Det skall inte vara tillämpligt på innehållet i elektronisk kommunikation, inklusive sådan information som användaren sökt med hjälp av ett elektroniskt kommunikationsnät.”

14 Artikel 3 i direktivet, med rubriken ”Skyldighet att lagra uppgifter”, hade följande lydelse:

”1. Genom avvikelse från artiklarna 5, 6 och 9 i direktiv [2002/58] skall medlemsstaterna anta åtgärder för att säkerställa lagring enligt bestämmelserna i det här direktivet av de uppgifter som specificeras i artikel 5 i detta, i den utsträckning som de genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät inom statens territorium i samband med att leverantörerna levererar de kommunikationstjänster som berörs.

2. Den lagringsskyldighet som anges i punkt 1 skall inbegripa lagring av sådana uppgifter som anges i artikel 5 rörande misslyckade uppringningsförsök där uppgifter genereras eller behandlas, och lagras (uppgifter rörande telefoni) eller loggas (uppgifter rörande Internet) av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät inom den berörda medlemsstatens jurisdiktion i samband med att de levererar de berörda kommunikationstjänsterna. Detta direktiv skall inte innebära krav på lagring av uppgifter rörande samtal som inte kopplats fram.”

Svensk rätt

15 Det framgår av begäran om förhandsavgörande i mål C-203/15 att den svenska lagstiftaren, i syfte att införliva direktiv 2006/24 med nationell rätt, ändrade lagen (2003:389) om elektronisk kommunikation (nedan kallad LEK) och förordningen (2003:396) om elektronisk kommunikation. Båda dessa författningar, i deras tillämpliga lydelse i det nationella målet, innehåller bestämmelser om lagring av uppgifter om elektronisk kommunikation och om de nationella myndigheternas tillgång till dessa uppgifter.

16 Tillgång till uppgifterna regleras även i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (nedan kallad inhämtningslagen) och i rättegångsbalken (nedan kallad RB).

Skyldigheten att lagra uppgifter om elektronisk kommunikation

17 Enligt vad Kammarrätten i Stockholm (nedan kallad Kammarrätten) har uppgett föreskriver 6 kap. 16 a § jämförd med 2 kap. 1 § LEK att leverantörer av elektroniska kommunikationstjänster är skyldiga att lagra sådana uppgifter som skulle lagras enligt direktiv 2006/24. Det gäller sådana uppgifter om abonnemang och om all elektronisk kommunikation som är nödvändiga för att finna och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typen av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut. Skyldigheten att lagra uppgifterna omfattar uppgifter som genereras eller behandlas vid telefonitjänst, telefonitjänst via mobil anslutningspunkt, meddelandehantering, internetåtkomst och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform). Denna skyldighet innefattar även uppgifter om misslyckad uppringning. Den gäller dock inte kommunikationens innehåll.

18 I 38–43 §§ i förordningen (2003:396) om elektronisk kommunikation preciseras vilka kategorier av uppgifter som ska lagras. Beträffande telefonitjänster ska bland annat uppringande och uppringt nummer samt datum och spårbar tid då kommunikationen påbörjades och avslutades lagras. När det gäller telefonitjänster via mobil anslutningspunkt framgår att ytterligare krav gäller, till exempel att även lokaliseringsuppgifter för kommunikationens början och slut ska lagras. När det gäller telefonitjänster som använder IP-paket ska utöver vad som anges ovan bland annat även den uppringandes och den uppringdes IP-adresser lagras. När det gäller meddelandehantering ska bland annat avsändares och mottagares nummer, IP-adress eller annan meddelandeadress lagras. När det gäller internetåtkomst ska exempelvis användares IP-adress samt datum och spårbar tid för på- och avloggning i den tjänst som ger internetåtkomst lagras.

Lagringstid för uppgifterna

19 Av 6 kap. 16 d § LEK framgår att leverantörer av elektroniska kommunikationstjänster ska lagra sådana uppgifter som avses i 6 kap. 16 a § LEK i sex månader räknat från den dag kommunikationen avslutades. Därefter ska uppgifterna genast utplånas, om inte annat följer av 6 kap. 16 d § andra stycket LEK.

Tillgång till lagrade uppgifter

20 Tillgång till uppgifter som har lagrats av nationella myndigheter regleras i bestämmelser i inhämtningslagen, LEK och RB.

– Inhämtningslagen

21 Polismyndigheten, Säkerhetspolisen och Tullverket får med stöd av 1 § inhämtningslagen, under de förutsättningar som anges i denna lag, i underrättelseverksamhet i hemlighet från den som enligt LEK tillhandahåller ett elektroniskt kommunikationsnät eller elektroniska kommunikationstjänster hämta in uppgifter om meddelanden som har överförts i ett elektroniskt kommunikationsnät, vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område, eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

22 Uppgifterna får enligt 2 och 3 §§ inhämtningslagen 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, eller sådana brott som omfattas av uppräkningen i 3 §, vilket inkluderar brott för vilka lindrigare straff än fängelse i två år kan utdömas. Skälen för åtgärden ska uppväga det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse. Enligt 5 § inhämtningslagen får den tid som åtgärden avser inte överstiga en månad.

23 Beslut om en sådan åtgärd fattas av myndighetschefen eller en annan anställd vid myndigheten som myndighetschefen delegerar beslutanderätten till. Beslutet är inte underkastat förhandskontroll av en domstol eller oberoende förvaltningsmyndighet.

24 Säkerhets- och integritetsskyddsnämnden ska enligt 6 § inhämtningslagen underrättas om ett beslut om inhämtning av uppgifter. Enligt 1 § lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet ska Säkerhets- och integritetsskyddsnämnden utöva tillsyn över brottsbekämpande myndigheters tillämpning av lagen.

– LEK

25 Av 6 kap. 22 § första stycket 2 LEK framgår att en leverantör av elektroniska kommunikationstjänster på begäran ska lämna ut abonnemangsuppgifter till åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brott, om uppgifterna gäller misstanke om brott. Enligt de upplysningar som Kammarrätten har lämnat krävs det inte att det är fråga om ett allvarligt brott.

– RB

26 RB reglerar kommunikation av uppgifter som lagrats av nationella myndigheter inom ramen för förundersökningar. Enligt 27 kap. 19 § RB får hemlig ”övervakning av elektronisk kommunikation” i princip användas vid en förundersökning om bland annat brott för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader. ”Övervakning av elektronisk kommunikation” innebär

enligt 27 kap. 19 § RB att uppgifter i hemlighet hämtas in om meddelanden som överförs eller har överförts i ett elektroniskt kommunikationsnät, om vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits.

27 Enligt de upplysningar som Kammarrätten har lämnat i mål C-203/15, kan uppgifter om innehållet i meddelanden inte inhämtas med stöd av 27 kap. 19 § RB. Av 27 kap. 20 § RB framgår att hemlig övervakning av elektronisk kommunikation som huvudregel endast får ske om någon är skäligen misstänkt för brottet och åtgärden är av synnerlig vikt för utredningen. Utredningen ska avse brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år eller försök, förberedelse eller stämpling till sådant brott, om en sådan gärning är belagd med straff. Enligt 27 kap. 21 § RB måste åklagaren, utom i brådskande fall, först inhämta rättens tillstånd till hemlig övervakning av elektronisk kommunikation.

Säkerhet och skydd för lagrade uppgifter

28 Av 6 kap. 3 a § LEK framgår att leverantörer av elektroniska kommunikationstjänster som är skyldiga att lagra uppgifter ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. Enligt de upplysningar som Kammarrätten har lämnat saknas emellertid i svensk rätt bestämmelser om var lagring av uppgifterna får ske.

Lagstiftningen i Förenade kungariket

Dripa

29 Section 1 i Dripa, med rubriken ”Befogenheter vad gäller lagring av uppgifter om kommunikation som omfattas av säkerhetsåtgärder”, stadgar följande:

”(1) Inrikesministern får genom beslut (nedan kallat föreläggande om lagring) förelägga en offentlig teleoperatör att lagra relevanta uppgifter om kommunikation om denne finner att detta är nödvändigt och proportionerligt mot bakgrund av ett eller flera av de syften som avses i punkterna a–h i section 22(2) i Regulation of Investigatory Powers Act 2000 (2000 års lag om utredningsbefogenheter) (syften för vilka uppgifter får inhämtas).

(2) Ett föreläggande om lagring får

(a) riktas mot en viss operatör eller en viss kategori av operatörer,

(b) avse samtliga uppgifter eller vissa kategorier av uppgifter,

(c) avse en specifikt angiven period under vilken uppgifter ska lagras,

(d) innehålla andra krav eller begränsningar avseende lagringen av uppgifter,

(e) innehålla olika föreskrifter för olika syften,

(f) avse uppgifter oberoende av huruvida de existerar när föreläggandet utfärdas eller träder i kraft.

(3) Inrikesministern får i förordning utfärda ytterligare föreskrifter om lagring av relevanta uppgifter om kommunikation.

(4) Sådana föreskrifter kan särskilt avse

(a) villkor som ska vara uppfyllda innan ett föreläggande om lagring får utfärdas,

(b) den längsta tid under vilken uppgifter ska lagras enligt ett föreläggande om lagring,

(c) innehållet i ett föreläggande om lagring samt utfärdande, ikraftträdande, omprövning, ändring eller återkallande av ett sådant föreläggande,

(d) integriteten hos, säkerheten för eller skydd av uppgifter som lagrats med stöd av förevarande section samt tillgång till, utlämnande eller utplånande av sådana uppgifter,

(e) genomförandet av relevanta krav eller begränsningar, eller kontrollen av detta genomförande,

(f) riktlinjer rörande relevanta krav, begränsningar eller befogenheter,

(g) återbetalning från inrikesministern (eventuellt underkastad villkor) av utgifter som offentliga teleoperatörer haft för att följa relevanta krav eller begränsningar, eller

(h) den omständigheten att [Data Retention (EC Directive) Regulations 2009 (2009 års förordning om datalagring (EG-direktiv))] upphör att gälla, samt övergången till lagring av uppgifter enligt förevarande section.

