Lagrådsremiss

Datalagring vid brottsbekämpning – anpassningar till EU-rätten

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 28 februari 2019

Mikael Damberg

Mikael Kullberg
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

Enligt EU-domstolens avgörande i den s.k. Tele2-domen är den svenska datalagringen alltför omfattande och inte förenlig med EU-rättens krav. Regeringen föreslår därför anpassningar av regleringen om lagring och tillgång till uppgifter om elektronisk kommunikation i brottsbekämpande syfte, s.k. datalagring, som syftar till att göra reglerna förenliga med EU-rätten på området.

Regeringen bedömer att lagringens omfattning bör minskas och föreslår att lagringstiderna differentieras. Lagringen bör inte få ske utanför EU. Dessutom föreslås att det ska krävas beslut av åklagare för att de brottsbekämpande myndigheterna ska få inhämta uppgifter om elektronisk kommunikation i underrättelseverksamhet.

Regeringen föreslår också att en bestämmelse som nu är tidsbegränsad ska permanentas i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Det ska dessutom bli möjligt att få tillstånd att hämta in uppgifter om brottslig verksamhet som innefattar statsstyrt företagsspioneri och grov misshandel eller olaga frihetsberövande i systemhotande syfte.

Lagändringarna föreslås träda i kraft den 1 oktober 2019.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om ändring i lagen (2003:389) om elektronisk kommunikation,
2. lag om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet,
3. lag om ändring i lagen (2017:718) om ändring i lagen (2012:279) om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

2 Lagtext

Regeringen har följande förslag till lagtext.

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

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

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
16 a §[1]	
Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § är skyldig att lagra sådana uppgifter som avses i 20 § första stycket 1 och 3 som är nödvändiga för att spåra och identifiera kommunikationskällan, *slutmålet* för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.	Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § är skyldig att lagra sådana uppgifter som avses i 20 § första stycket 1 och 3 som är nödvändiga för att spåra och identifiera kommunikationskällan, *målet* för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.
Skyldigheten att lagra uppgifter enligt första stycket omfattar uppgifter som genereras eller behandlas vid telefonitjänst, meddelandehantering, internetåtkomst *och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform)*. Även vid misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas.	Skyldigheten att lagra uppgifter enligt första stycket omfattar uppgifter som genereras eller behandlas vid telefonitjänst *och* meddelandehantering *via mobil nätanslutningspunkt samt vid* internetåtkomst. Även vid *en* misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas.
Den som är skyldig att lagra uppgifter enligt denna paragraf får uppdra åt någon annan att utföra lagringen.	

[1] Senaste lydelse 2012:127.

Regeringen eller den myndighet som regeringen bestämmer *meddelar* närmare föreskrifter om vilka uppgifter som ska lagras enligt denna paragraf.	Regeringen eller den myndighet som regeringen bestämmer *kan med stöd av 8 kap. 7 § regeringsformen meddela* närmare föreskrifter om vilka uppgifter som ska lagras enligt denna paragraf.
	16 d §[2]
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 *enligt följande:* *– Uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska dock endast lagras i två månader.* *– Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ska de dock endast lagras i sex månader.* *Lagringstiden räknas från den dag kommunikationen avslutades.*
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.	*När lagringstiden löpt ut ska den lagringsskyldige genast utplåna uppgifterna. Om en begäran om utlämnande har kommit in innan lagringstiden löpt ut, ska den lagringsskyldige dock fortsätta lagra uppgifterna till dess att de lämnats ut. Efter utlämnandet ska uppgifterna genast utplånas.* *Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om lagringstiden enligt första stycket.*

Denna lag träder i kraft den 1 oktober 2019.

[2] Senaste lydelse 2012:127.

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

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

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

dels att 2 § och de nya 3–5 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	2 §
Uppgifter får hämtas in om omständigheterna är sådana att	Uppgifter får hämtas in om omständigheterna är sådana att *åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar*
1. *åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar* brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, *och*	1. brott för vilket *det* inte är föreskrivet lindrigare straff än fängelse i två år,
2. *skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.*	2. *sabotage enligt 13 kap. 4 § brottsbalken,*
	3. kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
	4. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,
	5. spioneri, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5 eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,

6. företagsspioneri enligt 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understödjs av en främmande makt eller av någon som agerar för en främmande makts räkning,

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

8. grov misshandel eller olaga frihetsberövande enligt 3 kap. 6 § eller 4 kap. 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

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

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.*

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.

3 §[1]

Beslut om inhämtning av uppgifter fattas av *åklagare vid Åklagarmyndigheten efter ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket.*

[1] Tidigare 3 § upphävd genom 2019:000.

5 §	*4 §*
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.	I ett beslut om inhämtning av uppgifter ska det anges vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller *vilken* annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet avser. Tiden får inte bestämmas längre än nödvändigt och får, när det gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.
Om det inte längre finns skäl för ett beslut om inhämtning av uppgifter, ska 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 §	*5 §*
Säkerhets- och integritetsskyddsnämnden ska underrättas om ett beslut om inhämtning av uppgifter enligt denna lag. Underrättelsen ska lämnas senast en månad efter det att ärendet om inhämtning avslutades.	*Den ansökande myndigheten ska underrätta Säkerhets- och integritetsskyddsnämnden* om ett beslut om inhämtning av uppgifter enligt denna lag. Underrättelsen ska lämnas senast en månad efter det att ärendet om inhämtning avslutades.

Denna lag träder i kraft den 1 oktober 2019.

2.3 Förslag till lag om ändring i lagen (2017:718) om ändring i lagen (2012:279) om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Härigenom föreskrivs att lagen (2017:718) om ändring i lagen (2012:279) om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska ha följande lydelse.

3 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska upphöra att gälla vid utgången av september 2019.

3 Ärendet och dess beredning

Regeringen beslutade i juni 2014 att ge en särskild utredare i uppdrag att utvärdera lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbrottskämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Utredningen, som tog namnet Datalagringsutredningen, överlämnade i mars 2015 betänkandet Datalagring och integritet (SOU 2015:31). I betänkandet analyseras också om de rättssäkerhets- och integritetsstärkande åtgärder som vidtogs när lagen infördes är tillräckliga eller om det finns behov av ytterligare sådana åtgärder. Även frågan om Säkerhetspolisens behov av en möjlighet enligt lagen att hämta in uppgifter om brottslig verksamhet som innefattar vissa samhällsfarliga brott behandlas. Vidare behandlas frågan om det behövs förändringar för att stärka skyddet för den personliga integriteten när det gäller reglerna om lagring av uppgifter om elektronisk kommunikation för brottsbekämpande ändamål.

En sammanfattning av betänkandet och utredningens lagförslag finns i *bilaga 1* och *2*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 3*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2015/03153/Å).

I februari 2017 beslutade regeringen att ge en särskild utredare i uppdrag att bl.a. se över bestämmelserna om skyldigheten att lagra uppgifter om elektronisk kommunikation som gäller för leverantörer av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster, samt de brottsbekämpande myndigheternas tillgång till sådana uppgifter. Syftet var 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, den s.k. Tele2-domen. Domen finns i *bilaga 7*. Utredningen, som tog namnet Utredningen om datalagring och EU-rätten, överlämnade i oktober 2017 delbetänkandet Datalagring – brottsbekämpning och integritet (SOU 2017:75).

En sammanfattning av betänkandet och utredningens lagförslag finns i *bilaga 4* och *5*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 6*. Remissyttrandena finns tillgängliga i Justitiedepartementet (Ju2017/07896/Å).

I denna lagrådsremiss behandlar regeringen förslagen i betänkandet från Utredningen om datalagring och EU-rätten. Vidare behandlas Datalagringsutredningens förslag om ändringar i inhämtningslagen och dess förslag om att införa en förstörandeskyldighet för uppgifter som omfattas av yrkesmässig tystnadsplikt.

4 Datalagring och brottsbekämpning

4.1 Uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

Grundläggande rättigheter och datalagring

Grundläggande rättigheter som tillförsäkras enskilda finns i bl.a. regeringsformen (RF), Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) och i Europeiska unionens stadga om de grundläggande rättigheterna (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 är staten som ska se till att det finns ett ramverk som är förenligt med dessa delvis konkurrerande principer.

De rättigheter som främst är av intresse när det gäller lagring av uppgifter om elektronisk kommunikation (s.k. datalagring) är rätten till respekt för privatlivet och den personliga integriteten, rätten till skydd för personuppgifter och rätten till yttrande- och informationsfrihet. Samtliga dessa fri- och rättigheter garanteras i regeringsformen, Europakonventionen och EU:s rättighetsstadga.

För att säkerställa rätten till respekt för privatlivet och rätten till skydd för personuppgifter inom sektorn för elektronisk kommunikation har EU antagit Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), i det följande direktiv 2002/58. Direktivet föreskriver bl.a. att medlemsstaterna ska 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 i lagen (2003:389) om elektronisk kommunikation.

Uppgifter om elektronisk kommunikation har i svensk rätt delats in i olika grupper. Med uppgift om abonnemang avses främst uppgifter om abonnentens nummer, namn, titel och adress. Vidare innefattas uppgift om vem som använt en fast eller dynamisk ip-adress (ett nummer som används som adress på internet) eller ett IMSI-nummer (International Mobile Subscriber Identity, ett nummer som är kopplat till abonnentens simkort och telefonnummer). Med trafikuppgifter avses i detta sammanhang, enkelt uttryckt, uppgifter som behandlas i syfte att förmedla ett elektroniskt meddelande i ett elektroniskt kommunikationsnät eller för att fakturera ett sådant meddelande. Vid sidan av begreppet trafikuppgifter finns i lagen om elektronisk kommunikation även uttrycket lokaliseringsuppgift. Det är en

uppgift som visar den geografiska positionen för terminalutrustningen för en användare. Det kan t.ex. vara fråga om vilken cell (antenn på basstation) som utrustningen kopplat upp sig mot. De olika uppgiftskategorierna är delvis överlappande.

Uppgifter om elektronisk kommunikation är mycket viktiga för brottsbekämpningen. Det finns därför regler i lagen om elektronisk kommunikation och i förordningen (2003:396) om elektronisk kommunikation som har till syfte att säkerställa att dessa uppgifter lagras av dem som tillhandahåller elektroniska kommunikationstjänster och att de brottsbekämpande myndigheterna under vissa förutsättningar kan få tillgång till dem. Samtidigt är huvudregeln enligt 6 kap. 5 § lagen om elektronisk kommunikation, som syftar till att skydda användarnas grundläggande rättigheter, att trafikuppgifter ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande.

Lagringsskyldigheten omfattar vissa uppräknade uppgifter som genereras eller behandlas vid tillhandahållande av telefonitjänster (fasta och mobila), vid meddelandehantering samt vid internetåtkomst. Skyldigheten gäller i sex månader räknat från den dag kommunikationen avslutades. Lagringsskyldigheten omfattar inte innehållet i kommunikationen.

Skyldigheten att lagra dessa uppgifter inkräktar på rättigheter som enskilda är tillförsäkrade enligt regeringsformen, Europakonventionen och EU:s rättighetsstadga, däribland skyddet av den personliga integriteten. För att en sådan åtgärd ska vara godtagbar krävs att den vidtas för ett ändamål som är godtagbart i ett demokratiskt samhälle, att den objektivt sett är ägnad att uppnå syftet med åtgärden och att den är proportionerlig.

De brottsbekämpande myndigheternas verksamhet och tillgången till de uppgifter som lagrats

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, oftast 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.

För både brottsutredande verksamhet och underrättelseverksamhet finns det bestämmelser om hemliga tvångsmedel som reglerar förutsättningarna för att t.ex. få tillgång till lagrade uppgifter. Hur de brottsbekämpande 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 (RB) och i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Härtill kommer lagen (1991:572) om särskild utlänningskontroll och lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott (preventivlagen), som hänvisar till rättegångsbalkens bestämmelser. Tillgången till abonnemangsuppgifter har inte bedömts utgöra ett hemligt tvångsmedel och regleras direkt i lagen om elektronisk kommunikation (se t.ex. prop. 2013/14:237 s. 134).

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, vad gäller inhämtningslagen, krävs inte domstolsbeslut för att få tillgång till uppgifterna. Tillgången till uppgifter om abonnemang kräver inget domstolsbeslut utan får beslutas av den brottsbekämpande myndigheten själv. Det krävs inte heller att brottet är av viss svårighetsgrad.

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

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

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. 322–324). Uppgifterna är ofta av stor betydelse redan i utredningsarbetets inledningsskede. En kontroll av de trafikuppgifter som kan knytas till en brottsplats eller en misstänkt kan användas tillsammans med annan information för att föra utredningen framåt.

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. Inhämtade uppgifter kan i många fall också få till följd att personer avförs från utredningen genom att misstankarna mot dem visar sig sakna substans.