(5) Den längsta lagringstid som fastställs enligt punkt 4 b får inte överskrida 12 månader från och med den dag som anges i fråga om sådana uppgifter som avses med bestämmelserna i punkt 3.

…”

30 Section 2 i Dripa definierar begreppet ”relevanta uppgifter om kommunikation” som ”relevanta uppgifter om sådan kommunikation som avses i bilagan till 2009 års förordning om datalagring (EG-direktiv) i den utsträckning dessa uppgifter har genererats eller behandlats i Förenade kungariket av offentliga teleoperatörer i samband med tillhandahållandet av de berörda telekommunikationstjänsterna”.

Ripa

31 Section 21 i Regulation of Investigatory Powers Act 2000 (2000 års lag om utredningsbefogenheter, nedan kallad Ripa) ingår i kapitel II i den lagen och har rubriken ”Inhämtning och utlämnande av uppgifter om kommunikation”. Section 21.4 har följande lydelse:

”I detta kapitel avses med ’uppgifter om kommunikation’ något av följande:

(a) alla trafikuppgifter som ingår i eller bifogats en kommunikation (av avsändaren eller annan) i fråga om varje system för posttjänster eller telekommunikation genom vilket uppgifter överförs eller kan överföras,

(b) all information som inte innefattar något innehåll i en kommunikation (förutom information som avses i punkt a och som rör en persons användande av

(i) en post- eller telekommunikationstjänst, eller

(ii) någon del av ett telekommunikationssystem i samband med tillhandahållande till en person eller en persons användande av en telekommunikationstjänst,

(c) all information som inte omfattas av punkt a eller b som, i förhållande till tjänstemottagarna, innehas eller erhålls av en person som tillhandahåller en post- eller telekommunikationstjänst."

32 Enligt upplysningarna i begäran om förhandsavgörande i mål C-698/15 omfattar dessa uppgifter lokaliseringsuppgifterna för en användare men däremot inte innehållet i en kommunikation.

33 Vad gäller tillgång till lagrade uppgifter föreskriver section 22 i Ripa följande:

"(1) Denna section gäller när en ansvarig person enligt detta kapitel finner det nödvändigt, av skäl som omfattas av punkt 2 i denna section, att inhämta uppgifter om kommunikation.

(2) Det är nödvändigt att inhämta uppgifter om kommunikation av skäl som omfattas av denna punkt, om de är nödvändiga med hänsyn till

(a) skyddet av nationell säkerhet,

(b) förebyggande och upptäckande av brott eller förebyggande av störningar av den allmänna ordningen,

(c) Förenade kungarikets ekonomiska välstånd,

(d) skyddet av allmän säkerhet,

(e) skyddet av folkhälsan,

(f) fastställande och uppbörd av skatter och andra avgifter till offentliga myndigheter,

(g) förebyggande, i en nödsituation, av fara för liv eller skada på en persons fysiska eller psykiska hälsa eller lindring av skada på en persons fysiska eller psykiska hälsa, eller

(h) varje annat syfte (utöver vad som anges i punkterna a–g) som inrikesministern fastställer i föreskrifter.

(4) Om inte annat följer av punkt 5 kan den ansvariga personen, när denne bedömer att en teleoperatör eller postoperatör innehar, skulle kunna inneha eller skulle kunna ha kapacitet att inneha uppgifter, framställa en begäran till operatören om att denne

(a) ska inhämta uppgifterna, om denne inte redan innehar dem, och

(b) i alla händelser ska utlämna alla uppgifter som denne innehar eller som denne sedermera har inhämtat.

(5) Den ansvariga personen får endast ge tillstånd enligt punkt 3 eller framställa en begäran enligt punkt 4 om denne anser att inhämtning av uppgifterna i fråga genom ett handlande som är godkänt eller som fordras enligt ett tillstånd eller en begäran är proportionerlig mot det mål som eftersträvas med inhämtning av uppgifterna."

34 Enligt section 65 i Ripa kan klagomål ges in till Investigatory Powers Tribunal (domstol för utredningsbefogenheter, Förenade kungariket) om det finns misstanke om att uppgifter har inhämtats på felaktiga grunder.

Data Retention Regulations 2014

35 Data Retention Regulations 2014 (2014 års förordning om datalagring), som antagits med stöd av Dripa, är indelad i tre delar. Den andra delen omfattar sections 2–14 i förordningen. Section 4, med rubriken ”Föreläggande om lagring”, föreskriver följande:

”(1) Ett föreläggande om lagring ska ange

(a) den offentliga teleoperatör (eller en beskrivning av de operatörer) som föreläggandet är riktat till,

(b) de relevanta uppgifter om kommunikation som ska lagras,

(c) den period eller de perioder under vilken eller vilka uppgifterna ska lagras, och

(d) övriga krav eller begränsningar avseende lagringen av uppgifter.

(2) Ett föreläggande om lagring kan inte fordra att en uppgift lagras i mer än 12 månader, räknat från

(a) dagen för den berörda kommunikationen, när det gäller trafikuppgifter eller uppgifter om användningen av tjänsten, och

(b) den dag då den berörda personen avslutar kommunikationstjänsten i fråga, alternativt den dag då uppgiften ändras (om detta inträffar dessförinnan), när det gäller abonnentuppgifter.

…”

36 Enligt section 7 i förordningen, med rubriken ”Uppgifternas integritet och säkerhet”, gäller följande:

”(1) En offentlig teleoperatör som lagrar uppgifter i enlighet med section 1 i [Dripa] ska

(a) säkerställa att de lagrade uppgifterna har samma integritet och ges samma säkerhet och skydd som uppgifterna i de system de härrör från,

(b) säkerställa, genom lämpliga tekniska och organisatoriska åtgärder, att endast personal med särskilt tillstånd kan få tillgång till uppgifterna, och

(c) genom lämpliga tekniska och organisatoriska åtgärder, skydda uppgifterna mot olaglig förstöring och oavsiktlig förlust eller ändring och mot otillåten eller olaglig lagring av, behandling av, tillgång till eller avslöjande av uppgifterna.

(2) En offentlig teleoperatör som lagrar uppgifter om kommunikation i enlighet med section 1 i [Dripa] måste förstöra uppgifterna om lagringen inte längre är tillåten enligt den bestämmelsen och inte heller i övrigt är tillåten enligt lag.

(3) Kravet i punkt 2 att förstöra uppgifter innebär att uppgifterna ska raderas på ett sådant sätt att det är omöjligt att få tillgång till dessa uppgifter.

(4) Det räcker för operatören att vidta åtgärder för att radera uppgifter månatligen eller med kortare mellanrum alltefter operatörens praktiska möjligheter.”

37 Section 8 i förordningen har rubriken ”Utlämnande av lagrade uppgifter” och föreskriver följande:

”(1) En offentlig teleoperatör ska inrätta lämpliga säkerhetssystem (inbegripet tekniska och organisatoriska åtgärder) för att bestämma tillgången till uppgifter om kommunikation som lagrats i enlighet med section 1 i [Dripa] för att förhindra att uppgifter lämnas ut om så inte föreskrivs i section 1.6 a i [Dripa].

(2) En offentlig teleoperatör som lagrar uppgifter i enlighet med section 1 i [Dripa] ska lagra uppgifterna på ett sådant sätt att operatören utan oskäligt dröjsmål kan föra över dem på begäran.”

38 I section 9 i samma förordning, under rubriken ”Datainspektionens tillsyn”, anges följande:

”Datainspektionen (*Information Commissioner*) ska tillse att de krav eller begränsningar som föreskrivs i denna del iakttas, rörande integriteten hos och säkerheten för samt förstörelse av lagrade uppgifter enligt section 1 i [Dripa].”

Riktlinjerna

39 Acquisition and Disclosure of Communications Data Code of Practice (riktlinjer för inhämtning och utlämnande av uppgifter om kommunikation, nedan kallade riktlinjerna) innehåller, i punkterna 2.5–2.9 och 2.36–2.45, hållpunkter rörande nödvändighet och proportionalitet vid inhämtning av uppgifter om kommunikation. Enligt de upplysningar som den hänskjutande domstolen i mål C-698/15 har lämnat, ska enligt punkterna 3.72–3.77 i riktlinjerna särskild vikt läggas vid kriterierna rörande nödvändighet och proportionalitet när de eftersökta uppgifterna avser en person som tillhör en yrkeskår som handhar information som erhållits under tystnadsplikt eller annan konfidentiell information.

40 För att inhämta uppgifter om kommunikation i syfte att identifiera en journalists källa krävs enligt punkterna 3.78–3.84 i riktlinjerna beslut av domstol. Enligt punkterna 3.85–3.87 i riktlinjerna krävs tillstånd av domstol i fråga om en ansökan om tillgång till uppgifter som inges av lokala myndigheter. Däremot finns det inte något krav på tillstånd från en domstol eller ett oberoende organ för tillgång till uppgifter om kommunikation som omfattas av advokatsekretess eller som rör läkare, parlamentsledamöter eller präster.

41 Enligt punkt 7.1 i riktlinjerna måste uppgifter om kommunikation som har inhämtats eller erhållits med stöd av Ripa samt alla kopior, utdrag och sammanfattningar av uppgifterna hanteras och förvaras på ett säkert sätt. Vidare måste kraven i Data Protection Act (dataskyddslagen) iakttas.

42 När en myndighet i Förenade kungariket överväger att lämna ut uppgifter om kommunikation till utländska myndigheter, ska den enligt punkt 7.18 i riktlinjerna bland annat pröva om uppgifterna kommer att få tillräckligt skydd. Det framgår dock av punkt 7.22 i riktlinjerna att uppgifter får föras över till ett tredjeland om det behövs med hänsyn till ett viktigt allmänt intresse, även när tredjelandet inte garanterar en lämplig skyddsnivå. Enligt de upplysningar som den hänskjutande domstolen i mål C-698/15 har lämnat, får inrikesministern utfärda ett nationellt säkerhetscertifikat som undantar vissa uppgifter från lagstiftningens krav.

43 I punkt 8.1 i riktlinjerna erinras om att det genom Ripa inrättats en tillsynsmyndighet för avlyssning av kommunikation (*Interception of Communications Commissioner*) i Förenade kungariket, som ska utöva oberoende tillsyn över utövandet och genomförandet av befogenheter och skyldigheter enligt kapitel II i del I i Ripa. Som framgår av punkt 8.3 i riktlinjerna, får den myndigheten underrätta en person om en misstänkt felaktig användning av befogenheter om myndigheten kan ”styrka att en enskild har lidit skada till följd av ett uppsåtligt eller grovt oaktsamt åsidosättande”.

Målen vid de nationella domstolarna och tolkningsfrågorna

Mål C-203/15

44 Den 9 april 2014 underrättade Tele2 Sverige – en leverantör av elektroniska kommunikationstjänster etablerad i Sverige – PTS om att bolaget, efter att direktiv 2006/24 förklarats ogiltigt genom dom av den 8 april 2014, Digital Rights Ireland m.fl. (C-293/12 och C-594/12, nedan kallad Digital Rights-domen, EU:C:2014:238), från den 14 april 2014 avsåg att upphöra med att lagra uppgifter om elektronisk kommunikation i enlighet med LEK samt radera de uppgifter som lagrats fram till den tidpunkten.

45 Den 15 april 2014 inkom Rikspolisstyrelsen med en anmälan till PTS av vilken det framgick att Tele2 Sverige hade upphört med leveranser av dessa uppgifter till polisen.

46 Den 29 april 2014 tillsatte justitieministern en särskild utredare som skulle granska de svenska reglernas tillämplighet mot bakgrund av Digital Rights-domen. I en promemoria av den 13 juni 2014 ("Datalagring, EU-rätten och svensk rätt", Ds 2014:23) (nedan kallad promemorian) fann utredaren att det svenska regelverket avseende lagring enligt 6 kap. 16 a–f §§ LEK inte strider mot unionsrätten eller mot Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, som undertecknades i Rom den 4 november 1950 (nedan kallad Europakonventionen). Enligt den särskilda utredaren kunde Digital Rights-domen inte tolkas som att den kritiserade själva grundtanken med en generell och odifferentierad lagring av uppgifter. Domen skulle inte heller tolkas på så sätt att domstolen där presenterat en lista där alla punkter måste vara uppfyllda för att regleringen ska anses vara proportionerlig. Den svenska lagstiftningens förenlighet med unionsrätten kan avgöras först vid en sammantagen bedömning av alla omständigheter. Bland dessa omständigheter ingår lagringens omfattning i förhållande till bestämmelserna om tillgång till uppgifterna, lagringstiden samt skydd och säkerhet för uppgifterna.

47 Mot bakgrund av ovanstående underrättade PTS den 19 juni 2014 Tele2 Sverige om att bolaget inte uppfyllde skyldigheten enligt nationell lagstiftning att för brottsbekämpande ändamål lagra de uppgifter som avses i LEK i sex månader. PTS förelade den 27 juni 2014 bolaget att senast den 25 juli 2014 lagra dessa uppgifter.

48 Tele2 Sverige ansåg att promemorian grundade sig på en felaktig tolkning av Digital Rights-domen och att skyldigheten att lagra uppgifterna stred mot de grundläggande rättigheterna enligt stadgan. Bolaget överklagade därför föreläggandet av den 27 juni 2014 till Förvaltningsrätten i Stockholm. Förvaltningsrätten ogillade överklagandet genom dom av den 13 oktober 2014. Tele2 Sverige överklagade den domen till Kammarrätten.

49 Enligt Kammarrätten måste den svenska lagstiftningens förenlighet med unionsrätten prövas mot bakgrund av artikel 15.1 i direktiv 2002/58. Utgångspunkten enligt det direktivet är att trafikuppgifter och lokaliseringsuppgifter ska utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra kommunikationen. Artikel 15.1 i direktivet innehåller emellertid ett undantag från den utgångspunkten, såtillvida att medlemsstaterna tillåts att begränsa ovan nämnda krav på utplåning eller avidentifiering eller rentav föreskriva att uppgifter måste lagras. Unionsrätten medger således att uppgifter om elektronisk kommunikation lagras i vissa fall.

50 Kammarrätten frågar sig emellertid om en generell och odifferentierad skyldighet att lagra uppgifter om elektronisk kommunikation, såsom den som är i fråga i det nationella målet, mot bakgrund av Digital Rights-domen är förenlig med artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8 och 52.1 i stadgan. Med hänsyn till att parterna har olika uppfattningar i frågan, är det lämpligt att EU-domstolen uttalar sig entydigt om huruvida, som Tele2 Sverige anser, en generell och odifferentierad lagring av uppgifter om elektronisk kommunikation i sig är oförenlig med artiklarna 7,

8 och 52.1 i stadgan, eller huruvida, såsom anges i promemorian, förenligheten av en sådan lagring måste bedömas utifrån bestämmelserna om tillgång till uppgifterna, skydd och säkerhet för uppgifterna samt lagringstiden.

51 Mot denna bakgrund beslutade Kammarrätten att vilandeförklara målet och ställa följande frågor till EU-domstolen:

”1) Är en generell skyldighet att lagra trafikuppgifter som omfattar samtliga personer, samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter utan att det görs några åtskillnader, begränsningar eller undantag utifrån syftet att bekämpa brott … förenlig med artikel 15.1 i direktiv 2002/58 med beaktande av artiklarna 7, 8 och 52.1 i stadgan?

2) Om svaret på fråga 1 är nej, kan lagringen ändå vara tillåten

a) om de nationella myndigheternas tillgång till de uppgifter som lagras är fastställd så som beskrivs i punkterna 19–36 [i begäran om förhandsavgörande], och

b) om kraven på säkerhet regleras så som beskrivs i punkterna 38–43 [i begäran om förhandsavgörande], samt då

c) samtliga aktuella uppgifter ska lagras i sex månader räknat från den dag kommunikationen avslutades och därefter utplånas så som beskrivs i punkt 37 [i begäran om förhandsavgörande]?”

Mål C-698/15

52 Tom Watson, Peter Brice och Geoffrey Lewis har var och en väckt talan vid High Court of Justice (England & Wales), Queens’ Bench Division (Divisional Court) (Överdomstolen för England och Wales, avdelningen för överprövning av rättsfrågor, Förenade kungariket) och begärt en laglighetsprövning av section 1 i Dripa. De har bland annat anfört att den bestämmelsen är oförenlig med artiklarna 7 och 8 i stadgan och med artikel 8 i Europakonventionen.

53 I dom av den 17 juli 2015 fann High Court of Justice (England & Wales), Queens’ Bench Division (Divisional Court) (Överdomstolen för England och Wales, avdelningen för överprövning av rättsfrågor) att Digital Rights-domen uppställde ”tvingande unionsrättsliga krav” som gäller medlemsstaternas bestämmelser om lagring av uppgifter om kommunikation och tillgången till sådana uppgifter. Enligt nämnda domstol kunde en nationell lagstiftning med samma innehåll som direktiv 2006/24 inte längre vara förenlig med proportionalitetsprincipen, eftersom EU-domstolen i Digital Rights-domen slagit fast att direktivet var oförenligt med den principen. Av den underliggande logiken i Digital Rights-domen följer att en lagstiftning som inrättar ett generellt system för lagring av uppgifter om kommunikation kränker de rättigheter som garanteras i artiklarna 7 och 8 i stadgan, såvida inte den lagstiftningen kompletteras med ett i nationell rätt definierat system för tillgång till uppgifter som ger tillräckliga garantier för skydd av dessa rättigheter. Section 1 i Dripa är således inte förenlig med artiklarna 7 och 8 i stadgan, då den inte innehåller tydliga och precisa bestämmelser om tillgång till och användning av lagrade uppgifter och då den inte villkorar tillgången till dessa uppgifter med en förhandskontroll av en domstol eller ett oberoende förvaltningsorgan.

54 Inrikesministern överklagade den domen till Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål, Förenade kungariket) (nedan kallad Court of Appeal).

55 Den domstolen har anfört att inrikesministern enligt section 1.1 i Dripa utan förhandstillstånd från en domstol eller ett oberoende förvaltningsorgan får föreskriva en allmän ordning som ålägger offentliga teleoperatörer att lagra alla uppgifter i fråga om varje system för posttjänster eller telekommunikationer under högst 12 månader, om ministern bedömer att ett sådant krav är nödvändigt och proportionerligt för att uppnå de mål som anges i Förenade kungarikets lagstiftning. Även om dessa uppgifter inte innefattar innehållet i en kommunikation, skulle de kunna vara särskilt ingripande i privatlivet för kommunikationstjänsternas användare.

56 Den hänskjutande domstolen har i beslutet om hänskjutande och i sitt avgörande av den 20 november 2015, som meddelades inom ramen för målet om överklagande och där den beslutade att begära förhandsavgörande från EU-domstolen anfört att de nationella bestämmelserna om lagring av uppgifter med nödvändighet omfattas av artikel 15.1 i direktiv 2002/58 och således måste iaktta de krav som följer av stadgan. Enligt artikel 1.3 i direktivet har unionslagstiftaren emellertid inte harmoniserat bestämmelserna om tillgång till lagrade uppgifter.