När det gäller planeringsskedet av ett brott är det genom tillgången till trafikuppgifter ofta möjligt att ta reda på t.ex. hur gärningsmännen har sammanträffat och hur de har rekognoserat vid gömställen, längs flyktvägar och vid brottsplatsen samt hur de införskaffat brottsverktyg eller stulit flyktbilar. 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 från brottsplatsen. Dessa uppgifter kan leda till att gömställen upptäcks, att stulna pengar, flyktbilar eller annat gods påträffas och att bortförda personer eller döda kroppar hittas.

Vid utredningen av internetrelaterad brottslighet är uppgifter om elektronisk kommunikation ofta avgörande för att möjliggöra identifiering av en misstänkt gärningsman. Möjligheten till anonymitet och frånvaro av annan teknisk bevisning vid sådan brottslighet medför därför att uppgifter om elektronisk kommunikation i många fall inte kan undvaras vid utredningen, om sådan brottslighet ska kunna utredas. 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). Utredningen om hemlig dataavläsning har i sitt delbetänkande Hemlig dataavläsning – ett viktigt verktyg i kampen mot allvarlig brottslighet (SOU 2017:89) föreslagit att det ska införas en ny lag som, om vissa förutsättningar är uppfyllda, ger de brottsbekämpande myndigheterna möjlighet till hemlig dataavläsning. Med hemlig dataavläsning avses i utredningen en metod för de brottsbekämpande myndigheterna att med någon form av tekniskt hjälpmedel i hemlighet bereda sig tillgång till en dator eller annan teknisk utrustning som kan användas för kommunikation, och därigenom få besked om hur utrustningen används eller har använts och vilken information som finns i

den. Utredningens förslag bereds nu i Regeringskansliet. Hemlig dataavläsning, liksom andra hemliga tvångsmedel eller polisiära metoder som t.ex. fysisk spaning, kan dock inte ses som en ersättning för datalagringen. De skilda metoderna bör snarare ses som olika verktyg i den brottsbekämpande verksamheten som kan komplettera varandra.

När det gäller nyttan av inhämtningen av uppgifter om elektronisk kommunikation i underrättelseverksamhet, har Polismyndigheten och Tullverket konstaterat att information om elektronisk kommunikation är väsentlig för myndigheternas underrättelseverksamhet och att de möjligheter till inhämtning som inhämtningslagen medger har varit avgörande för att inleda förundersökning för en lång rad grova brott. Tillgången till uppgifter om elektronisk kommunikation i underrättelsestadiet är 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. 2017/18:69 s. 30–31). I Säkerhetspolisens underrättelsearbete bidrar datalagringen bl.a. med mycket värdefull information t.ex. för att kartlägga aktörer eller nätverk som har en avsikt och förmåga att begå brott som är allvarliga för rikets säkerhet. Inhämtningen möjliggör således att på ett tidigt stadium fånga upp eventuella grupperingar, skeenden och modus i syfte att förhindra sådan brottslighet (SOU 2015:31 s. 87).

Sammanfattningsvis finns det alltså ett påtagligt behov av uppgifter om elektronisk kommunikation för brottsbekämpningen och uppgifterna ger de brottsbekämpande myndigheterna stor nytta. Däremot är inte nyttan och behovet desamma för alla uppgifter och inte heller desamma över tid, eftersom beteendemönster och teknik hela tiden förändras. Som exempel kan nämnas den minskade användningen av fast telefoni och den ökande användningen av internet i mobiltelefoner.

4.2 Datalagring i ett EU-rättsligt sammanhang

Datalagringsdirektivet och Digital Rights-domen

Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av trafikuppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG, i det följande datalagringsdirektivet, syftade till att harmonisera medlemsstaternas regler om skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra vissa uppgifter om elektronisk kommunikation för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal av allvarliga brott. De bestämmelser som genomförde direktivet i svensk rätt finns huvudsakligen i lagen om elektronisk kommunikation.

I april 2014 meddelade EU-domstolen dom i målen C-293/12 och C-594/12, Digital Rights Ireland m.fl. (Digital Rights-domen) angående giltigheten av datalagringsdirektivet. EU-domstolen förklarade i domen datalagringsdirektivet ogiltigt (punkt 71). Domstolen konstaterade att direktivet innebar ett långtgående och synnerligen allvarligt intrång i rätten till respekt för privatlivet och skyddet av personuppgifter (punkt 37). Domstolen ansåg att ingreppet svarade mot ett mål av allmänt samhällsintresse, bl.a. då syftet med direktivet var att bidra till bekämpandet av grov brottslighet och bidra till den allmänna säkerheten (punkterna 41–44). Domstolen ansåg också att lagringen var ägnad att uppnå det mål som eftersträvades med direktivet eftersom lagringen innebär att brottsbekämpande myndigheter får ytterligare möjligheter att klara upp grova brott och utgör ett värdefullt verktyg i brottsutredningar (punkt 49). När det gäller frågan om huruvida lagringen som föreskrevs enligt direktivet var nödvändig, konstaterade domstolen att bekämpandet av grov brottslighet, särskilt av organiserad brottslighet och terrorism, är av största betydelse för att garantera allmän säkerhet och att dess effektivitet i stor utsträckning kan bero på användningen av moderna utredningstekniker. Ett sådant mål av allmänt samhällsintresse kan emellertid inte, trots dess grundläggande betydelse, i sig ensamt motivera att en sådan lagringsåtgärd ska anses vara nödvändig för nämnda bekämpande (punkt 51). Intrånget var enligt domstolen inte begränsat till vad som var strängt nödvändigt bl.a. då direktivet generellt omfattade samtliga personer, samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter utan att det gjordes några åtskillnader, begränsningar eller undantag utifrån syftet att bekämpa allvarliga brott (punkt 57). Domstolen pekade på olika brister i direktivet och fann att direktivet inte föreskrev några tydliga och precisa regler som reglerade räckvidden av ingreppen i de grundläggande rättigheterna enligt artikel 7 (privatliv) och 8 (personuppgifter) i EU:s rättighetsstadga. Direktivet innebar således ett ingrepp i dessa rättigheter som var långtgående och synnerligen allvarligt. Ingreppet var inte noggrant avgränsat genom bestämmelser som gjorde det möjligt att säkerställa att det verkligen var begränsat till vad som var strängt nödvändigt (punkt 65). Domstolen fann vid en samlad bedömning att unionslagstiftaren överskridit de gränser som proportionalitetsprincipen uppställer mot bakgrund av de aktuella rättigheterna (punkt 69).

Med anledning av att datalagringsdirektivet ogiltigförklarades 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 därefter 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 i april 2015 ett förhandsavgörande av EU-domstolen med anledning av ett överklagat föreläggande från Post- och telestyrelsen (PTS) mot ett lagringsskyldigt företag om att lagra uppgifter om elektronisk kommunikation. I december 2016 besvarade EU-domstolen kammarrättens begäran genom dom i målen C-203/15 och C-698/15, Tele2 Sverige AB m.fl. (Tele2-domen).

EU-domstolen ansåg att direktiv 2002/58 är tillämpligt på nationell lagstiftning som reglerar lagring och tillgång till trafikuppgifter och lokaliseringsuppgifter i brottsbekämpande syfte (punkterna 65–81). Artikel 15.1 i direktivet, som i viss utsträckning tillåter lagring och tillgång till uppgifter om elektronisk kommunikation för t.ex. brottsbekämpande syften och för att skydda nationell säkerhet, ska enligt domstolen tolkas strikt och mot bakgrund av EU:s rättighetsstadga. Sådan lagstiftning bedömdes utgöra inskränkningar i rättigheterna enligt artiklarna 7 (privatliv), 8 (personuppgifter) och 11 (yttrandefrihet) i stadgan (punkterna 88–93). Inskränkningar i rättigheterna får enligt EU-domstolen endast göras under vissa förutsättningar, däribland att de är proportionerliga och strängt nödvändiga (punkterna 94–95).

EU-domstolen uttalade vidare att även om en effektiv bekämpning av grov brottslighet är av allmänt samhällsintresse och även i stor utsträckning kan vara beroende av moderna utredningstekniker, kan det inte i sig ensamt motivera att en nationell lagstiftning som föreskriver en generell och odifferentierad lagring av samtliga trafik- och lokaliseringsuppgifter ska anses vara nödvändig för detta ändamål (punkt 103). 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 (punkterna 115–119). 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 (punkterna 120–121). Därutöver uttalade domstolen att leverantörerna av elektroniska kommunikationstjänster måste garantera en särskilt hög skydds- och säkerhetsnivå genom lämpliga tekniska och organisatoriska åtgärder, att uppgifterna måste förstöras när lagringstiden gått ut och att lagringen måste ske inom unionen (punkt 122).

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 PTS (Kammarrätten i Stockholm, dom den 7 mars 2017, mål nr 7380-14).

Mot bakgrund av de redovisade domarna finns det behov av att anpassa de svenska reglerna om datalagring för att lagstiftningen ska vara förenlig med EU-rätten.

5 En begränsad lagringsskyldighet

5.1 EU-rättens inflytande på området

Regeringens bedömning: EU-rätten sätter upp ramarna för nationell lagstiftning om datalagring för brottsbekämpande ändamål.

På området för nationell säkerhet är frågan om EU-rättens eventuella tillämplighet ännu inte klarlagd i avvaktan på avgöranden från EU-domstolen. Det finns inte skäl att dessförinnan överväga att i svensk rätt införa en särskild reglering för datalagring respektive tillgång till lagrade uppgifter när det gäller brottsbekämpning med koppling till nationell säkerhet.

Utredningens bedömning överensstämmer delvis med regeringens. Utredningen bedömer att oavsett för vilket ändamål uppgifter används är operatörernas lagring och myndigheternas tillgång till dessa uppgifter underkastade den reglering som följer av EU-rätten. Enligt utredningens bedömning innebär detta 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 är datalagringsfrågan underkastad samma EU-rättsliga regelverk, dock att EU-domstolen öppnar för något mer tillåtande nationella regler när det gäller tillgång till uppgifter inom Säkerhetspolisens verksamhetsområde.

Remissinstanserna: De flesta remissinstanser kommenterar inte bedömningen särskilt. *Säkerhetspolisen* saknar ett vidare resonemang om utrymmet att i svensk rätt ha en mer långtgående datalagringslagstiftning inom området nationell säkerhet och vill att denna fråga ska övervägas ytterligare. Även *Försvarsmakten* och *Försvarets radioanstalt* är inne på samma linje och ifrågasätter, med hänvisning till artikel 4 och 5 i fördraget om Europeiska unionen, utredningens bedömning att EU-rätten skulle ha ett sådant direkt inflytande på Säkerhetspolisens verksamhet som rör nationell säkerhet.

Skälen för regeringens bedömning: EU:s kompetens och befogenheter framgår av EU:s grundfördrag. Ett av dem är fördraget om Europeiska unionen (FEU). I det 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).

Vid handläggningen av Tele2-målet hade medlemsstaterna olika uppfattningar i fråga om direktiv 2002/58 överhuvudtaget var tillämpligt. Det som gav upphov till de olika uppfattningarna är att direktivet föreskriver att det inte ska tillämpas på verksamhet som avser allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och statens verksamhet på straffrättens område (artikel 1.3). Samtidigt anger direktivet 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 att bl.a. skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för 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 unionslagstiftningen.

EU-domstolen kom i Tele2-domen till slutsatsen att om man såg till den allmänna systematiken i direktiv 2002/58 betyder inte det att de lagstiftningsåtgärder som avses i artikel 15.1 ska anses uteslutna från direktivets tillämpningsområde. Det skulle enligt domstolen helt frånta artikel 15.1 dess ändamålsenliga verkan. Denna 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 (punkt 73 i domen). EU-domstolen ansåg att direktivet omfattade både lagstiftning som reglerar lagringen av uppgifter och lagstiftning som reglerar tillgången till dessa uppgifter (punkterna 75 och 76 i domen).

I likhet med utredningen konstaterar regeringen att 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 att möjliggöra fri rörlighet för dessa uppgifter inom gemenskapen (artikel 1.1). Direktivet har till syfte att uppfylla målen om fri rörlighet på den inre marknaden men innehåller även bestämmelser som under vissa förutsättningar möjliggör nationella undantag från direktivet om det sker för t.ex. 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). Som nämns ovan konstaterar EU-domstolen i detta sammanhang att, för att undantagsbestämmelsen inte helt ska förlora sin verkan, måste även statens verksamhet på det brottsbekämpande området omfattas av direktivets tillämpningsområde (punkt 73 i domen). Av domen framgår, i linje med det nu anförda, att direktivet är tillämpligt och att EU-domstolen därmed har kompetens på området för datalagring för brottsbekämpande ändamål. EU-rätten sätter således upp ramarna för nationell lagstiftning om datalagring för brottsbekämpande ändamål.

När det gäller området för nationell säkerhet är bedömningen av EU-rättens eventuella tillämplighet mer svårbedömd. *Säkerhetspolisen, Försvarsmakten* och *Försvarets radioanstalt* ifrågasätter utredningens bedömning att Tele2-domen innebär att EU-rätten har inflytande även på datalagringsverksamhet som rör nationell säkerhet.