57 Vad gäller Digital Rights-domens inverkan på de frågor som aktualiserats i det nationella målet, har den hänskjutande domstolen anfört att EU-domstolen i det mål som avgjordes genom Digital Rights-domen hade att pröva giltigheten av direktiv 2006/24, inte giltigheten av den nationella lagstiftningen. Med hänsyn bland annat till det nära sambandet mellan lagring av uppgifter och tillgång till uppgifterna, var det nödvändigt att direktivet åtföljdes av en rad garantier och att EU-domstolen i Digital Rights-domen, som ett led i prövningen av lagenligheten av direktivets bestämmelser om lagring av uppgifter, även bedömde bestämmelserna om tillgången till dessa uppgifter. Domstolen hade således i den domen inte i åtanke att formulera några tvingande krav på nationell lagstiftning rörande tillgång till uppgifter som inte genomför unionsrätten. Domstolens resonemang var vidare nära kopplat till direktivets syfte. En nationell lagstiftning måste dock bedömas utifrån syftena med den lagstiftningen och det sammanhang den ingår i.

58 Vad gäller behovet av att begära ett förhandsavgörande från EU-domstolen, har den hänskjutande domstolen betonat att vid den tidpunkt då den fattade beslut om hänskjutande, hade sex domstolar i andra medlemsstater, däribland fem i högsta instans, ogiltigförklarat nationell lagstiftning med stöd av Digital Rights-domen. Svaret på de frågor som aktualiseras är således inte uppenbart, och det är nödvändigt att besvara dem för att kunna avgöra de nationella målen.

59 Mot denna bakgrund beslutade Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål) att vilandeförklara målen och ställa följande frågor till EU-domstolen:

”1) Innebär Digital Rights-domen (särskilt punkterna 60–62) att det i unionsrätten uppställs tvingande krav som en medlemsstats nationella bestämmelser om tillgång till uppgifter som lagrats i enlighet med nationell lagstiftning måste uppfylla för att vara förenliga med artiklarna 7 och 8 i stadgan?

2) Innebär Digital Rights-domen att artikel 7 och/eller artikel 8 i stadgan ges ett mer vidsträckt tillämpningsområde än artikel 8 i Europakonventionen såsom den bestämmelsens tillämpningsområde har fastställts i praxis från Europeiska domstolen för de mänskliga rättigheterna (Europadomstolen)?”

Förfarandet vid domstolen

60 Genom beslut av den 1 februari 2016, Davis m.fl. (C-698/15, ej publicerat, EU:C:2016:70) biföll domstolens ordförande begäran från Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål) om att mål C-698/15 skulle handläggas skyndsamt i enlighet med artikel 105.1 i domstolens rättegångsregler.

61 Genom beslut av domstolens ordförande av den 10 mars 2016 förenades målen C-203/15 och C-698/15 vad gäller det muntliga förfarandet och domen.

Prövning av tolkningsfrågorna

Den första frågan i mål C-203/15

62 Kammarrätten har ställt den första frågan i mål C-203/15 för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8 och 52.1 i stadgan ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning – som den i det nationella målet – som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.

63 Frågan har uppkommit bland annat av den anledningen att direktiv 2006/24, som den berörda svenska lagstiftningen syftade till att införliva, förklarades ogiltigt genom Digital Rights-domen, men parterna är oense om räckvidden av den domen och dess inverkan på nämnda lagstiftning, vilken reglerar lagring av trafikuppgifter och lokaliseringsuppgifter samt de nationella myndigheternas tillgång till dessa uppgifter.

64 Domstolen ska inledningsvis pröva om sådan nationell lagstiftning som den som är i fråga i målet omfattas av unionsrättens tillämpningsområde.

Tillämpningsområdet för direktiv 2002/58

65 De medlemsstater som har yttrat sig skriftligen till domstolen har uttryckt skilda meningar om huruvida, och i så fall i vilken utsträckning, nationell lagstiftning som reglerar lagring av trafikuppgifter och lokaliseringsuppgifter samt nationella myndigheters tillgång till sådana uppgifter, i brottsbekämpande syfte, omfattas av tillämpningsområdet för direktiv 2002/58. Enligt den belgiska, den danska, den tyska, den estniska regeringen och Irland samt den nederländska regeringen bör denna fråga besvaras jakande, medan den tjeckiska regeringen har föreslagit att den ska besvaras nekande, eftersom sådan lagstiftning har brottsbekämpning som enda syfte. Förenade kungarikets regering har gjort gällande att endast lagstiftning om lagring av uppgifter, men däremot inte lagstiftning om behöriga nationella brottsbekämpande myndigheters tillgång till sådana uppgifter, omfattas av direktivets tillämpningsområde.

66 Slutligen har kommissionen, i sitt skriftliga yttrande till domstolen i mål C-203/15, hävdat att den svenska lagstiftning som är i fråga i det målet omfattas av tillämpningsområdet för direktiv 2002/58. Samtidigt har den i sitt skriftliga yttrande i mål C-698/15 anfört att direktivets tillämpningsområde endast omfattar nationella bestämmelser som reglerar lagring av uppgifter, och inte bestämmelser som reglerar nationella myndigheters tillgång till uppgifterna. De sistnämnda bestämmelserna ska dock enligt kommissionen beaktas vid bedömningen av om en nationell lagstiftning som reglerar lagring av uppgifter hos leverantörer av elektroniska kommunikationstjänster utgör ett proportionerligt ingrepp i de grundläggande rättigheter som garanteras i artiklarna 7 och 8 i stadgan.

67 Domstolen vill i det sammanhanget påpeka att tillämpningsområdet för direktiv 2002/58 ska bedömas med hänsyn bland annat till direktivets allmänna systematik.

68 Enligt lydelsen i artikel 1.1 i direktiv 2002/58 harmoniserar direktivet bland annat medlemsstaternas bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, i synnerhet rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation.

69 Enligt artikel 1.3 i direktiv 2002/58 ska direktivet inte tillämpas på ”statens verksamhet” på de områden som avses här, det vill säga bland annat statens verksamhet på straffrättens område och verksamheter som avser allmän säkerhet, försvar och statens säkerhet, inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet (se analogt, beträffande artikel 3.2 första strecksatsen i direktiv 95/46, dom av den 6 november 2003, Lindqvist, C-101/01, EU:C:2003:596, punkt 43, och dom av den 16 december 2008, Satakunnan Markkinapörssi och Satamedia, C-73/07, EU:C:2008:727, punkt 41).

70 Artikel 3 i direktiv 2002/58 anger att direktivet ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom unionen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning (nedan kallade elektroniska kommunikationstjänster). Direktivet ska därför anses reglera verksamheten för leverantörer av sådana tjänster.

71 Artikel 15.1 i direktiv 2002/58 låter medlemsstaterna, på de villkor den föreskriver, ”genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv”. Artikel 15.1 andra meningen i samma direktiv nämner, som exempel på åtgärder som medlemsstaterna får vidta, åtgärder ”som innebär att uppgifter får bevaras”.

72 De lagstiftningsåtgärder som avses i artikel 15.1 i direktiv 2002/58 avser förvisso sådan verksamhet som endast kan bedrivas av staten eller statliga myndigheter och som inte kan bedrivas av enskilda personer (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 51). De syften som dessa åtgärder ska ha enligt nämnda bestämmelse, det vill säga att skydda nationell säkerhet, försvaret och allmän säkerhet samt att förebygga, undersöka, avslöja och väcka åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem, sammanfattar också väsentligen syftena med de verksamheter som avses i artikel 1.3 i direktivet.

73 Sett till den allmänna systematiken i direktiv 2002/58 betyder dock inte de omständigheter som nämns i föregående punkt att de lagstiftningsåtgärder som avses i artikel 15.1 i direktivet ska anses uteslutna från direktivets tillämpningsområde. Det skulle helt frånta den bestämmelsen dess ändamålsenliga verkan. Nämnda bestämmelse förutsätter nämligen med nödvändighet att de där avsedda nationella åtgärderna, såsom de om lagring av uppgifter i brottsbekämpande syfte, omfattas av direktivets tillämpningsområde, eftersom direktivet uttryckligen tillåter medlemsstaterna att vidta sådana åtgärder endast under förutsättning att de däri angivna villkoren är uppfyllda.

74 De lagstiftningsåtgärder som avses i artikel 15.1 i direktiv 2002/58 reglerar dessutom – för de syften som anges i bestämmelsen – verksamheten för leverantörer av elektroniska kommunikationstjänster. Den bestämmelsen, jämförd med artikel 3 i samma direktiv, ska därför tolkas på så sätt att sådana lagstiftningsåtgärder omfattas av direktivets tillämpningsområde.

75 I tillämpningsområdet ingår i synnerhet en lagstiftningsåtgärd, såsom den som är i fråga i det nationella målet, som ålägger sådana leverantörer en skyldighet att lagra trafikuppgifter och lokaliseringsuppgifter. Deras verksamhet innebär nämligen med nödvändighet att de behandlar personuppgifter.

76 Tillämpningsområdet inkluderar även en lagstiftningsåtgärd som, såsom i det nationella målet, innebär att nationella myndigheter får tillgång till uppgifter som lagrats av leverantörer av elektroniska kommunikationstjänster.

77 Skyddet för konfidentialitet vid elektronisk kommunikation och för därmed förbundna trafikuppgifter, som säkerställs i artikel 5.1 i direktiv 2002/58, gäller för åtgärder som vidtas av andra personer än användarna, oavsett om de är privatpersoner eller privata enheter eller om de är statliga enheter. Som

bekräftas av skäl 21 i samma direktiv, syftar direktivet till att hindra obehörig åtkomst av kommunikation, inbegripet ”uppgifter som har samband med sådan kommunikation”, för att skydda konfidentialiteten vid elektronisk kommunikation.

78 En lagstiftningsåtgärd genom vilken en medlemsstat med stöd av artikel 15.1 i direktiv 2002/58 ålägger leverantörer av elektronisk kommunikation att, för de syften som nämns i denna bestämmelse, ge de nationella myndigheterna tillgång till uppgifter som leverantörerna lagrat, på de villkor som föreskrivs genom åtgärden, rör följaktligen behandling av personuppgifter från leverantörernas sida, och denna behandling omfattas av direktivets tillämpningsområde.