Regeringen kan konstatera att fokus i Tele2-domen låg på lagring och tillgång till uppgifter för brottsbekämpande ändamål och inte på verksamhet som tar sikte på nationell säkerhet. I en del av domen (punkt 119) uttalar sig domstolen om att tillgång i princip bara bör beviljas, i samband med bekämpning av brott, till uppgifter om personer som misstänks kunna planera, begå eller ha begått ett allvarligt brott eller på något sätt vara inblandade i ett sådant brott. Domstolen tillägger sedan att i särskilda fall, som när vitala intressen för nationell säkerhet, försvar eller allmän säkerhet hotas av terrorism, skulle 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.

Frågan om ett krav på att tillhandahållare av elektroniska kommunikationstjänster måste lämna ut uppgifter till en medlemsstats säkerhets- och underrättelseorgan ska anses omfattas av unionsrätten eller inte är för närvarande föremål för prövning med anledning av en begäran om förhandsavgörande hos EU-domstolen i målet Privacy International m.fl. (C-623/17). Även frågan om hur man ska tolka EU-domstolens uttalande i Tele2-domen om tillgång till uppgifter i fall det handlar om bl.a. nationell säkerhet är uppe till prövning i målet. Även Belgiens konstitutionsdomstol och Frankrikes högsta förvaltningsdomstol har begärt förhandsavgöranden från EU-domstolen i frågor som rör lagstiftning som föreskriver att tillhandahållare av elektroniska kommunikationstjänster är skyldiga att lagra och tillhandahålla myndigheter uppgifter om elektronisk kommunikation, när syftet med lagstiftningen bl.a. är att skydda nationell säkerhet (Ordre des barreaux francophones et germanophone m.fl. [C-520/18] samt förenade målen La Quadrature du Net m.fl. och French Data Network m.fl. [C-511/18 och C-512/18]). Regeringen har yttrat sig i målen och som sin inställning bl.a. angett att åtgärder till skydd för nationell säkerhet faller utanför EU-rättens tillämpningsområde i enlighet med artikel 4.2 i FEU.

Det finns inte något beredningsunderlag för en särskild reglering avseende datalagring som sker med anledning av brottsbekämpning kopplad till nationell säkerhet, exempelvis inom Säkerhetspolisens verksamhet. Det saknas vidare skäl att före EU-domstolens avgörande överväga att göra

åtskillnad i nationell lagstiftning mellan lagring av uppgifter som sker för brottsbekämpande ändamål och lagring av uppgifter på området för nationell säkerhet. När det gäller tillgången till lagrade uppgifter föreslår regeringen i avsnitt 6.8 att 3 § inhämtningslagen ska permanentas och att brottskatalogen i den lagen ska utvidgas till att även omfatta s.k. statsstyrt företagsspionerі och grov misshandel eller olaga frihetsberövande i systemhotande syfte. Före EU-domstolens avgörande finns det i övrigt inte anledning att överväga några förändringar i möjligheten för exempelvis Säkerhetspolisen att få tillgång till uppgifter i brottsbekämpande verksamhet vars syfte är att skydda nationell säkerhet. Frågan om tillgång till lagrade uppgifter behandlas i avsnitt 6.

5.2 Det är nödvändigt att anpassa den svenska lagstiftningen

Regeringens bedömning: Det är nödvändigt att anpassa reglerna om datalagring för att dessa ska vara förenliga med EU-rätten.

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. Lagringsskyldigheten måste dock göras mindre omfattande än i dag och anpassas till vad som är strängt nödvändigt. En begränsad och differentierad lagring, sett till antalet uppgiftstyper, bör därför föreskrivas.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Remissutfallet är blandat. De brottsbekämpande myndigheterna, t.ex. *Polismyndigheten, Åklagarmyndigheten, Säkerhetspolisen* och *Tullverket,* framhåller vikten av datalagring för att kunna upptäcka, förhindra, bekämpa, utreda och lagföra brott. Varje begränsning av lagringsskyldigheten kommer att få allvarliga konsekvenser för myndigheternas förmåga i detta avseende. De anser att gällande lagringsskyldighet redan utgör en miniminivå. *Säkerhetspolisen* framhåller det förändrade säkerhetsläget och anser att en begränsning av lagringsskyldigheten skulle kunna få mycket allvarliga konsekvenser. *Säkerhetspolisen, Försvarsmakten* och *Försvarets radioanstalt* anser att även en mer omfattande lagringsskyldighet skulle vara förenlig med EU-rätten, särskilt inom området för nationell säkerhet.

Rädda barnen och *Ecpat Sverige* påpekar att datalagring har stor betydelse för brott mot barn, särskilt sexualbrott mot barn. Även organisationer inom film-, tv- och musikbranschen – *Ifpi, Rättighetsalliansen, Dataspelsbranschen, Sveriges Biografägareförbund, Musikförläggarna, Sveriges filmuthyrareförening, Film- och TV-branschens samarbetskommitté* och *Sveriges*

Videodistributörers förening – framhåller datalagringens vikt för att upptäcka, utreda och lagföra immaterialrättsliga brott.

Datainspektionen, Journalistförbundet, Bahnhof AB, Com Hem AB, RISE SICS AB, Colt Technology Services AB, Dataskydd.net, Svenska stadsnätsföreningen, Föreningen Digitala fri- och rättigheter (Dfri), Stiftelsen för Internetsinfrastruktur och *IT&Telekomföretagen* anser att utredningens förslag även fortsättningsvis innebär en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter. I förslaget blir, trots föreslagna ändringar, lagring en huvudregel och inte ett undantag. Dessa remissinstanser anser att förslagen med största sannolikhet bryter mot EU-rätten och att det finns en risk att återigen hamna i en rättslig osäkerhet där företag åläggs nya skyldigheter som driver kostnader och blockerar utvecklingsresurser, tills det med stor sannolikhet kommer att konstateras att lagringsskyldigheten bryter mot EU-rätten och måste rivas upp. *Hi3G Access AB (Tre)* och *Telia AB* anser att det kan ifrågasättas om förslagen innebär att de svenska reglerna anpassats till de krav som EU-rätten uppställer.

Svea hovrätt, Stockholms universitet (Juridiska fakulteten), Kammarrätten i Göteborg, Göteborgs universitet (Juridiska institutionen) och *Hovrätten för Övre Norrland* anser att de ändringar som föreslagits är marginella och att förslagen även fortsättningsvis innebär en generell lagring. De bedömer att det är mycket som talar för att förslagen inte är tillräckliga för att göra regelverket fullt ut förenligt med EU-rätten.

Stockholms tingsrätt, Göteborgs tingsrätt, Säkerhets- och integritetsskyddsnämnden (SIN) och *Sveriges advokatsamfund* ställer sig bakom förslagen i huvudsak och anser att de i stort överensstämmer med EU-rätten. Även *Justitiekanslern* anser att den modell för lagring som utredningen föreslår kan antas leva upp till de EU-rättsliga krav som framgår av bl.a. Tele2-domen, under förutsättning att utredningens iakttagelser om riktad lagring är riktiga. *Svea hovrätt* och *Hovrätten för Övre Norrland* anser att frågan om riktad och differentierad lagring måste belysas och övervägas närmare och att det annars finns en överhängande risk att den svenska lagstiftningen inte kommer att uppfylla de krav som följer av unionsrätten och Europakonventionen. *Datainspektionen, Tre, Telia AB, IT&Telekomföretagen, Bahnhof AB, RISE SICS AB, Föreningen för Digitala fri- och rättigheter (Dfri)* och *Civil Rights Defenders* anser att det är en brist att utredningen inte redovisar det alternativ som EU-domstolen pekar ut som en proportionerlig lösning, nämligen riktad lagring.

Åklagarmyndigheten, Ekobrottsmyndigheten, Säkerhetspolisen, *Tullverket, Ecpat Sverige, Rädda barnen, Stockholms tingsrätt* och *Göteborgs tingsrätt* delar utredningens bedömning att riktad lagring skulle vara till ringa nytta för de brottsbekämpande myndigheterna och således inte ett gångbart alternativ.

Åklagarmyndigheten och *Säkerhetspolisen* delar utredningens bedömning att uttalandena i domskälen om en riktad lagring inte kan ses som något annat än ett exempel på hur datalagringsregler skulle kunna utformas. *Datainspektionen, Dataskydd.net, Föreningen Digitala fri- och rättigheter (Dfri), Svenska stadsnätsföreningen*, *Bahnhof AB, Svea hovrätt, Umeå universitet (Juridiska institutionen)* och *Hovrätten för Övre Norrland* delar inte

utredningens bedömning att EU-domstolens uttalanden om riktad lagring skulle vara ett s.k. obiter dictum. *Svea hovrätt* anser att detta resonemang är EU-rättsligt främmande och att detta särskilt gäller när det som här är fråga om en dom som har meddelats med anledning av en begäran om förhandsavgörande.

Skälen för regeringens bedömning

EU-domstolens uttalanden om lagringsskyldigheten i Tele2-domen

Som framgår i föregående avsnitt anser EU-domstolen i Tele2-domen att direktiv 2002/58 är tillämpligt på de svenska reglerna om datalagring. Artikel 15.1 i direktivet, som i viss utsträckning tillåter datalagring för t.ex. brottsbekämpande syften, ska enligt domstolen tolkas strikt och mot bakgrund av EU:s rättighetsstadga.

Enligt artikel 52.1 i EU:s rättighetsstadga 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 (punkt 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. 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 (punkt 96 i domen).

När det gäller frågan om den svenska lagstiftningen uppfyller kraven på proportionalitet, anför 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 (punkt 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 (punkt 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 (punkt 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 (punkt 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 (punkt 101 i domen).

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, anför EU-domstolen att endast bekämpning av grov brottslighet kan motivera en sådan åtgärd (punkt 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. Trots att 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 (punkt 103 i domen). En sådan lagstiftning skulle få till följd att lagringen av trafik- och lokaliseringsuppgifter blir huvudregeln, trots att direktiv 2002/58 kräver att en sådan lagring ska vara ett undantag.

EU-domstolen anför att den svenska lagstiftningen omfattar samtliga abonnenter och avser samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter, och att det inte görs några åtskillnader, 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 finns 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 (punkt 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 (punkt 106 i domen).

EU-domstolen finner sammanfattningsvis 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 EU:s rättighetsstadga (punkt 107 i domen).

Domstolen anför 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 (punkt 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 (punkt 109 i domen).

Vad 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 (punkt 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 när behöriga myndigheter 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 (punkt 111 i domen).

Effektiva verktyg för brottsbekämpningen behövs även framöver

Mot bakgrund av EU-domstolens slutsatser i Tele2-domen kan det konstateras att EU-rätten ställer strängare krav på lagringen av uppgifter än vad svensk rätt gör. Svensk rätt behöver således anpassas för att vara förenlig med EU-rätten. Ett sätt att hantera detta på skulle kunna vara att upphäva de bestämmelser som föreskriver att operatörerna ska lagra uppgifter om elektronisk kommunikation. En sådan lösning är emellertid utesluten av både brottsbekämpande och folkrättsliga skäl.

Under senare år har den ökande internationaliseringen i kombination med teknikutvecklingen och en tilltagande internetanvändning inneburit att kriminaliteten delvis har ändrat karaktär. Internet erbjuder lättillgängliga kontaktytor för brottsplanering inom och utom landets gränser och utgör bl.a. en etablerad plattform för våldsbejakande extremism och terrorismpropaganda. Viss typ av kriminalitet, t.ex. barnpornografibrott, begås ofta med hjälp av it-verktyg och elektroniska kommunikationsnät, t.ex. via internet, och den webbaserade narkotikahandeln har ökat massivt de senaste åren. Utvecklingen innebär att 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. Om de brottsbekämpande myndigheterna inte skulle ha tillgång till adekvata utredningsverktyg i den elektroniska miljön skulle brotten i vissa fall vara omöjliga att klara upp och brottsoffer i motsvarande omfattning vara rättslösa. 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 enligt t.ex. Europakonventionen. 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. Detta följer bl.a. av artikel 8 i Europakonventionen (se t.ex. Europadomstolens mål Söderman mot Sverige, 12 november 2013, punkt 78 och von Hannover mot Tyskland, 24 juni 2004, punkt 57). Motsvarande skydd följer av EU:s rättighetsstadga inom EU-rättens tillämpningsområde (artikel 6, 7 och 52.3 i

stadgan). Även om det inte har förekommit något ingripande från en myndighet eller en offentlig tjänsteman kan staten alltså bryta mot artikel 8 i Europakonventionen 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 intrånget i någon enskilds rättighet har utförts av någon annan enskild, 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. 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 det enligt den nationella lagstiftningen inte var möjligt att inhämta uppgift om vem som använt en ip-adress från operatören. I det aktuella fallet uttalade Europadomstolen särskilt att konfidentialitet för kommunikation och yttrandefrihet ibland måste få vika för brottsbekämpande ändamål. (K.U. mot Finland, 2 december 2008, mål nr 2872/02 särskilt punkt 49). Statens skyldighet att upprätthålla ett straffrättsligt skydd och göra skyndsamma ingripanden mot allvarliga brott följer även av andra artiklar i Europakonventionen och EU:s rättighetsstadga, exempelvis avseende frihetsberövanden, artikel 5 i Europakonventionen samt artiklarna 6 och 52.3 i EU:s rättighetsstadga (se även Hans Danelius, Mänskliga rättigheter i Europeisk praxis, 5:e uppl. s. 112 och punkt 42 i Digital Rights-domen). Sveriges folkrättsliga åtaganden skulle således riskera att inte uppfyllas om de brottsbekämpande myndigheterna inte ges 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 t.ex. 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 artikel 30 i 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 åtaganden enligt konventionen.

Tillgång till uppgifter om elektronisk kommunikation är också ett sätt för de brottsbekämpande myndigheterna att vid brottsmisstankar kunna kontrollera misstanken på ett så effektivt sätt som möjligt och med minsta möjliga integritetsintrång för den berörda personen. Detta är viktigt för att åstadkomma en ändamålsenlig tillämpning av behovsprincipen och

proportionalitetsprincipen som enligt svensk rätt gäller för all användning av tvångsmedel. Tvångsmedel får nämligen endast användas 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 det intrång eller men som åtgärden innebär. Om de brottsbekämpande myndigheterna inte skulle ha möjlighet att få tillgång till uppgifter om elektronisk kommunikation i brottsutredningar kan de behöva använda sig av andra metoder som kan vara mer ingripande ur ett integritetsperspektiv. 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 personen till den aktuella platsen (eller ge honom eller henne alibi). Om polis och åklagare inte skulle ges möjlighet att ta del av dessa uppgifter kan de, i enlighet med det ovan anförda, inte lägga ned förundersökningen utan måste i stället arbeta vidare med de andra metoder som står till buds. En sådan metod är t.ex. hemlig avlyssning av elektronisk kommunikation. Det innebär alltså att frånvaron av möjlighet att inhämta lokaliseringsuppgifter skulle kunna leda till ett ännu allvarligare integritetsintrång (avlyssning) för den enskilde, vilket framstår som mindre lämpligt i förhållande till behovs- och proportionalitetsprinciperna.

Sammanfattningsvis kan det således konstateras att det även i fortsättningen behövs effektiva verktyg för den brottsbekämpande verksamheten och att ett av dessa verktyg är lagring och tillgång till uppgifter om elektronisk kommunikation. Reglerna måste vara förenliga med både EU-rätten och andra internationella förpliktelser. Mot bakgrund av att EU-domstolen i Tele2-domen funnit att de svenska reglerna inte uppfyller EU-rättens krav behöver den svenska regleringen anpassas till vad som krävs när det gäller skyddet mot statens ingrepp i den personliga integriteten. I detta avseende ska den EU-rättsliga proportionalitetsprincipen iakttas, enligt vilken skyddet av den grundläggande rätten till respekt för privatlivet kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt. Samtidigt måste lagstiftningen tillgodose Sveriges positiva förpliktelser enligt bl.a. Europakonventionen att skydda enskilda från ingrepp i de grundläggande fri- och rättigheterna från andra enskilda. Hur balansen mellan dessa olika skyldigheter bör göras utvecklas i det följande.

Samtliga trafikuppgifter och lokaliseringsuppgifter lagras inte enligt dagens regelverk

När det gäller lagringens omfattning slår EU-domstolen fast att EU:s rättighetsstadga 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 (punkt 1 i domslutet).

När det gäller uttrycket ”samtliga trafikuppgifter och lokaliserings-uppgifter ” kan det – som utredningen och några remissinstanser påpekar –

noteras att flera trafik- och lokaliseringsuppgifter inte ska lagras enligt den nu gällande svenska lagstiftningen, som har sin grund i det numera upphävda datalagringsdirektivet. Exempel på sådana uppgifter är 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, uppgift om port vid internetåtkomst, 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 några rena lokaliseringsuppgifter, dvs. positioner som inte är kopplade till kommunikation, inte lagras. Det är således långt ifrån samtliga trafik- och lokaliseringsuppgifter som omfattas av lagringsskyldigheten.

Även om det inte har någon bäring på vad som utgör trafik- och lokaliseringsuppgifter enligt direktiv 2002/58, kan det också noteras att kommunikationsmönstren på senare tid alltmer har övergått till sådana tjänster som inte ger upphov till någon lagringsskyldighet hos operatörerna, dvs. till tjänster som inte tillhandahålls av en lagringsskyldig operatör utan av andra tjänsteleverantörer som t.ex. Apple I-message och Facetime, Facebook Messenger, Skype, G-mail och Hotmail. Lagringsskyldigheten omfattar inte heller uppgifter om samtal med annat än vanliga telefonnummer, t.ex. appar som möjliggör samtal med användarnamn. Lagringsskyldigheten omfattar inte heller t.ex. webbplatsbesök (surfning), sökningar med sökmotorer, onlinespel eller uppgifter om filöverföring med hjälp av filöverföringsprotokoll (File Transfer Protocol, FTP).

Trots att det alltså är långt ifrån samtliga trafik- och lokaliseringsuppgifter som omfattas av lagringsskyldigheten, innebär den svenska lagstiftningens utformning en alltför omfattande lagringsskyldighet. Det är således inte möjligt att lämna de svenska lagringsreglerna oförändrade som vissa remissinstanser förespråkar. Däremot anser regeringen att EU-domstolens slutsatser bör kunna tolkas i ljuset av tolkningsfrågorna och mot bakgrund av utvecklingen av alternativa kommunikationstjänster. För att kunna avgöra lagringens proportionalitet behöver nämligen helheten beaktas.

Lagringens omfattning behöver begränsas

Av Tele2-domens domslut framgår att EU-rätten hindrar 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.

I domskälen motsvaras denna slutsats av det resonemang som domstolen för i punkterna 97–107 och som 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 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. 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. EU-domstolens slutsats är att en sådan lagstiftning utgör ingrepp i de rättigheter som följer av EU:s rättighetsstadga och att därför endast grov brottslighet kan motivera lagring. Dock kan inte ens grov brottslighet i sig ensamt motivera en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter. 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 och att lagringen inte är begränsad till tid, geografiskt område eller krets av personer.

Domstolens slutsats 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 EU:s rättighetsstadga. Denna slutsats är också den som finns i domslutet.

Domstolen resonerar kring hur en möjlig nationell lagstiftning angående datalagring skulle kunna se ut. Resonemanget i denna del handlar om s.k. riktad lagring. Det anförs 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 (punkt 108). För att uppfylla kraven behöver den nationella lagstiftningen föreskriva tydliga och precisa bestämmelser som reglerar omfattningen och tillämpligheten av en lagringsåtgärd och som slår fast minimikrav, så att de personer vars uppgifter lagrats har garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk (punkt 109). Även om villkoren kan variera utifrån vilka åtgärder som vidtas för att förebygga, undersöka, avslöja och väcka åtal för grov brottslighet, måste lagringen alltid uppfylla objektiva kriterier som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträvade syftet. Enligt domstolen behöver villkoren vara sådana att de klart avgränsar åtgärdens omfattning och följaktligen den berörda personkretsen (punkt 110). När det gäller den berörda personkretsen och de situationer som det kan handla om uttalar domstolen att 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 på annat sätt bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten. En sådan avgränsning skulle, enligt domstolen, kunna säkerställas genom att lagring sker inom särskilt brottsutsatta geografiska områden (punkt 111).

Några remissinstanser, t.ex. *Bahnhof AB, Föreningen för Digitala fri- och rättigheter* och *Dataskydd.net,* anför att endast en riktad lagring skulle vara förenlig med EU-rätten eftersom EU-domstolen i Tele2-domen uttalat att villkoren för den nationella lagringen måste vara sådana att de klart

avgränsar åtgärdens omfattning och följaktligen den berörda personkretsen. *Svea hovrätt* anser att utredningens resonemang om att domstolens skrivningar om riktad lagring endast är ett exempel på en tillåten lagringsform, är EU-rättsligt främmande. Enligt regeringen är dock domstolens skrivningar om riktad lagring, som bl.a. *Åklagarmyndigheten* anför, just att se som en möjlig form av lagring. Att på angivet sätt dra slutsatser om tolkningen av en dom från EU-domstolen är inget främmande utan väl förenligt med hur den nationella lagstiftaren förutsätts verka inom ramen för EU-rätten. Uttalandena om avgränsning av den berörda personkretsen, t.ex. genom ett geografiskt kriterium, tar, enligt regeringens uppfattning, sikte på denna riktade lagring och således inte generellt på hur nationell lagstiftning om lagring måste vara utformad.

I detta sammanhang kan det vidare noteras att EU-domstolen efter Tele2-domen i en näraliggande fråga har accepterat att lagring som sker i brottsbekämpande syfte av flygbolags passageraruppgifter omfattar samtliga flygpassagerare och således inte är riktad till sådana passagerare om vilka det förelåg någon misstanke att de kunde hota den allmänna säkerheten (EU-domstolens yttrande 1/15, den 26 juli 2017 punkterna 41, 186 och 189). I yttrandet konstaterar domstolen att behandlingen av samtliga passagerares personuppgifter syftar till att identifiera den risk för säkerheten som vissa personer skulle utgöra, vilket inte vid lagringen är känt för myndigheterna. Att utesluta vissa personer eller vissa ursprungsområden skulle, enligt domstolen, kunna utgöra hinder för uppnåendet av ändamålet med behandlingen av uppgifterna, nämligen identifieringen bland samtliga passagerare av de personer som kan utgöra risk för den allmänna säkerheten, och skulle kunna göra det möjligt att kringgå kontrollen. Trots att yttrandet endast tar sikte på registrering av passageraruppgifter och således inte avser samma situation som lagring av uppgifter om elektronisk kommunikation, anser regeringen att EU-domstolens övergripande resonemang i yttrandet även kan vara av visst intresse för lagring av uppgifter om elektronisk kommunikation i brottsbekämpande syfte. Om lagringen skulle riktas mot vissa i förväg utpekade personkretsar eller geografiska områden skulle nämligen syftet med lagringen kunna förfelas eftersom det inte på förhand går att veta av vem, var eller när ett brott kommer att begås.

Vid sitt konstaterande att den svenska regleringen avseende datalagring inte är förenlig med EU:s rättighetsstadga betonar EU-domstolen i Tele2-målet på flera ställen att det är just den allomfattande generella 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. Sammanfattningsvis innebär domen alltså att en generell och odifferentierad lagring inte är tillåten enligt EU-rätten. Eftersom EU-domstolen har ansett att den svenska lagringen föreskriver en sådan generell lagring måste de svenska lagringsreglerna göras mindre omfattande. Ett sätt att göra det på är att införa ett system med s.k. riktad lagring (se mer om detta nedan). Domen utesluter emellertid inte andra former av datalagring, så länge skyldigheten att lagra inte blir huvudregel och den i varje del begränsas till vad som är strängt nödvändigt.

Datalagringsutredningen (SOU 2015:31), som kom med sitt betänkande efter Digital Rights-domen men före Tele2-domen, bedömde att det inte behövde göras några förändringar av lagringsskyldighetens omfattning. Med anledning av Tele2-domens uttalanden gällande den svenska regleringen får denna bedömning anses ha förlorat sin aktualitet. Regeringen redogör därför inte särskilt för de remissvar som kommit in med anledning av Datalagrings-utredningens bedömning i denna fråga.

En riktad lagring bör inte införas

Som framgår ovan har EU-domstolen uttalat sig om riktad lagring som en möjlig form av lagring. Riktad lagring innebär en situationsanpassad förebyggande lagring av uppgifter hänförliga till vissa personer, nummer, kommunikationsutrustningar eller platser. Frågan är om en sådan lagring bör införas i Sverige. Utredningen kommer fram till att en riktad lagring skulle vara till ringa nytta för de brottsbekämpande myndigheterna och lämnar därför inget förslag på en sådan lagring. Denna bedömning får stöd från flera remissinstanser, bl.a. *Åklagarmyndigheten, Säkerhetspolisen*, *Tullverket, Stockholms tingsrätt* och *Rädda barnen*. Andra remissinstanser, t.ex. *Datainspektionen, Svea hovrätt, IT&Telekomföretagen, Bahnhof AB* och *Civil Rights Defenders*, anser dock att frågan om riktad lagring behöver belysas och övervägas närmare och efterlyser en mer ingående analys av förutsättningarna att införa ett system med riktad lagring.

Vid analysen av denna fråga måste nyttan och behovet av en riktad lagring vägas mot intrånget för de berörda personerna.