79 Då datalagringen endast sker för att i förekommande fall ge behöriga nationella myndigheter tillgång till uppgifterna, måste dessutom en nationell lagstiftning som föreskriver att uppgifter ska lagras i princip innehålla bestämmelser om behöriga nationella myndigheters tillgång till de uppgifter som lagrats av leverantörer av elektroniska kommunikationstjänster.

80 Den tolkningen får också stöd av artikel 15.1b i direktiv 2002/58, enligt vilken leverantörerna ska införa interna förfaranden för att besvara förfrågningar om tillgång till användarnas personuppgifter, på grundval av nationella bestämmelser som antagits med stöd av artikel 15.1 i direktivet.

81 Av vad som anförts följer att nationell lagstiftning av det slag som är i fråga i de båda nationella målen omfattas av tillämpningsområdet för direktiv 2002/58.

Tolkningen av artikel 15.1 i direktiv 2002/58, mot bakgrund av artiklarna 7, 8, 11 och 52.1 i stadgan

82 Enligt artikel 1.2 i direktiv 2002/58 ska bestämmelserna i detta direktiv ”precisera och komplettera” direktiv 95/46. Som framgår av skäl 2 i direktiv 2002/58, eftersträvas i detta direktiv i synnerhet att säkerställa full respekt för rättigheterna i artiklarna 7 och 8 i stadgan. Det framgår av redogörelsen för skälen i förslaget till Europaparlamentets och rådets direktiv om behandling av personuppgifter och skydd för privatlivet inom sektorn för elektronisk kommunikation (KOM/2000/385 slutlig), som låg till grund för direktiv 2002/58, att unionslagstiftaren avsett att ”garantera en fortsatt hög skyddsnivå för personuppgifter och privatliv för alla elektroniska kommunikationstjänster, oavsett vilken teknik som används”.

83 Direktiv 2002/58 innehåller specifika bestämmelser för detta ändamål, vilka – såsom framgår av bland annat skälen 6 och 7 – syftar till att skydda användarna av elektroniska kommunikationstjänster mot de risker för deras personuppgifter och integritet som ny teknik och den ökade kapaciteten för automatisk lagring och behandling av uppgifter medför.

84 Enligt artikel 5.1 i direktiv 2002/58 ska medlemsstaterna genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster liksom för därmed förbundna trafikuppgifter.

85 Principen om konfidentialitet vid kommunikation som infördes genom direktiv 2002/58 innebär bland annat, som framgår av artikel 5.1 andra meningen i direktivet, i princip förbud för andra personer än användarna att utan användarnas samtycke lagra trafikuppgifter avseende elektronisk kommunikation. Undantag gäller endast för personer som har laglig rätt att göra detta i enlighet med artikel 15.1 i direktivet, samt för teknisk lagring som är nödvändig för överföring av kommunikationen (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 47).

86 Enligt artikel 6 i direktiv 2002/58, och som också framgår av skälen 22 och 26 i direktivet, får trafikuppgifter behandlas och lagras i den utsträckning och under den tid som krävs för att kunna fakturera för tjänster, marknadsföra tjänster eller tillhandahålla kringtjänster (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkterna 47

och 48). Vad specifikt gäller fakturering för tjänster, är sådan behandling endast tillåten fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning. När den perioden har löpt ut, ska de behandlade och lagrade uppgifterna utplånas eller avidentifieras. Vad gäller andra lokaliseringsuppgifter än trafikuppgifter, föreskriver artikel 9.1 i direktivet att de endast får behandlas på vissa villkor och sedan de har avidentifierats eller om användarna eller abonnenterna gett sitt samtycke.

87 Räckvidden av bestämmelserna i artiklarna 5, 6 och 9.1 i direktiv 2002/58, som syftar till att säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter och minimera riskerna för missbruk, ska vidare bedömas mot bakgrund av skäl 30 i direktivet. Där anges att ”[s]ystemen för tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster bör utformas så att mängden nödvändiga personuppgifter begränsas till ett absolut minimum”.

88 Artikel 15.1 i direktiv 2002/58 ger förvisso medlemsstaterna möjlighet att föreskriva undantag från deras principiella skyldighet enligt artikel 5.1 i samma direktiv att garantera konfidentialiteten för personuppgifter liksom från motsvarande skyldigheter enligt bland annat artiklarna 6 och 9 i direktivet (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 50).

89 I och med att artikel 15.1 i direktiv 2002/58 ger medlemsstaterna möjlighet att begränsa omfattningen av den principiella skyldigheten att säkerställa konfidentialiteten för kommunikation och därmed förbundna trafikuppgifter, ska denna artikel emellertid enligt domstolens fasta praxis tolkas strikt (se, analogt, dom av den 22 november 2012, Probst, C-119/12, EU:C:2012:748, punkt 23). En sådan bestämmelse kan alltså inte motivera att undantaget från denna principiella skyldighet, i synnerhet förbudet i artikel 5 i direktivet mot att lagra dessa uppgifter, görs till huvudregel. Det skulle i stor utsträckning förta verkan av sistnämnda bestämmelse.

90 Artikel 15.1 första meningen i direktiv 2002/58 föreskriver att de lagstiftningsåtgärder som den bestämmelsen avser och som avviker från principen om konfidentialitet för kommunikationer och därmed förbundna trafikuppgifter ska syfta till att ”skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem” eller ha ett annat syfte enligt artikel 13.1 i direktiv 95/46, som artikel 15.1 första meningen i direktiv 2002/58 hänvisar till (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 53). Denna uppräkning av syftena är uttömmande, vilket också framgår av artikel 15.1 andra meningen i direktivet, enligt vilken lagstiftningsåtgärder ska vara motiverade av ”de skäl” som fastställs i artikel 15.1 första meningen. Medlemsstaterna kan alltså inte anta sådana åtgärder för andra syften än de som räknas upp i artikel 15.1 första meningen i direktiv 2002/58.

91 Vidare föreskrivs i artikel 15.1 tredje meningen i direktiv 2002/58 att ”[a]lla åtgärder som avses i [artikel 15.1 i direktivet] skall vara i enlighet med de allmänna principerna i [union]slagstiftningen, inklusive principerna i artikel 6.1 och 6.2 [FEU]”. Bland dessa ingår de allmänna principer och grundläggande rättigheter som numera garanteras i stadgan. Nämnda artikel 15.1 ska alltså tolkas mot bakgrund av de grundläggande rättigheter som garanteras i stadgan (se, analogt, beträffande direktiv 95/46, dom av den 20 maj 2003, Österreichischer Rundfunk m.fl., C-465/00, C-138/01 och C-139/01, EU:C:2003:294, punkt 68, dom av den 13 maj 2014, Google Spain och Google, C-131/12, EU:C:2014:317, punkt 68, och dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkt 38).

92 Skyldigheten, enligt nationell lagstiftning av nu aktuellt slag, för leverantörer av elektroniska kommunikationstjänster att lagra trafikuppgifter i syfte att vid behov göra dem tillgängliga för behöriga nationella myndigheter väcker frågor om sådan lagstiftnings förenlighet inte bara med

artiklarna 7 och 8 i stadgan, som uttryckligen nämns i tolkningsfrågorna, utan även med yttrandefriheten, som garanteras i artikel 11 i stadgan (se, analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkterna 25 och 70).

93 Betydelsen av såväl rätten till respekt för privatlivet, vilken garanteras i artikel 7 i stadgan, som rätten till skydd för personuppgifter, vilken garanteras i artikel 8 i stadgan, framgår av domstolens praxis (se, för ett liknande resonemang, dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkt 39 och där angiven rättspraxis) och ska beaktas vid tolkningen av artikel 15.1 i direktiv 2002/58. Detsamma gäller yttrandefriheten, med tanke på den särskilda betydelse den har i varje demokratiskt samhälle. Denna grundläggande rättighet, som garanteras i artikel 11 i stadgan, utgör en av grundvalarna för ett demokratiskt och pluralistiskt samhälle och ingår i de värden som unionen enligt artikel 2 FEU bygger på (se, för ett liknande resonemang, dom av den 12 juni 2003, Schmidberger, C-112/00, EU:C:2003:333, punkt 79, och dom av den 6 september 2011, Patriciello, C-163/10, EU:C:2011:543, punkt 31).

94 Enligt artikel 52.1 i stadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara föreskriven i lag och vara förenlig med deras väsentliga innehåll. Begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt intresse som erkänns av unionen eller mot behovet av skydd för andra människors rättigheter och friheter (dom av den 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punkt 50).

95 Artikel 15.1 första meningen i direktiv 2002/58 föreskriver att medlemsstaterna får vidta en åtgärd som avviker från principen om konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter om åtgärden ”i ett demokratiskt samhälle är nödvändig, lämplig och proportionell” för de syften som anges i den bestämmelsen. Skäl 11 i direktivet preciserar att en åtgärd av sådant slag måste stå i ”strikt” proportion till det avsedda ändamålet. Vad särskilt gäller lagring av uppgifter kräver artikel 15.1 andra meningen i direktivet att uppgifter endast bevaras ”under en begränsad period” och att lagringen ”motiveras” av de skäl som fastställs i artikel 15.1 första meningen i direktivet.

96 Att proportionalitetsprincipen ska iakttas framgår även av domstolens fasta praxis, enligt vilken skyddet av den grundläggande rätten till respekt för privatlivet på unionsnivå kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt (dom av den 16 december 2008, Satakunnan Markkinapörssi och Satamedia, C-73/07, EU:C:2008:727, punkt 56, dom av den 9 november 2010, Volker und Markus Schecke och Eifert, C-92/09 och C-93/09, EU:C:2010:662, punkt 77, Digital Rights-domen, punkt 52, och dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkt 92).