När det gäller nyttan och behovet av en riktad lagring kan det konstateras att det är komplicerat att med någon större precision i förväg veta hur man ska rikta lagringen. Det är t.ex. svårt att veta vilka som kan komma att begå olaga hot över internet, barnpornografibrott eller misshandel. När det gäller den brottsbekämpande verksamheten syftar datalagring framför allt till att i efterhand, när ett brott har begåtts, kunna få ta del av information som t.ex. kan klarlägga händelser som anknyter såväl till själva brottstillfället som till planläggningen och flykten från brottsplatsen. Dessa uppgifter syftar bl.a. till att kunna ta reda på vem eller vilka som kan misstänkas för brottet eller för att kunna avföra sådana misstankar. Att i förväg ringa in vissa personer eller vissa områden skulle alltså, som framhålls i det föregående, innebära en påtaglig risk för att ändamålet med lagringen skulle hindras, eftersom det inte på förhand går att veta av vem, var eller när ett brott kommer att begås.

När det gäller frågan om riktad lagring gentemot vissa personer har Europadomstolen i ett mål om bl.a. avlyssning av mängddata (eng. bulk interception) i underrättelseverksamhet, gjort vissa uttalanden som också kan vara relevanta i detta sammanhang. Europadomstolen ansåg i målet att det inte är lämpligt att kräva att det ska finnas en viss misstankegrad (eng. reasonable suspicion) mot de personer som information får hämtas från, något som klagandena hade gjort gällande borde införas. Domstolen uttalade att det vore fel att automatiskt förutsätta att avlyssning av mängddata skulle innebära ett större intrång i privatlivet än en riktad avlyssning mot misstänkta personer, eftersom den senare till sin natur mer sannolikt skulle resultera i inhämtning och undersökning av stora mängder data gällande den ifrågavarande personens kommunikationer. Avlyssning av mängddata är också per definition inte riktad, och att kräva att det ska finnas en viss misstankegrad gentemot den avlyssnade skulle, enligt domstolen, omöjliggöra ett sådant system (Big Brother Watch m.fl. mot Förenade Kungariket, 13 september 2018, mål nr 58170/13, 62322/14 och 24960/15, punkterna 316–317). Europadomstolen beslutade den 4 februari 2019 att målet – som rör en rad olika frågor om avlyssning och inhämtning av mängddata – ska prövas i stor sammansättning, s.k. stor kammare (eng. Grand Chamber).

När det gäller en riktad lagring som begränsar sig till vissa geografiska områden skulle det innebära att förutsättningarna för att lösa allvarlig brottslighet blir olika för olika delar av landet, vilket skulle vara mycket problematiskt. Att införa ett regelverk som får till följd att allvarliga brott skulle bli väsentligt svårare, och i vissa fall kanske omöjliga, att klara upp beroende på var själva brottet begicks eller planerades är enligt regeringens mening oacceptabelt. Det skulle också kunna innebära att viss brottslighet anpassar sig till detta och förläggs på en plats där lagring inte sker i syfte att förhindra eller försvåra upptäckt. En geografisk avgränsning är också problematisk vid sådan brottslighet som inte kan sägas vara kopplad till geografiska förhållanden överhuvudtaget, t.ex. internetrelaterad brottslighet. I vissa fall kan det dock vara så att brottsrisken ökar i ett visst område vid speciella händelser, t.ex. vid statsbesök, högnivåmöten eller större evenemang som innebär att många människor samlas på en och samma plats. I sådana fall skulle man kunna tänka sig en riktad lagring kring den plats där mötet eller evenemanget ska äga rum. Dock är värdet av en sådan lagring inte särskilt stort. 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.

Man skulle även kunna tänka sig en lagring som bara riktar sig mot personer som använder vissa specifika tekniker, t.ex. lagring av elektronisk kommunikation avseende personer som använder vissa mjukvaror för anonymisering. Problemet med en sådan lagring är att den skulle fånga in en försvinnande liten del av de uppgifter som är nödvändiga för brottsbekämpningen. Dessutom skulle det innebära ett större integritetsintrång för

den enskilde eftersom man skulle behöva ta del av vilken mjukvara som personen använder för kommunikationen.

I likhet med utredningen och bl.a. *Åklagarmyndigheten, Säkerhetspolisen* och *Tullverket*, kan regeringen mot bakgrund av det anförda inte se någon större praktisk nytta eller något större behov av riktad lagring. Dessutom är det inte säkert att en riktad lagring innebär integritetsvinster.

När det gäller 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), utan att det finns någon konkret misstanke mot dessa personer, innebär rimligen en än större rättighetskränkning mot dessa människor och skulle riskera att vara diskriminerande mot vissa grupper, vilket också påpekas av *Diskrimineringsombudsmannen* och *Civil Rights Defenders*. Vid sådan lagring måste nämligen vissa personer eller personkategorier pekas ut som mer brottsbenägna än andra så att lagring av just deras uppgifter ska utföras. Regeringen har svårt att se hur en sådan urvalsprocess i praktiken ska kunna ske på objektiva grunder. Tvärtom torde risken för diskriminering eller i övrigt stötande effekter vara stor.

Utöver den ovan redovisade bristande ändamålsenligheten och proportionaliteten, är riktad lagring förknippad med ett annat problem. Om man ska rikta lagringen mot vissa tider eller områden måste operatörerna underrättas om detta beslut så att rätt uppgifter kan lagras. Antalet operatörer överstiger 500 stycken. Även om antalet mobiloperatörer, som i första hand torde beröras av en riktad lagring, är väsentligt färre och står för en mycket stor marknadsandel, riskerar en underrättelse att behöva gå till många operatörer. Det skulle bli en praktiskt utmanande uppgift samtidigt som uppgiften om att ett visst område eller vissa personer är av intresse för den brottsbekämpande verksamheten skulle spridas till en alltför stor krets av personer. Det är särskilt problematiskt i underrättelseverksamheten där kraven på sekretess är särskilt stora.

Sammantaget anser regeringen att en riktad lagring till en viss personkrets, ett visst geografiskt område eller till personer som använder vissa specifika tekniker vid en första anblick kan framstå som en lösning som är rimlig med hänsyn till avvägningen mellan integritetsintrånget och effektiviteten i brottsbekämpningen. Som framgår ovan innebär dock en sådan riktad lagring varken en ändamålsenlig, proportionerlig eller lämplig lösning. Regeringen lämnar därför inget förslag på en sådan lagring. Av de skäl som utredningen anför anser regeringen inte heller att lagring i form av bevarandeföreläggande, kryptering eller lagring av senaste abonnemangsaktivitet skulle vara en framkomlig väg i detta sammanhang. Den enda rimliga kvarvarande modellen är enligt regeringen i stället en lagringsskyldighet som inte omfattar alla kommunikationssätt, som är mindre omfattande än i dag och som är anpassad efter vad som är strängt nödvändigt för att bekämpa grov brottslighet. Hur en sådan begränsad lagringsmodell kan utformas utvecklas nedan.

En begränsad lagringsskyldighet bör gälla framöver

Enligt utredningen bör lagringsskyldigheten begränsas på så vis att endast sådana uppgiftskategorier som är påtagligt viktiga för brottsbekämpningen och som inte är möjliga att få del av genom en mindre ingripande åtgärd ska lagras. Både informationen och lagringen måste alltså vara nödvändiga. Lagringen får således inte omfatta uppgifter som sällan eller aldrig inhämtas eller för vilka nyttan eller behovet inte är stort. Det är inte heller tillräckligt att den lagrade uppgiften allmänt sett är användbar eller bra att ha för de brottsbekämpande myndigheterna. 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 begränsad och differentierad, dvs. i varje del anpassad efter vad som är strängt nödvändigt. Regeringen delar denna bedömning och anser att en sådan lagring är förenlig med EU-rätten.

Flera av de brottsbekämpande myndigheterna, t.ex. *Polismyndigheten, Åklagarmyndigheten, Säkerhetspolisen* och *Tullverket,* påpekar att de allra flesta uppgifter som omfattas av lagringsskyldigheten i dag är till stor nytta för brottsbekämpningen och att varje begränsning i lagringsskyldigheten skulle innebära att möjligheten att bekämpa grov brottslighet försämras. Regeringen ifrågasätter inte denna bedömning men vill samtidigt framhålla att en begränsad och proportionerlig lagringsskyldighet som är förenlig med EU-rätten gör det möjligt att behålla datalagring som verktyg för de brottsbekämpande myndigheterna. En lagringsskyldighet som inte är förenlig med EU-rätten och andra grundläggande rättigheter kommer, som bl.a. *IT&Telekomföretagen* och *Svenska stadsnätsföreningen* påpekar, inte att kunna tillämpas och skulle alltså innebära att inga uppgifter lagras i syfte att bekämpa brott. En begränsad lagringsskyldighet kan således öka förmågan för de brottsbekämpande myndigheterna att förhindra och utreda allvarliga brott, skydda nationella säkerhetsintressen och göra Sverige till ett säkrare land att vistas i.

Säkerhetspolisen, Åklagarmyndigheten, Ekobrottsmyndigheten och *Tullverket* påpekar att en begränsning av vilka uppgifter som lagras riskerar att bli handlingsdirigerande för den brottsbenägne. Det argumentet har emellertid inte den tyngd som det framstår vid ett första påseende. Redan i dag är lagringen så pass 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. Påverkan på möjligheterna att utreda brott där dessa personer är inblandade torde alltså inte bli så stor. 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.

Sammanfattningsvis anser regeringen att en sådan begränsad lagringsskyldighet som beskrivs ovan framstår som det lämpligaste sättet att uppnå ett system som överensstämmer med EU-rätten och som beaktar såväl integritetsintressena som behovet av en effektiv brottsbekämpning. Vilka uppgifter som bör lagras inom ramen för ett sådant system redovisas i det följande.

5.3 Vilka uppgifter bör lagras fortsättningsvis?

Regeringens förslag: Lagringsskyldigheten enligt lagen om elektronisk kommunikation ska inte längre omfatta uppgifter

- vid telefoni eller meddelandehantering som sker helt inom det fasta telefoninätet eller genom fasta internetanslutningar
- om nummer som samtal styrts till (dvs. vidarekopplade samtal)
- om tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform).

Regeringens bedömning: Lagringsskyldigheten enligt lagen om elektronisk kommunikation bör även fortsättningsvis omfatta uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, målet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.

Skyldigheten att lagra ovanstående uppgifter bör även i fortsättningen omfatta uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt samt vid internetåtkomst. Även vid en misslyckad uppringning bör det gälla en skyldighet att lagra uppgifter som genereras eller behandlas.

Lagringsskyldighetens ramar bör även fortsättningsvis framgå av lag och de mer detaljerade föreskrifterna bör meddelas i förordning eller, efter regeringens bemyndigande, i myndighetsföreskrifter.

Utredningens bedömning och förslag överensstämmer huvudsakligen med regeringens. Utredningen bedömer att samtliga författningsändringar som behöver göras med anledning av att vissa uppgiftskategorier inte längre bör omfattas av lagringsskyldigheten kan göras genom ändringar i förordningen om elektronisk kommunikation.

Remissinstanserna: *Åklagarmyndigheten* har ingen invändning mot utredningens bedömning av vilka uppgifter och kommunikationsmedel som i förhållande till den ursprungliga lagringsskyldigheten är mindre värdefulla för brottsutredningar. Det framstår enligt myndigheten t.ex. som självklart att mobiltelefonin är mer angelägen att kunna följa än den fasta telefonin.

Tele2 Sverige AB tillstyrker att uppgifter hänförliga till fasta telefonitjänster undantas från lagringsskyldigheten eftersom detta skulle innebära en anpassning till EU-domstolens krav. *Ekobrottsmyndigheten, Säkerhetspolisen, Polismyndigheten, Skatteverket* och *Tullverket* anser att borttagandet av lagring gällande fast telefoni, inklusive ip-telefoni, kommer att leda till negativa konsekvenser för brottsbekämpningen. *Polismyndigheten* anser att om man gör skillnad på fast och mobil telefon respektive fasta och mobila anslutningspunkter riskerar det föra med sig svårigheter att rekonstruera en trafikväg men också att kunna knyta en person till en viss plats vid en viss tid. *Säkerhetspolisen* påpekar att det kan innebära svåra gränsdragningar mellan vad som är en fast respektive en mobil anslutningspunkt. Ip-telefoni kan t.ex. användas från såväl fast telefon som mobiltelefon. *Hi3G Access AB* är inne på samma linje och avstyrker därför förslaget eftersom det skulle göra regleringen mindre teknikneutral och inte beakta den konvergens mellan fast och mobil telefoni som pågått ett antal år och som kommer öka ytterligare framöver. Även *Göteborgs tingsrätt* ifrågasätter om förslaget främjar ett långsiktigt och hållbart regelverk eftersom teknikutvecklingen innebär att gränsen mellan fast och mobil anslutningspunkt alltmer kommer att suddas ut.

Hi3G Access AB anser att förslaget att ta bort lagringen av vissa uppgifter vid samtal och meddelanden, bl.a. uppgifter om vidarekoppling, om vilken tjänst som använts samt datum och spårbar tid för på- och avloggning i tjänsten, innebär att lagstiftningen blir mer proportionerlig. *Åklagarmyndigheten, Säkerhetspolisen, Tullverket, Ecpat Sverige* och *Rädda barnen* anser att uppgift om lokalisering vid meddelandehantering såsom sms, också måste anses vara en sådan uppgift som är strängt nödvändig att lagra. Dessa uppgifter är minst lika viktiga som lokaliseringsuppgifter vid samtal.

Åklagarmyndigheten, Polismyndigheten, Säkerhetspolisen, Tullverket, Ecpat Sverige, Rädda Barnen, IFPI Sverige, Rättighetsalliansen, Dataspelsbranschen, Sveriges Biografägareförbund, Musikförläggarna, Sveriges filmuthyrareförening, Film- och TV-branschens samarbetskommitté och *Sveriges Videodistributörers förening* välkomnar förslaget om att möjliggöra identifiering av slutanvändare vid internetåtkomst genom s.k. NAT-teknik. *Åklagarmyndigheten* anser att förslaget innebär en ändamålsenlig uppdatering och att reglerna blir teknikneutrala. Genom förslaget motverkas den tilltagande anonymiseringen på internet som kriminella personer på senare år i ökad utsträckning har kunnat dölja sig bakom. *Ecpat Sverige* betonar problemet med NAT-tekniken i ärenden om sexuella övergrepp mot barn och att polisen i dag har mycket svårt att identifiera slutanvändaren i dessa fall. Även *Hi3G Access AB* är positiv till förslaget eftersom det är viktigt att de uppgifter som måste lagras också faktiskt kan användas för att bekämpa brott. *Post- och Telestyrelsen (PTS)* ser positivt på en reglering som möter problematiken med att det i dag är valet av teknisk lösning som avgör om det går att spåra källan till en kommunikation på internet. PTS påpekar dock att mängden uppgifter som lagras kommer att öka betydligt för de operatörer som använder NAT-teknik. Ur ett integritetsperspektiv kan denna lagring vara känslig eftersom uppgifter om varje internetsession i praktiken

kommer att behöva lagras. *Netnod Internet Exchange i Sverige AB*, *RISE SICS AB*, *Telia AB, Svenska stadsnätsföreningen, Dataskydd.net, Colt Technology Services AB* och *The Business Carrier Coalition (BCC)* anför att förslaget om att NAT-adresser ska lagras kommer innebära att mycket stor mängd data kommer att behöva lagras. Mot bakgrund av osäkerheten kring förslagets förenlighet med EU-rätten bör en kraftigt utökad lagring inte införas. *Umeå universitet (Juridiska institutionen)* anser att det är olämpligt att utvidga lagringsskyldigheten gällande NAT-tekniken. Skrivningen möjliggör en långtgående lagringsskyldighet och delegation av normgivningsmakt på ett område som påtagligt påverkar individens rättighetsskydd. *Datainspektionen* anser att det är oklart hur förslaget om att internetåtkomst ska vara teknikneutralt kommer att påverka anonymiseringstjänster och VPN-tunnlar som tillhandahålls av operatörerna. Inspektionen anför att det är oklart hur långtgående effekten av en sådan bestämmelse kan bli.

Skälen för regeringens förslag och bedömning

Lagringsskyldighetens rättsliga struktur

Som framgår i föregående avsnitt anser regeringen, i likhet med utredningen, att nuvarande modell för lagringsskyldigheten bör anpassas för telefonitjänst, meddelandehantering och internetåtkomst genom att vissa uppgiftsslag inom dessa kategorier tas bort från lagringsskyldigheten. Samtidigt bör lagringstiderna differentieras utifrån skillnader i behov och uppgifternas integritetskänslighet, vilket regeringen återkommer till i avsnitt 5.4. Innan regeringen går in på vilka förändringar som nu bör göras i regelverket bör det dock inledningsvis betonas att området för elektronisk kommunikation är i ständig förändring med nya kommunikationstjänster som tillkommer samtidigt som andra tjänster försvinner eller används mindre. Dessa nya tjänster leder till nya kommunikationsmönster hos användarna. Det leder i sin tur till att bedömningen av vad som är strängt nödvändigt att lagra kan förändras över tid. Det är alltså nödvändigt att utvärdera regelverket kring lagringsskyldigheten i takt med sådana förändringar, dels för att enskilda inte ska utsättas för lagring som inte längre är strängt nödvändig, dels för att de brottsbekämpande myndigheterna måste kunna bibehålla sin brottsutredande förmåga även när tekniken utvecklas. Som framgår i avsnitt 10 anser regeringen därför att regelverket bör ses över senast inom fyra år från ikraftträdandet av nu föreslagna ändringar.

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Inskränkningar genom lag är tillåtna enligt de förutsättningar som anges i 2 kap. 20–22 §§ regeringsformen. Det innebär bl.a. att en begränsning av rätten till skydd för den personliga integriteten är tillåten endast under förutsättning att den tillgodoser ett ändamål som är godtagbart i ett demokratiskt samhälle. Det innebär också att en begränsning inte får gå utöver vad som är nödvändigt med hänsyn till det ändamål som

har föranlett den eller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen.

Lagringsskyldighetens omfattning anges i lagen om elektronisk kommunikation (6 kap. 16 a §), medan den tekniska beskrivningen av vad som ska lagras anges i förordningen om elektronisk kommunikation (39–43 §§). Förhållandet mellan vad som med hänsyn till integritetsintrånget bör regleras i lag respektive i förordning var föremål för överväganden i samband med att datalagringsbestämmelserna infördes (prop. 2010/11:46 s. 19–20 och 28). Regeringen bedömde att principen bör vara att lagringsskyldighetens omfattning bör regleras i lag, men däremot inte den mer tekniska specifikationen av lagringskravet, som i stället kunde regleras i förordning. I lagen anges därför vilka teknikområden som omfattas av lagringsskyldigheten, t.ex. telefonitjänst, och ändamålet med lagringen, t.ex. identifiera eller spåra en kommunikationskälla. Den tekniska beskrivningen av vad som ska lagras anges genom verkställighetsföreskrifter i förordning. Denna ordning bedömdes vid införandet av datalagringsbestämmelserna vara förenlig med regeringsformens skydd av den personliga integriteten. Regeringen gör inte någon annan bedömning nu.

Utredningen anser att samtliga författningsändringar som behöver göras med anledning av att vissa uppgiftskategorier inte längre bör omfattas av lagringsskyldigheten bör göras i förordningen om elektronisk kommunikation. För att lagringsskyldighetens ramar även fortsättningsvis ska framgå av lag gör emellertid regeringen bedömningen att vissa av de ändringar som utredningen föreslår bör göras i lagen om elektronisk kommunikation. Det gäller t.ex. den föreslagna ändringen om att kommunikation som sker helt i det fasta nätet ska tas bort från lagringsskyldigheten, vilket innebär att 6 kap. 16 a § lagen om elektronisk kommunikation bör ändras så att det av lagen framgår att det endast är telefonitjänst och meddelandehantering via mobil nätanslutningspunkt som får lagras framöver (se mer nedan). I likhet med vad som är fallet i dag kan emellertid de mer detaljerade specifikationerna av lagringskravet även fortsättningsvis göras i förordning. Den författningsmässiga strukturen, där riksdagen beslutar ramarna för datalagringen och regeringen den mer exakta utformningen, bör således behållas. Regeringen redogör nedan närmare för lagringens föreslagna omfattning vad gäller dels telefonitjänst och meddelandehantering, dels internetåtkomst.

Telefonitjänst och meddelandehantering

Enligt 6 kap. 16 a § lagen om elektronisk kommunikation ska uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering lagras. Utredningen föreslår att endast uppgifter om kommunikation via en mobil nätanslutningspunkt bör lagras framöver. Det betyder att det inte lagras några uppgifter om telefonitjänster eller meddelandehantering som sker helt inom det fasta telefonnätet eller genom fasta internetanslutningar enligt datalagringsreglerna. Om någon av parterna kommunicerar via en mobil nätanslutningspunkt bör däremot information lagras, men bara hos den

partens operatör. Regeringen delar utredningens bedömning i denna del. Såsom flera av de brottsbekämpande myndigheterna – t.ex. *Ekobrottsmyndigheten, Polismyndigheten, Skatteverket* och *Tullverket* – påpekar kommer borttagandet av lagring gällande den s.k. fasta telefonin påverka statens möjligheter att utreda allvarlig brottslighet. Samtidigt kan det konstateras att det av tidigare analyser framgår att det nästan uteslutande är uppgifter hänförliga till mobiltelefontrafik som inhämtas (se t.ex. SOU 2015:31 s. 215, 253 och 262 och SOU 2012:44 s. 389, 447–447, 462 och 514). Enligt de brottskämpande myndigheterna är denna bild fortfarande korrekt, även om det också förekommer inhämtning från det fasta nätet. Mot denna bakgrund framstår det inte som strängt nödvändigt att lagra telefoni- och meddelandeuppgifter hänförliga till annat än tjänster via en mobil nätanslutningspunkt. Härtill kommer att den fasta telefonin typiskt sett används av fler personer än en mobiltelefon som oftast är personlig. Integritetsintrånget vid lagring av uppgifter knutna till mobiltelefoner är därmed fokuserat till en snävare personkrets och det totala integritetsintrånget blir således mindre vid varje lagringstillfälle. En lagringsskyldighet som endast omfattar trafik via en mobil nätanslutningspunkt blir därmed mer riktad än vad som följer av nuvarande lagstiftning.

Säkerhetspolisen påpekar att den föreslagna ändringen skulle kunna innebära gränsdragningsproblem mellan vad som är en fast respektive en mobil nätanslutningspunkt. De eventuella gränsdragningsproblem som kan uppkomma bör dock enligt regeringens mening kunna överkommas. Med mobil nätanslutningspunkt avses t.ex. en mobiltelefon som kopplar upp mot en mobilmast eller mot ett trådlöst lokalt nätverk (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 ska den partens operatör lagra uppgifterna, men inte operatören för den part som kommunicerar via fast anslutning. I vissa undantagsfall kan det, beroende på teknisk lösning, dock uppstå situationer när den lagringsskyldige inte har all information som krävs för att avgöra om lagringsskyldighet har inträtt för en viss kommunikation. 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 uppgifterna inte lagras av den operatör som inte har tillräcklig information för att avgöra om lagrings-skyldighet inträtt för kommunikationen.

Några remissinstanser, såsom t.ex. *Hi3G Access AB* och *Göteborgs tingsrätt*, påpekar att förslaget skulle göra regleringen mindre teknikneutral och inte beakta den teknikutveckling som sker och som innebär att gränsen mellan fast och mobil nätanslutningspunkt alltmer suddas ut. Regeringen ifrågasätter inte det men kan samtidigt konstatera att endast uppgifter som bedöms strängt nödvändiga att lagra bör ingå i lagringsskyldigheten för att regelverket ska vara proportionerligt.

Regeringen gör sammanfattningsvis bedömningen att lagringsskyldigheten för den s.k. fasta telefonin bör tas bort. Detta bör återspeglas i lagen om elektronisk kommunikation genom att det i 6 kap. 16 a § andra stycket anges

att lagringsskyldigheten omfattar uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt.

Enligt 6 kap. 16 a § första stycket lagen om elektronisk kommunikation omfattar lagringsskyldigheten även uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen samt kommunikationsutrustning. Det är typiskt sett fråga om uppgifter om vem som kontaktat vem (nummer och abonnent eller registrerad användare samt för telefonitjänst även abonnemangs- och utrustningsidentitet) vid vilken tidpunkt och varaktigheten av kommunikationen. Möjligheten för de brottsbekämpande myndigheterna att få reda på vem som har haft kontakt med vem och vid vilken tidpunkt kommunikationen skedde utgör en viktig hörnsten för den brottsbekämpande verksamheten. Samtidigt är uppgifterna integritetskänsliga, eftersom lagring av dem inkräktar på rätten till en privat kommunikation (trots att inte innehållet i kommunikationen framgår och tillgången till uppgifterna är begränsad). En lagring som inte omfattar uppgift om vem som kontaktat vem och när är emellertid utesluten, eftersom det är just den informationen som över huvud taget motiverar en lagringsskyldighet. I likhet med utredningen anser regeringen därför att dessa uppgifter alltjämt bör lagras.

Utredningen bedömer dock att det nummer som ett samtal styrts till (dvs. vidarekopplade samtal) bör tas bort från lagringsskyldigheten. Regeringen delar denna bedömning. Även om uppgifterna i vissa fall kan bidra till brottsbekämpningen har det inte framkommit något omfattande behov av att veta vilket nummer ett samtal vidarekopplats till. Uppgifterna bör därför inte längre omfattas av lagringsskyldigheten. Detta bör återspeglas i lagtexten genom att det föreskrivs att uppgifter som är nödvändiga för att identifiera målet – men inte slutmålet – för kommunikationen ska lagras.