97 Vad gäller frågan huruvida en nationell lagstiftning som den som är i fråga i mål C-203/15 uppfyller de villkoren, påpekar domstolen att den lagstiftningen föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter för samtliga abonnenter och registrerade användare avseende samtliga elektroniska kommunikationsmedel och ålägger leverantörer av elektroniska kommunikationstjänster att systematiskt och kontinuerligt lagra dessa uppgifter, utan undantag. Som framgår av begäran om förhandsavgörande, motsvarar de kategorier av uppgifter som avses med denna lagstiftning väsentligen dem för vilka lagring föreskrevs i direktiv 2006/24.

98 De uppgifter som leverantörer av elektroniska kommunikationstjänster således är skyldiga att lagra är sådana som gör det möjligt att spåra och identifiera en kommunikationskälla, identifiera slutmålet för en kommunikation, identifiera en kommunikations datum, tidpunkt, varaktighet och typ, identifiera användarnas kommunikationsutrustning och identifiera lokaliseringen av mobil kommunikationsutrustning. Bland dessa uppgifter ingår abonnentens eller den registrerade användarens namn och adress, det uppringande telefonnumret, det uppringda numret och IP-adressen för internettjänster. Dessa uppgifter gör det möjligt att få kännedom om med vilken person en abonnent eller registrerad användare har kommunicerat och på vilket sätt, hur länge kommunikationen varat och från vilken plats kommunikationen skett. Uppgifterna gör det dessutom

möjligt att få kännedom om hur ofta abonnenten eller den registrerade användaren kommunicerat med vissa personer under en viss tidsperiod (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 26).

99 Dessa uppgifter kan sammantagna göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 27). Dessa uppgifter gör det möjligt att, som generaladvokaten påpekat i punkterna 253, 254 och 257–259 i sitt förslag till avgörande, kartlägga de berörda personerna på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationerna.

100 Det ingrepp som en sådan lagstiftning utgör i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan är långtgående och måste betraktas som synnerligen allvarligt. Den omständigheten att lagringen av uppgifterna och den senare användningen av dem sker utan att abonnenten eller den registrerade användaren är underrättad om detta kan ge de berörda personerna en känsla av att deras privatliv står under ständig övervakning (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 37).

101 Även om en sådan lagstiftning inte medger lagring av innehållet i en kommunikation, och därför inte kan kränka det väsentliga innehållet i dessa grundläggande rättigheter (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 39), skulle lagringen av trafikuppgifter och lokaliseringsuppgifter emellertid kunna inverka på användningen av de elektroniska kommunikationsmedlen och följaktligen på användarnas utövande av sin i artikel 11 i stadgan garanterade yttrandefrihet (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 28).

102 Med hänsyn till det allvarliga ingrepp i de berörda grundläggande rättigheterna som en nationell lagstiftning som i brottsbekämpande syfte föreskriver lagring av trafikuppgifter och lokaliseringsuppgifter utgör, kan endast bekämpning av grov brottslighet motivera en sådan åtgärd (se analogt, angående direktiv 2006/24, Digital Rights-domen, punkt 60).

103 En effektiv bekämpning av grov brottslighet och särskilt av organiserad brottslighet och terrorism kan förvisso i stor utsträckning vara beroende av användningen av moderna utredningstekniker. Fastän det syftet är av allmänt samhällsintresse kan det emellertid inte, trots sin grundläggande betydelse, i sig ensamt motivera att en nationell lagstiftning som föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter ska anses vara nödvändig för detta ändamål (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 51).

104 För det första får en sådan lagstiftning till följd, sett till dess särdrag såsom de beskrivits i punkt 97 ovan, att lagring av trafikuppgifter och lokaliseringsuppgifter blir huvudregeln, trots att det system som inrättats genom direktiv 2002/58 kräver att sådan lagring ska vara ett undantag.

105 För det andra innebär en nationell lagstiftning som den som är i fråga i det nationella målet, som på ett generellt sätt omfattar samtliga abonnenter och registrerade användare och avser samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter, att det inte görs några åtskillnader, begränsningar eller undantag utifrån det eftersträvade syftet. Den berör på ett allomfattande sätt samtliga personer som använder elektroniska kommunikationstjänster, utan att dessa personer ens indirekt befinner sig i en situation som kan föranleda lagföring. Den är således även tillämplig på personer beträffande vilka det inte föreligger något indicium som ger anledning att tro att deras beteende ens kan ha ett indirekt eller avlägset samband med grov brottslighet. Den föreskriver inte heller några undantag, vilket innebär att den även är tillämplig på personer vilkas kommunikationer enligt nationell rätt omfattas av tystnadsplikt (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkterna 57 och 58).

106 En sådan lagstiftning kräver inte något samband mellan de uppgifter som ska lagras och ett hot mot den allmänna säkerheten. Den är inte begränsad till lagring av uppgifter avseende en viss tidsperiod och/eller ett visst geografiskt område och/eller en viss krets av personer som på något sätt kan vara inblandade i ett allvarligt brott eller till personer beträffande vilka lagringen av uppgifter av andra skäl skulle kunna bidra till bekämpningen av brott (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 59).

107 En nationell lagstiftning som den som är i fråga i det nationella målet överskrider således gränserna för vad som är strängt nödvändigt och kan inte anses motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan.

108 Artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan hindrar däremot inte att en medlemsstat antar lagstiftning som i förebyggande syfte tillåter en riktad lagring av trafikuppgifter och lokaliseringsuppgifter, i syfte att bekämpa grov brottslighet, förutsatt att lagringen av uppgifterna, vad gäller vilka slags uppgifter som ska lagras, vilka kommunikationsmedel som avses, vilka personer som berörs och hur länge lagringen ska ske, begränsas till vad som är strängt nödvändigt.

109 För att uppfylla kraven i föregående punkt måste den nationella lagstiftningen för det första föreskriva tydliga och precisa bestämmelser som reglerar omfattningen och tillämpligheten av en sådan lagringsåtgärd och som slår fast minimikrav, så att de personer vars uppgifter har lagrats har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk. Den måste särskilt precisera under vilka omständigheter och villkor en sådan lagringsåtgärd får vidtas i förebyggande syfte, vilket säkerställer att lagringen begränsas till vad som är strängt nödvändigt (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 54 och där angiven rättspraxis).

110 Vad för det andra gäller de materiella villkor som en nationell lagstiftning som inom ramen för brottsbekämpning tillåter lagring i förebyggande syfte av trafikuppgifter och lokaliseringsuppgifter måste uppfylla för att säkerställa att den är begränsad till vad som är strängt nödvändigt, påpekar domstolen att även om de villkoren kan variera utifrån vilka åtgärder som vidtas för att förebygga, undersöka, avslöja och väcka åtal för grov brottslighet, måste lagringen av uppgifterna alltid uppfylla objektiva kriterier, som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträvade syftet. I synnerhet måste villkoren vara sådana att de klart avgränsar åtgärdens omfattning och följaktligen den berörda personkretsen.

111 Vad gäller avgränsningen av en sådan åtgärd beträffande den personkrets och de situationer som kan komma att beröras gör domstolen följande bedömning. Den nationella lagstiftningen ska grunda sig på objektiva omständigheter som gör det möjligt att ta sikte på en personkrets vars uppgifter kan avslöja en, åtminstone indirekt, koppling till grov brottslighet och på ett eller annat sätt kan bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten. En sådan avgränsning kan säkerställas genom ett geografiskt kriterium när de behöriga nationella myndigheterna på grundval av objektiva omständigheter bedömer att det i ett eller flera geografiska områden finns en förhöjd risk för förberedelse eller genomförande av sådana handlingar.

112 Den första frågan i mål C-203/15 ska mot denna bakgrund besvaras på följande sätt. Artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.

Den andra frågan i mål C-203/15 och den första frågan i mål C-698/15

113 Kammarrätten i Stockholm har ställt sin andra fråga, i mål C-203/15, endast för det fall att den första frågan i målet besvaras nekande. Denna andra fråga är dock oberoende av om en lagring av uppgifter är generell eller riktad, i den mening som avses i punkterna 108–111 ovan. Den andra frågan i mål C-203/15 ska därför besvaras gemensamt med den första frågan i mål C-698/15, vilken ställts oberoende av omfattningen av den skyldighet att lagra uppgifter som ålagts leverantörer av elektroniska kommunikationstjänster.

114 De hänskjutande domstolarna har ställt den andra frågan i mål C-203/15 respektive den första frågan i mål C-698/15 för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8 och 52.1 i stadgan, ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som reglerar skydd och säkerhet för trafikuppgifter och lokaliseringsuppgifter samt, i synnerhet, behöriga nationella myndigheters tillgång till lagrade uppgifter och som inte begränsar denna tillgång till enbart syftet att bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet och inte kräver att uppgifterna ska lagras inom unionen.

115 Vad gäller de syften som kan motivera en nationell lagstiftning som avviker från principen om konfidentialitet vid elektronisk kommunikation vill domstolen anföra följande. Såsom konstaterats i punkterna 90 och 102 ovan är uppräkningen av syftena i artikel 15.1 första meningen i direktiv 2002/58 uttömmande. Därför måste tillgång till lagrade uppgifter vara faktiskt och strikt begränsad till de fall då tillgången krävs för ett av dessa syften. Då syftet med lagstiftningen måste stå i proportion till hur allvarligt ingrepp i de grundläggande rättigheterna det innebär att ge tillgång till de lagrade uppgifterna, är det vid förebyggande, undersökning, avslöjande av och åtal för brott endast bekämpning av grov brottslighet som kan motivera en sådan tillgång.

116 Vad gäller proportionalitetsprincipen, måste en nationell lagstiftning som reglerar på vilka villkor en leverantör av elektronisk kommunikation ska ge behöriga nationella myndigheter tillgång till lagrade uppgifter garantera – i enlighet med vad domstolen konstaterat i punkterna 95 och 96 ovan – att tillgång inte ges utöver vad som är strängt nödvändigt.

117 Eftersom de lagstiftningsåtgärder som avses i artikel 15.1 i direktiv 2002/58 enligt skäl 11 i direktivet ska ”omfattas av lämpliga skyddsmekanismer”, måste en sådan åtgärd dessutom, som framgår av ovan i punkt 109 angiven rättspraxis, föreskriva klara och precisa bestämmelser som anger under vilka omständigheter och på vilka villkor leverantörer av elektroniska kommunikationstjänster måste ge behöriga nationella myndigheter tillgång till uppgifterna. En åtgärd av detta slag måste också vara rättsligt bindande i nationell rätt.

118 För att säkerställa att behöriga nationella myndigheters tillgång till lagrade uppgifter begränsas till vad som är strängt nödvändigt, ankommer det förvisso på nationell rätt att fastställa på vilka villkor leverantörer av elektroniska kommunikationstjänster ska ge sådan tillgång. Det räcker dock inte att den berörda nationella lagstiftningen stadgar att tillgång enbart ska medges för något av de syften som avses i artikel 15.1 i direktiv 2002/58, även om det gäller bekämpning av grov brottslighet. Den måste även ange de materiella och formella villkoren för de behöriga nationella myndigheternas tillgång till de lagrade uppgifterna (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 61).

119 Eftersom en allmän tillgång till samtliga lagrade uppgifter, oberoende av om det finns någon koppling, ens indirekt, till det eftersträvade syftet, inte kan anses vara begränsad till vad som är strängt nödvändigt, måste den berörda nationella lagstiftningen således vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till uppgifter om abonnenter eller registrerade användare. Tillgång kan i princip bara beviljas, i samband med bekämpning av brott, till uppgifter om personer som misstänks planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott (se, analogt,

Europadomstolens dom av den 4 december 2015, Zakharov mot Ryssland, CE:ECHR:2015:1204JUD004714306, § 260). I särskilda fall, som när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism, skulle dock tillgång kunna ges även till uppgifter om andra personer när det finns objektiva omständigheter som ger skäl att anta att de uppgifterna i ett konkret fall effektivt skulle kunna bidra till att bekämpa terrorism.

120 För att säkerställa att dessa villkor uppfylls fullt ut i praktiken, är det väsentligt att behöriga nationella myndigheters tillgång till de lagrade uppgifterna i princip, utom i vederbörligen motiverade brådskande fall, är underkastad förhandskontroll av en domstol eller en oberoende myndighet och att domstolen meddelar sitt avgörande eller myndigheten fattar sitt beslut efter det att de behöriga nationella myndigheterna framställt en motiverad ansökan, vilket kan ske bland annat inom ramen för ett förfarande för förebyggande, avslöjande eller lagföring av brott (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkt 62; se även analogt, vad gäller artikel 8 i Europakonventionen, Europadomstolen, 12 januari 2016, Szabó och Vissy mot Ungern, CE:ECHR:2016:0112JUD003713814, §§ 77 och 80).

121 Vidare krävs att de behöriga nationella myndigheter som beviljats tillgång till lagrade uppgifter informerar de berörda personerna om detta, enligt tillämpliga nationella förfaranden, så snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar. Den informationen är i själva verket nödvändig bland annat för att dessa personer ska kunna utöva sin rätt till rättslig prövning vid kränkning av deras rättigheter, såsom uttryckligen stadgas i artikel 15.2 i direktiv 2002/58, jämförd med artikel 22 i direktiv 95/46 (se, analogt, dom av den 7 maj 2009, Rijkeboer, C-553/07, EU:C:2009:293, punkt 52, och dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkt 95).

122 Vad gäller bestämmelserna om skydd av och säkerhet för de uppgifter som lagras av leverantörer av elektroniska kommunikationstjänster, konstaterar domstolen att artikel 15.1 i direktiv 2002/58 inte medger att medlemsstaterna avviker från artikel 4.1 eller 4.1a i direktivet. De sistnämnda bestämmelserna kräver att leverantörerna vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa ett effektivt skydd av de lagrade uppgifterna mot riskerna för missbruk och otillåten tillgång till uppgifterna. Med hänsyn till att det är fråga om en stor mängd uppgifter och att dessa är av känslig natur samt att det finns en risk för otillåten tillgång till uppgifterna, måste leverantörerna av elektroniska kommunikationstjänster, för att säkerställa fullständig integritet och konfidentialitet för uppgifterna, garantera en särskilt hög skydds- och säkerhetsnivå genom lämpliga tekniska och organisatoriska åtgärder. Den nationella lagstiftningen måste i synnerhet föreskriva att lagringen sker inom unionen och att uppgifterna oåterkalleligen förstörs när deras lagringstid gått ut (se analogt, beträffande direktiv 2006/24, Digital Rights-domen, punkterna 66–68).

123 Medlemsstaterna måste i alla händelser garantera att en oberoende myndighet kontrollerar att den skyddsnivå som säkerställs i unionsrätten iakttas vad gäller skyddet för fysiska personer vid behandlingen av personuppgifter. En sådan kontroll krävs uttryckligen enligt artikel 8.3 i stadgan och utgör enligt domstolens fasta praxis en grundläggande beståndsdel i skyddet för enskilda i samband med behandlingen av personuppgifter. Annars skulle de personer vars personuppgifter har lagrats berövas sin rätt enligt artikel 8.1 och 8.3 i stadgan att vända sig till de nationella tillsynsmyndigheterna med begäran om skydd för sina personuppgifter (se, för ett liknande resonemang, Digital Rights-domen, punkt 68, och dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650, punkterna 41 och 58).

124 Det ankommer på de hänskjutande domstolarna att pröva huruvida och i så fall i vilken utsträckning de nu aktuella nationella lagstiftningarna uppfyller kraven enligt artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, såsom de preciserats i punkterna 115–123 ovan, vad gäller såväl behöriga nationella myndigheters tillgång till lagrade uppgifter som skyddet och säkerhetsnivån för dessa uppgifter.

125 Den andra frågan i mål C-203/15 och den första frågan i mål C-698/15 ska mot denna bakgrund besvaras på följande sätt. Artikel 15.1 i direktiv 2002/58 jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som reglerar skydd och säkerhet för trafikuppgifter och lokaliseringsuppgifter och, i synnerhet, behöriga nationella myndigheters tillgång till lagrade uppgifter och som inte – inom ramen för brottsbekämpning – begränsar denna tillgång till enbart åtgärder som syftar till att bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet och inte kräver att uppgifterna ska lagras inom unionen.

Den andra frågan i mål C-698/15

126 Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål) har ställt sin andra fråga för att få klarhet i huruvida domstolen i Digital Rights-domen tolkade artikel 7 och/eller artikel 8 i stadgan på så sätt att de bestämmelserna anses gå längre än artikel 8 i Europakonventionen enligt Europadomstolens tolkning.

127 Domstolen erinrar inledningsvis om att de grundläggande rättigheter som erkänns i Europakonventionen ingår i unionsrätten som allmänna principer, såsom bekräftas i artikel 6.3 FEU. Europakonventionen utgör emellertid inte något rättsligt instrument som formellt har införlivats med unionens rättsordning, så länge som unionen inte har anslutit sig till denna konvention (se, för ett liknande resonemang, dom av den 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punkt 45 och där angiven rättspraxis).

128 Tolkningen av direktiv 2002/58, som är i fråga här, ska följaktligen göras enbart utifrån de grundläggande rättigheter som garanteras i stadgan (se, för ett liknande resonemang, dom av den 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punkt 46 och där angiven rättspraxis).

129 I förklaringarna avseende artikel 52 i stadgan anges att artikel 52.3 syftar till att trygga det nödvändiga sammanhanget mellan stadgan och Europakonventionen ”utan att detta inkräktar på unionsrättens och Europeiska unionens domstols autonomi” (dom av den 15 februari 2016, N., C-601/15 PPU, EU:C:2016:84, punkt 47). Som uttryckligen anges i artikel 52.3 andra meningen, hindrar inte första meningen i den bestämmelsen unionsrätten från att tillförsäkra ett mer långtgående skydd än Europakonventionen. Till detta kommer slutligen att artikel 8 i stadgan rör en grundläggande rättighet som är skild från den som slås fast i artikel 7 i stadgan och som saknar motsvarighet i Europakonventionen.

130 Enligt domstolens fasta praxis är domstolens uppgift rörande en begäran om förhandsavgörande att bidra till den faktiska lösningen av en tvist som rör unionsrätten och inte att uttala sig om allmänna eller hypotetiska frågor (se, för ett liknande resonemang, dom av den 24 april 2012, Kamberaj, C-571/10, EU:C:2012:233, punkt 41, dom av den 26 februari 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, punkt 42, och dom av den 27 februari 2014, Pohotovosť, C-470/12, EU:C:2014:101, punkt 29).

131 I förevarande fall finner domstolen mot bakgrund av övervägandena i bland annat punkterna 128 och 129 ovan att frågan huruvida skyddet enligt artiklarna 7 och 8 i stadgan går längre än det enligt artikel 8 i Europakonventionen inte påverkar tolkningen av direktiv 2002/58, jämförd med stadgan, vilket är vad den nationella domstolen har att ta ställning till i mål C-698/15.

132 Att besvara den andra frågan i mål C-698/15 tycks således inte bidra till tolkningen av unionsrätten på ett sätt som är nödvändigt för att, i unionsrättsligt avseende, avgöra tvisten i det nationella målet.

133 Den andra frågan i mål C-698/15 kan därför inte tas upp till prövning.

Rättegångskostnader

134 Eftersom förfarandet i förhållande till parterna i de nationella målen utgör ett led i beredningen av samma mål, ankommer det på de hänskjutande domstolarna att besluta om rättegångskostnaderna. De kostnader för att avge yttrande till domstolen som andra än nämnda parter har haft är inte ersättningsgilla.