Lagringsskyldigheten enligt 6 kap. 16 a § första stycket lagen om elektronisk kommunikation omfattar vidare lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut. När det gäller nyttan av lokaliseringsuppgifter är det naturligtvis av stort intresse att få information om kommunikation som skett i anslutning till en känd brottsplats och brottstidpunkt, vilket kräver att positionen för kommunikationen är lagrad. Denna information kan fås genom basstationstömningar. Genom att på så sätt få information om 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. Lokaliseringsuppgifter är också nödvändiga för att kunna analysera såväl kända som okända gärningsmäns rörelsemönster. Det är också ett sätt att bekräfta eller vederlägga 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.

Lokaliseringsuppgifter vid kommunikation utgör en mycket viktig pusselbit vid analysen av en misstänkts kommunikation. En uppgift om att A ringt B är t.ex. betydligt mindre värd än en uppgift om att A ringde B just när A var på en specifik plats och B på en annan plats. Det kan alltså sägas att lokaliseringsuppgifter bidrar till att öka nyttan av övriga uppgifter och således gör lagringen av dessa uppgifter mer proportionerlig. Lokaliseringsuppgifter är emellertid generellt sett tämligen integritetskänsliga. Som EU-domstolen nämner i Tele2-domen, kan man dra mycket precisa slutsatser om personers geografiska förflyttningar och därmed om privatlivet för de personer vars uppgifter lagras. Det är emellertid det som gör lokaliseringsuppgifter till ett välanvänt och extremt värdefullt verktyg, både i den vanliga brottsbekämpande verksamheten och i underrättelseverksamheten. Sammanfattningsvis bedömer regeringen, i likhet med utredningen, det som strängt nödvändigt att lagringsskyldigheten även i fortsättningen ska omfatta lokaliseringsuppgifter. Någon lagring under en pågående kommunikation bör dock, liksom hittills, inte ingå i lagringsskyldigheten.

Åklagarmyndigheten, Säkerhetspolisen, Tullverket, Ecpat Sverige och *Rädda barnen* påpekar att det i förordningen om elektronisk kommunikation inte finns någon skyldighet att lagra uppgifter om lokalisering vid meddelandehantering (såsom sms) och anser att sådana uppgifter bör lagras framöver. Som remissinstanserna påpekar 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. Som remissinstanserna framhåller är det, enligt de ramar som 6 kap. 16 a § lagen om elektronisk kommunikation ställer upp, möjligt att i förordning föreskriva en sådan lagringsskyldighet. Regeringen har för avsikt att närmare överväga en sådan ordning.

Det kan också noteras att lagstiftningens ramar medger lagring av uppgifter om första aktiveringen av förbetalda anonyma tjänster (oregistrerade kontantkort). Det bör vara fallet även fortsättningsvis. Det blir nämligen allt vanligare att personer använder sig av anonyma kontantkort som aktiveras innan ett grovt brott ska begås. En analys av vilka av de kontantkortsabonnemang som kan kopplas till en brottsplats 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. Vidare används uppgifterna ofta i det inledande skedet av vissa utredningar och när andra spaningsuppslag saknas. Uppgifterna kan också användas för att hitta bomber som kan fjärraktiveras genom elektronisk kommunikation (se SOU 2015:31 s. 164–165). Uppgifterna bedöms inte som särskilt integritetskänsliga eftersom de avser anonyma tjänster och avslöjar mycket lite om personens övriga kommunikation, aktiviteter eller privatliv.

Slutligen omfattar lagringsskyldigheten enligt 6 kap. 16 a § andra stycket lagen om elektronisk kommunikation även misslyckade uppringningar, dvs. obesvarade samtal. Regeringen delar utredningens bedömning att denna lagringsskyldighet bör gälla även framöver. Som utredningen konstaterar bör lagringsskyldigheten 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 (se SOU 2007:76 s. 159). På liknande sätt kan de användas som koder mellan en underrättelseofficer och en agent. Det bedöms därför som strängt nödvändigt att uppgifter om misslyckade uppringningar ska omfattas av lagringsskyldigheten. Lagringsskyldigheten bör dock, liksom hittills, inte omfatta samtal som inte kopplas fram, t.ex. på grund av tekniskt fel.

Internetåtkomst

Enligt 6 kap. 16 a § andra stycket lagen om elektronisk kommunikation ska uppgifter som genereras eller behandlas vid internetåtkomst lagras. I likhet med vad som gäller för telefonitjänst och meddelandehantering omfattar lagringsskyldigheten uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan. Vid internetåtkomst är det alltså enligt lagen möjligt att lagra uppgifter som gör det möjligt att identifiera abonnenten eller den registrerade användaren, t.ex. ip-adress och andra tekniska uppgifter som är nödvändiga för identifiering av abonnenten eller den registrerade användaren. För utredningen av brott begångna över internet är sådana uppgifter om abonnemang (se vidare avsnitt 7), dvs. vilken person som innehar en specifik ip-adress eller annan unik användaradress vid varje tillfälle, den absolut viktigaste informationen. Denna information är 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 underrättelseofficer eller för att rekrytera andra till terrorism. Som anförs i avsnitt 5.2 ökar internetbrottsligheten och därmed behovet av verktyg för brottsbekämpningen på denna arena i takt med att fler och fler använder internet och användningsområdet för internet utökas. Nyttan av uppgifterna är således mycket stor. Det saknas dessutom i praktiken ofta andra möjligheter att identifiera en aktör på internet på annat sätt än genom uppgift om ip-adress i kombination med andra uppgifter om abonnemang. Även behovet av uppgifterna är således påtagligt. Uppgifter om abonnemang för internet utgörs i princip av uppgift om vilken abonnent som vid varje tidpunkt var användare av en specifik ip-adress. Som framgår i avsnitt 7 bedöms dessa uppgifter inte som särskilt integritetskänsliga, eftersom de endast anger 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 integritetskänsliga. Vid bedömningen av hur integritetskänsliga uppgifterna är bör det emellertid 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 uppgifter om abonnemang. Det bör också påpekas att inga uppgifter om t.ex. besök på webbplatser omfattas av lagringsskyldigheten. Sådana uppgifter är operatörerna skyldiga att förstöra, om de inte behöver dem för vissa egna ändamål. Tillgång till endast de uppgifter som ska lagras enligt datalagringsreglerna kan således aldrig innebära att det kan kartläggas hur en person har trafikerat internet.

För att de brottsbekämpande myndigheterna ska kunna bekämpa brott som begåtts eller planlagts över internet bedömer regeringen, i likhet med utredningen, att det i enlighet med vad som anförs ovan är strängt nödvändigt att lagra sådana uppgifter som gör att det vid internetåtkomst går att spåra och identifiera kommunikationskällan, såsom uppgift om ip-adress och uppgift om abonnent och registrerad användare. Nyttan och behovet av att lagra uppgifterna är så stora att de uppväger det integritetsintrång som lagringen innebär. Uppgifterna bör således alltjämt omfattas av lagrings-skyldigheten.

Lagringsskyldighetens ramar enligt 6 kap. 16 a § är teknikneutrala i den meningen att det, för lagringsskyldighetens omfattning, inte spelar någon roll vilken tekniklösning en operatör valt, för att kunna spåra användaren bakom en ip-adress. På grund av brist på ip-adresser enligt den nuvarande huvudsakliga standarden (IPv4) har s.k. NAT-teknik kommit att användas av vissa internetleverantörer för att de tillgängliga ip-adresserna ska räcka för att koppla upp alla abonnenter. Tekniken innebär att flera abonnenter (upp till drygt 60 000 abonnenter) delar på en och samma publika ip-adress. Detta har inneburit att det inte är möjligt att ta reda på användaren bakom kommunikationen enbart genom att få del av vilken ip-adress som använts. Att valet av teknisk lösning hos operatörerna är avgörande för om det går att spåra en brottsmisstänkt eller inte framstår som orimligt och även oavsiktligt. Lagstiftningen bör därför, liksom hittills, vara teknikneutral i detta avseende. Det bör således även i fortsättningen vara möjligt för regeringen att i förordning föreskriva en skyldighet att lagra uppgifter som gör det möjligt att identifiera en abonnent. En teknikneutral bestämmelse är även rimlig med beaktande av att det aktuella teknikområdet är under konstant utveckling och alltför specifika bestämmelser riskerar att snabbt bli inaktuella. Vissa remissinstanser, t.ex. *Telia Sverige AB* och *RISE SICS AB*, anser att en sådan ändring innebär en utvidgning av lagringsskyldigheten som inte ligger i linje med bedömningen att färre uppgifter måste omfattas av en lagringsskyldighet för att den ska vara förenlig med EU-rätten. Regeringen konstaterar, i likhet med utredningen, att en sådan ändring visserligen kan leda till att fler

uppgifter lagras, men att en sådan utvidgning inte står i strid med EU-rätten. De ytterligare uppgifter som behöver lagras avser nämligen samma sakförhållande och krävs för att huvudinformationen (dvs. ip-adressen) inte ska vara värdelös. Den begränsning som dagens reglering leder till är, som nämns ovan, oavsedd och beror på att operatörerna nu använder sig av en viss ny teknik. Av samma anledning ökar inte integritetsintrånget i sig särskilt mycket av att fler tekniska uppgifter lagras i syfte att få fram den grundinformation som på grund av den tekniska utvecklingen inte längre går att få fram enbart genom lagring av själva ip-adressen. De extra uppgifter som behöver lagras torde oftast vara operatörens portnummer och ytterligare en ip-adress för varje användare samt en exakt tidsangivelse.

När det gäller *Datainspektionens* fråga om huruvida förslaget kommer att påverka t.ex. anonymiseringstjänster och VPN-tunnlar som tillhandahålls av operatörerna, kan det konstateras att förslaget inte innebär att sådana uppgifter ska lagras eftersom sådana tjänster aktiveras först efter internetåtkomsten.

Lagringsskyldigheten enligt 6 kap. 16 a § första stycket omfattar också uppgifter om datum, tidpunkt och varaktighet för kommunikationen. För internetåtkomst kan det t.ex. vara fråga om tidsuppgifter för på- och avloggning i tjänsten som ger internetåtkomst. Utredningen anser att sådana uppgifter alltjämt bör omfattas av lagringsskyldigheten. Dessa uppgifter är ofta avgörande för att kunna spåra rätt internetanvändare, eftersom samma ip-adress kan tilldelas olika användare vid olika tidpunkter. Om t.ex. polisen genom en leverantör av en chatt-app 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. Precis som vid telefonitjänst och meddelandehantering blir uppgiften om internetåtkomst betydligt mindre värdefull om det inte finns någon tid kopplad till den.

För mobil uppkoppling blir tidsuppgifterna särskilt viktiga. Eftersom utrustningen kopplar upp sig direkt mot en cell (mast) lagras en lokaliseringsuppgift vid internetåtkomsten, se 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.

Av vad som framkommit är nyttan av tidsuppgifter för på- och avloggning i tjänsten som ger internetåtkomst mycket stor. Utan uppgifter om tid blir den övriga lagringen av uppgifter om internetåtkomst betydligt mindre värdefull. Sedda för sig själva är uppgifterna inte särskilt integritetskänsliga, eftersom de inte ger någon information om hur användaren har använt internet, utan endast om vilken tid som abonnenten haft internetåtkomst. Informationen kan visserligen säga något om en persons kommunikationsmönster och uppgifterna är i viss mån integritetskänsliga eftersom de tillsammans med annan information möjliggör att en ip-adress kan sammankopplas med en abonnent. I likhet med utredningen bedömer regeringen – vid en sammantagen bedömning av nyttan av uppgifterna och det begränsade

integritetsintrång som lagringen av uppgifterna innebär – dock att det är strängt nödvändigt att lagringsskyldigheten även fortsättningsvis omfattar uppgifterna i fråga.

Vidare omfattar lagringsskyldigheten i 6 kap. 16 a § första stycket lagen om elektronisk kommunikation uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan och kommunikationsutrustning. Vid internetåtkomst avses i detta sammanhang t.ex. uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs. Denna utrustning är den sista punkten som den lagringsskyldige ansvarar för. Om den som slutligt avskiljer kommunikationen till den enskilda abonnenten inte är lagringsskyldig lagras i stället uppgifter som identifierar utrustningen vid den punkt där kommunikationen avskiljs till den som slutligt avskiljer kommunikationen till den enskilda abonnenten. Här handlar det alltså om 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. Uppgifterna är viktiga för att kunna hitta den geografiska plats som användaren kommunicerar från. Eftersom det blir allt vanligare med samtals- och meddelandekommunikation genom appar och tjänster från leverantörer som inte omfattas av lagringsskyldigheten är uppgifterna hänförliga till internetåtkomst ännu viktigare än tidigare. Uppgifterna används också för att säkra uppgifter om hela kommunikationskedjan. Det är inte ovanligt att kommunikationskedjans 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 verkningsfulla och oberoende av infra- och bolagsstrukturella lösningar bör lagringsskyldigheten liksom hittills vara utformad så att den tillåter lagring av 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 uppgifterna i många fall nödvändiga för att hitta rätt slutanvändare. De är också nyttiga för att de gör bestämmelserna om lagring av kommunikation mer teknikneutrala och anpassade till dagens teknik och användning av kommunikationstjänster. 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 anser regeringen, i likhet med utredningen, att det är strängt nödvändigt att uppgifterna lagras.