Mot denna bakgrund beslutar domstolen (stora avdelningen) följande:

1) **Artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009, jämförd med artiklarna 7, 8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna, ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.**

2) **Artikel 15.1 i direktiv 2002/58, i dess lydelse enligt direktiv 2009/136, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan om de grundläggande rättigheterna ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som reglerar skydd och säkerhet för trafikuppgifter och lokaliseringsuppgifter och, i synnerhet, behöriga nationella myndigheters tillgång till lagrade uppgifter och som inte – inom ramen för brottsbekämpning – begränsar denna tillgång till enbart åtgärder som syftar till att bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet och inte kräver att uppgifterna ska lagras inom unionen.**

3) **Den andra frågan från Court of Appeal (England & Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål) avvisas.**

Lenaerts	Tizzano	Silva de Lapuerta
von Danwitz	Da Cruz Vilaça	Juhász
Vilaras	Borg Barthet	Malenovský
Levits	Bonichot	Arabadjiev
Rodin	Biltgen	Lycourgos

Avkunnad vid offentligt sammanträde i Luxemburg den 21 december 2016.

A. Calot Escobar Justitiesekreterare	K. Lenaerts Ordförande

Statens offentliga utredningar 2017

Kronologisk förteckning

1. För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. N.
2. Kraftsamling för framtidens energi. M.
3. Karens för statsråd och statssekreterare. Fi.
4. För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. S.
5. Svensk social trygghet i en globaliserad värld. Del 1 och 2. S.
6. Se barnet! Ju.
7. Straffprocessens ramar och domstolens beslutsunderlag i brottmål – en bättre hantering av stora mål. Ju.
8. Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. M.
9. Det handlar om oss. – unga som varken arbetar eller studerar. U.
10. Ny ordning för att främja god sed och hantera oredlighet i forskning. U.
11. Vägskatt. Volym 1 och 2. Fi.
12. Att ta emot människor på flykt. Sverige hösten 2015. Ju.
13. Finansiering av infrastruktur med privat kapital? Fi.
14. Migrationsärenden vid utlandsmyndigheterna. Ju.
15. Kvalitet och säkerhet på apoteksmarknaden. S.
16. Sverige i Afghanistan 2002–2014. UD.
17. Om oskuldspresumtionen och rätten att närvara vid rättegången. Genomförande av EU:s oskuldspresumtionsdirektiv. Ju.
18. En nationell strategi för validering. U.
19. Uppdrag: Samverkan. Steg på vägen mot fördjupad lokal samverkan för unga arbetslösa. A.
20. Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. U.
21. Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. S.
22. Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. M.
23. digitalforvaltning.nu. Fi.
24. Ett arbetsliv i förändring – hur påverkas ansvaret för arbetsmiljön? A.
25. Samlad kunskap – stärkt handläggning. S.
26. Delningsekonomi. På användarnas villkor. Fi.
27. Vissa frågor inom fastighets- och stämpelskatteområdet. Fi.
28. Ett nationellt centrum för kunskap om och utvärdering av arbetsmiljö. A.
29. Brottsdatalag. Ju
30. En omreglerad spelmarknad. Del 1 och 2. Fi.
31. Stärkt konsumentskydd på bostadsrättsmarknaden. Ju.
32. Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. M.
33. Stärkt ställning för hyresgäster. Ju.
34. Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. M.
35. Samling för skolan. Nationell strategi för kunskap och likvärdighet. U.
36. Informationssäkerhet för samhällsviktiga och digitala tjänster. Ju.
37. Kvalificerad välfärdsbrottslighet – förebygga, förhindra, upptäcka och beivra. Ju.

38. Kvalitet i välfärden – bättre upphandling och uppföljning. Fi.
39. Ny dataskyddslag. Kompletterande bestämmelser till EU:s dataskyddsförordning. Ju.
40. För dig och för alla. S.
41. Meddelarskyddslagen – fler verksamheter med stärkt meddelarskydd. Ju.
42. Vem har ansvaret? M.
43. På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. S.
44. Entreprenad, fjärrundervisning och distansundervisning. U.
45. Ny lag om företagshemligheter. Ju.
46. Stärkt ordning och säkerhet i domstol. Ju.
47. Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. S.
48. Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. S.
49. EU:s dataskyddsförordning och utbildningsområdet. U.
50. Personuppgiftsbehandling för forskningsändamål. U.
51. Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. U.
52. Så stärker vi den personliga integriteten. Ju.
53. God och nära vård. En gemensam färdplan och målbild. S.
54. Fler nyanlända elever ska uppnå behörighet till gymnasiet. U.
55. En ny kamerabevakningslag. Ju.
56. Jakten på den perfekta ersättningsmodellen. Vad händer med medarbetarnas handlingsutrymme? Fi.
57. Lag om flygpassageraruppgifter i brottsbekämpningen. Ju.
58. Amerikansk inresekontroll vid utresa från Sverige – så kan avtalen genomföras. Ju.
59. Reglering av alkoglass m.fl. produkter. S.
60. Nästa steg? Förslag för en stärkt minoritetspolitik. Ku.
61. Villkorlig frigivning – förstärkta åtgärder mot återfall i brott. Ju.
62. Kärnavfallsrådets yttrande över SKB:s Fud-program 2016. M.
63. Miljötillsyn och sanktioner – en tillsyn präglad av ansvar, respekt och enkelhet. M.
64. Detaljplanekravet. N.
65. Hyran vid nyproduktion – en utvärdering och utveckling av modellen med presumtionshyra. Ju.
66. Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning. S.
67. Våldsbejakande extremism. En forskarantologi. Ku.
68. Barnets rättigheter i ett straffrättsligt förfarande m.m. Genomförande av EU:s barnrättsdirektiv och två andra straffprocessuella frågor. Ju.
69. Marknadskontrollmyndigheter – befogenheter och sanktionsmöjligheter. UD.
70. Förstärkt skydd för uppgifter av betydelse för ett internationellt samarbete för fred och säkerhet som Sverige deltar i. Ju.
71. Bostäder på statens mark – en möjlighet? N.
72. Genomförande av vissa straffrättsliga åtaganden för att förhindra och bekämpa terrorism. Ju.
73. En gemensam bild av bostadsbyggnadsbehovet. N.
74. Brottsdatalag – kompletterande lagstiftning. Ju.
75. Datalagring – brottsbekämpning och integritet. Ju.

Statens offentliga utredningar 2017

Systematisk förteckning

Brottsdatalag – kompletterande lagstiftning. [74]

Datalagring – brottsbekämpning och integritet. [75]

Kulturdepartementet

Nästa steg? Förslag för en stärkt minoritetspolitik. [60]

Våldsbejakande extremism. En forskarantologi. [67]

Miljö- och energidepartementet

Kraftsamling för framtidens energi. [2]

Kunskapsläget på kärnavfallsområdet 2017. Kärnavfallet – en fråga i ständig förändring. [8]

Från värdekedja till värdecykel – så får Sverige en mer cirkulär ekonomi. [22]

Substitution i Centrum – stärkt konkurrenskraft med kemikaliesmarta lösningar. [32]

Ekologisk kompensation – Åtgärder för att motverka nettoförluster av biologisk mångfald och ekosystemtjänster, samtidigt som behovet av markexploatering tillgodoses. [34]

Vem har ansvaret? [42]

Kärnavfallsrådets yttrande över SKB:s Fud-program 2016. [62]

Miljötillsyn och sanktioner – en tillsyn präglad av ansvar, respekt och enkelhet. [63]

Näringsdepartementet

För Sveriges landsbygder – en sammanhållen politik för arbete, hållbar tillväxt och välfärd. [1]

Detaljplanekravet. [64]

Bostäder på statens mark – en möjlighet? [71]

En gemensam bild av bostadsbyggnadsbehovet. [73]

Socialdepartementet

För en god och jämlik hälsa. En utveckling av det folkhälsopolitiska ramverket. [4]

Svensk social trygghet i en globaliserad värld. Del 1 och 2.[5]

Kvalitet och säkerhet på apoteksmarknaden. [15]

Läs mig! Nationell kvalitetsplan för vård och omsorg om äldre personer. Del 1 och 2. [21]

Samlad kunskap – stärkt handläggning. [25]

För dig och för alla. [40]

På lika villkor! Delaktighet, jämlikhet och effektivitet i hjälpmedelsförsörjningen. [43]

Nästa steg på vägen mot en mer jämlik hälsa. Förslag för ett långsiktigt arbete för en god och jämlik hälsa. [47]

Kunskapsbaserad och jämlik vård. Förutsättningar för en lärande hälso- och sjukvård. [48]

God och nära vård. En gemensam färdplan och målbild. [53]

Reglering av alkoglass m.fl. produkter. [59]

Dataskydd inom Socialdepartementets verksamhetsområde – en anpassning till EU:s dataskyddsförordning. [66]

Utbildningsdepartementet

Det handlar om oss. – unga som varken arbetar eller studerar. [9]

Ny ordning för att främja god sed och hantera oredlighet i forskning. [10]

En nationell strategi för validering [18]

Tillträde för nybörjare – ett öppnare och enklare system för tillträde till högskoleutbildning. [20]

Samling för skolan. Nationell strategi för kunskap och likvärdighet. [35]

Entreprenad, fjärrundervisning och distansundervisning. [44]

EU:s dataskyddsförordning och utbildningsområdet. [49]

Personuppgiftsbehandling för forskningsändamål.[50]

Utbildning, undervisning och ledning – reformvård till stöd för en bättre skola. [51]

Fler nyanlända elever ska uppnå behörighet till gymnasiet. [54]

Utrikesdepartementet

Sverige i Afghanistan 2002–2014. [16]

Marknadskontrollmyndigheter – befogenheter och sanktionsmöjligheter. [69]