Enligt 6 kap. 16 a § lagen om elektronisk kommunikation ska uppgifter som genereras eller behandlas vid tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform) lagras. Utredningen bedömer att denna lagringsskyldighet bör tas bort. Information om kapacitet för överföring vid

internetåtkomst har i jämförelse med andra uppgifter värderats lägre av de brottsbekämpande myndigheterna. 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 det 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. Som utredningen konstaterar har något omfattande behov av uppgifterna emellertid inte framkommit. Sammantaget är det regeringens bedömning att det inte är strängt nödvändigt att behålla lagringsskyldigheten för uppgifter som genereras eller behandlas vid tillhandahållande av kapacitet för att få internetåtkomst. Detta bör återspeglas i lagtexten genom att uppgift om tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform) tas bort från lagringsskyldigheten.

Sammanfattande bedömning av lagringsskyldigheten

Genom de förändringar som beskrivs ovan anser utredningen att man uppnår en lagringsskyldighet som är förenlig med EU-rätten. Remissinstanserna har olika uppfattningar i denna fråga. En del remissinstanser, bl.a. *Säkerhets- och integritetsskyddsnämnden, Sveriges advokatsamfund, Stockholms tingsrätt* och *Göteborgs tingsrätt,* ställer sig bakom utredningens bedömning och anser att begränsningarna kommer att innebära att systemet blir förenligt med EU-rätten. Andra remissinstanser, bl.a. *Svea hovrätt, Stockholms universitet (Juridiska fakulteten), Datainspektionen, Journalistförbundet, Bahnhof AB, Com Hem AB, IT&Telekomföretagen* och *Dataskydd.net,* är kritiska eller tveksamma till bedömningen och anser att förslaget även fortsättningsvis innebär en generell och odifferentierad lagring i strid med EU-rätten.

Regeringens bedömning är att de begränsningar i lagringsskyldigheten som nu föreslås innebär att en stor del av uppgifterna inte längre kommer att omfattas av lagringsskyldigheten. Lagringsskyldigheten 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. Samtidigt differentieras lagringstiderna utifrån skillnader i behov och uppgifternas integritetskänslighet, vilket regeringen återkommer till i avsnitt 5.4. Förslagen innebär att integritetsintrånget för användarna blir mindre, men även att möjligheterna att förebygga, förhindra och utreda brott i vissa fall kan försämras. Begränsningarna är dock nödvändiga för att regelverket ska vara förenligt med EU-rätten.

De lagstiftningsåtgärder som föreslås och som innebär inskränkningar av rätten till konfidentialitet vid elektronisk kommunikation bedöms därför sammanfattningsvis som nödvändiga, lämpliga och proportionerliga i ett demokratiskt samhälle för att skydda allmän säkerhet och för förebyggande, undersökning, avslöjande av och åtal för brott (artikel 15.1 i direktiv

2002/58). Vidare bedöms dessa ändamål inte kunna uppnås genom mindre ingripande åtgärder.

5.4 En differentierad lagringstid

Regeringens förslag: I lagen om elektronisk kommunikation ska lagringstiderna differentieras beroende på vilken typ av uppgift det är fråga om enligt följande:

- Uppgifter som gäller telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska dock endast lagras i två månader.
- Uppgifter som gäller internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ska de dock endast lagras i sex månader.

Regeringen eller den myndighet som regeringen bestämmer kan meddela närmare föreskrifter om lagringstiden.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen föreslår att det i lag ska 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.

Remissinstanserna: Remissinstanserna tillstyrker eller har inget att invända mot förslaget att differentiera lagringstiden för de olika uppgiftskategorierna. Vissa remissinstanser har synpunkter på de olika delarna av förslaget enligt nedan.

Svea hovrätt och *Svenska stadsnätsföreningen* påpekar att förslaget innebär att en längre maximal lagringstid generellt skulle bli tillåten i lag och anser att en sådan ändring i praktiken blir svår att försvara i det unionsrättsliga perspektivet. *Svea hovrätt*, *Malmö tingsrätt* och *Umeå universitet (Juridiska institutionen)* ifrågasätter om det är lämpligt att bemyndiga regeringen att utvidga lagringstiden till tio månader avseende samtliga uppgifter. Universitetet anser att det vore mer lämpligt att fastslå tidsgränserna i lag. *Journalistförbundet* anser att det är positivt att det finns en maxgräns för lagringstiden inskriven i lagen, men anför att den inte bör vara längre än dagens sex månader. Förbundet anser att det är positivt att regeringen kan föreskriva en kortare lagringstid än sex månader, men anser att förändringen är negativ eftersom den öppnar upp för regeringar att enkelt kunna förlänga lagringstiderna för samtliga kategorier av uppgifter.

Stockholms tingsrätt är positiv till förslagen men anser att det bör övervägas om det av transparens- och rättssäkerhetsskäl bör framgå direkt av lagtexten att den tid som uppgifterna ska lagras inte får bestämmas till längre tid än vad som är proportionerligt och strängt nödvändigt i ett demokratiskt samhälle och att hänsyn vid den bedömningen ska tas till de brottsbekämpande myndigheternas behov och nytta av uppgiften och till hur integritetskänslig uppgiften är.

Åklagarmyndigheten och *Tullverket* poängterar att varje förkortning av lagringstiden innebär en motsvarande försämring för möjligheterna att utreda och lagföra brott. *Ekobrottsmyndigheten, Säkerhetspolisen, Tullverket, Rädda barnen* och *Ecpat Sverige* är kritiska till den förkortade lagringstiden för lokaliseringsuppgifter till två månader eftersom den kommer att innebära en försämrad möjlighet att utreda och lagföra brott. *Ekobrottsmyndigheten* poängterar att det i många fall är fråga om seriebrottslighet där man först efter en tid kan skönja de mönster som kan vara av intresse. När det gäller ekonomisk brottslighet kommer ofta anmälningarna lång tid efter den brottsliga handlingen, vilket innebär att en så kort tid som två månader kan leda till att vissa brott inte kan utredas. *Säkerhetspolisen* är inne på samma linje och anser att en så kort lagringstid som två månader i många fall kommer att göra det omöjligt att rekonstruera en kommunikationskedja.

Ekobrottsmyndigheten, Rädda barnen, Ecpat Sverige och flera organisationer inom film-, tv- och musikbranschen, såsom *Rättighetsalliansen, Dataspelsbranschen, Film- och TV-branschens samarbetskommitté* och *Musikförläggarna,* välkomnar att lagringstiden utökas till tio månader för vissa uppgifter om internetåtkomst. *Ecpat Sverige* anför att sexualbrott mot barn ofta har internationella kopplingar och en längre lagringstid kan göra att fler brott kan utredas, i stället för i dag då hälften av utredningarna måste läggas ner. *Rädda barnen* föreslår att lagringstiden för samtliga uppgifter ska vara tio månader. Organisationerna inom film-, tv- och musikbranschen framför att utvecklingen när det gäller upphovsrättsbrott går mot alltmer komplexa brottsstrukturer med internationella kopplingar och att en förlängd lagringstid av abonnentuppgifter till tio månader skulle ge de brottsbekämpande myndigheterna bättre möjligheter.

Tele2 Sverige AB tillstyrker förslaget på två månaders lagringstid för lokaliseringsuppgifter, men avstyrker förslaget om sex månaders lagringstid för uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten hänförliga till internetåtkomst, eftersom dessa uppgifter är känsliga ur integritetssynpunkt. Även *Göteborgs tingsrätt* påpekar att sådana uppgifter i princip utgör en lokaliseringsuppgift som därför är mer integritetskänslig än andra uppgifter med motsvarande lagringstid och efterfrågar en utförligare analys av lagringstidens proportionalitet.

Skälen för regeringens förslag: I det numera upphävda datalagringsdirektivet föreskrevs att medlemsstaterna skulle se till att uppgifter lagrades under en viss tid. 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. I 6 kap. 16 d § lagen om elektronisk kommunikation görs det inte någon skillnad på vilken uppgift det är fråga om, utan alla uppgifter som faller under lagringsskyldigheten enligt 6 kap. 16 a § lagen om elektronisk kommunikation ska lagras i sex månader. Vid utgången av denna tid ska uppgifterna utplånas om de inte dessförinnan begärts utlämnade.

Som framgår i avsnitt 5.2 och 5.3 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. Remissinstanserna tillstyrker eller har inte någon invändning mot att lagringstiderna differentieras. Genom att differentiera lagringstiden för respektive uppgiftsslag kan man för varje uppgiftskategori väga hur integritetskänslig uppgiftsslaget är mot brottskämpningens behov och nytta av uppgiften. Detta har inte varit möjligt tidigare och är en viktig del för att regleringen ska bli proportionerlig. För att lagringen ska vara förenlig med EU-rätten måste lagringstiderna således bestämmas efter vad som är proportionerligt och får inte vara längre än vad som är strängt nödvändigt. De lagringstider som ska gälla för de olika uppgiftskategorierna måste alltså vara motiverade på objektivt godtagbara grunder. Att en proportionalitets-bedömning utifrån ovannämnda aspekter ska göras följer direkt av EU-rätten och regeringen ser därför inte något behov av att också i lagtexten ange detta, såsom *Stockholms tingsrätt* föreslår.

För att åstadkomma en differentiering föreslår utredningen en ordning där det i lag föreskrivs en längsta lagringsfrist om tio månader och att regeringen inom denna ram får föreskriva kortare lagringsfrister. Några remissinstanser, t.ex. *Malmö tingsrätt* och *Umeå universitet (Juridiska institutionen)*, ifrågasätter om det är lämpligt att bemyndiga regeringen att utvidga lagringstiden till tio månader avseende samtliga uppgifter. Umeå universitet anser att det vore lämpligare att fastslå tidsgränserna i lag. Regeringen delar denna bedömning och anser, till skillnad från utredningen, att de lagringstider som ska gälla framöver bör framgå direkt i lagen om elektronisk kommunikation. I likhet med den modell som gäller för lagrings-skyldighetens omfattning, bör det dock finnas möjlighet för regeringen eller den myndighet regeringen bestämmer att meddela närmare föreskrifter om lagringstiderna om det behövs, t.ex. om vad som närmare ska hänföras till de olika uppgiftskategorierna och därmed precisera vilken information som faller under respektive lagringstid.

Vissa remissinstanser framför synpunkter på utredningens bedömning av vilka lagringstider som bör gälla framöver, där en del remissinstanser vill behålla eller utvidga tiden för vissa uppgiftsslag, medan andra vill begränsa den ytterligare.

De uppgifter om elektronisk kommunikation som inhämtas av polisen i underrättelseverksamheten är i de flesta fall yngre än en månad, men det finns även ärenden där historik upp till sex månader varit av stor vikt vid analysarbetet. I polisens utredningsverksamhet är den största andelen historiska uppgifter yngre än tre månader. Omkring 20–25 procent är äldre än tre månader 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 grova seriebrott såsom våldtäkter och mordförsök (SOU 2015:31 s. 129). Detta bör beaktas vid bestämmandet av lagringstiden. En annan faktor att beakta är att de brotts-bekämpande myndigheterna har behov av längre lagringstid för ip-adresser vid ärenden som har internationell koppling, t.ex. barnpornografibrott. Exempelvis har Polismyndigheten uppgett att den med en lagringstid på sex månader måste lägga ner ungefär hälften av alla barnpornografiärenden som

upparbetas utomlands. Skälet till att dessa ärenden tar lång tid att utreda är att det krävs många olika typer av åtgärder (såsom beslag, analys av beslagtagen materiel och identifiering av gärningsman och brottsoffer) där det krävs samarbeten med en eller flera polismyndigheter utomlands. Myndigheterna har sammanfattningsvis uppgett att de har behov av längst lagringstider för uppgifter hänförliga till mobil telefoni och ip-telefoni samt för abonnemangsuppgifter hänförliga till internetåtkomst.

Som framgår ovan är de flesta uppgifterna som inhämtas yngre än fem månader. 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, minskar nyttan av tillgång till de datalagrade uppgifterna. Denna minskade omfattning av lagringen kan leda till att kartläggningen av elektroniska spår i brottsutredningar tar något längre tid. Dessutom är det framför allt vid bekämpning av grova brott som de äldre uppgifterna behövs. Mot denna bakgrund anser regeringen att lagringstiden alltjämt som huvudregel bör vara sex månader. De allra flesta uppgifterna för telefonitjänst och meddelandehantering bör omfattas av huvudregeln.

Vad gäller lokaliseringsuppgifter bör, enligt utredningen, dock lagringstiden vara betydligt kortare. Flera remissinstanser, bl.a. *Ekobrotts-myndigheten, Säkerhetspolisen* och *Rädda barnen,* är kritiska till detta eftersom det enligt dem kommer att innebära en försämrad möjlighet att utreda och lagföra brott. Regeringen ifrågasätter inte det, men kan samtidigt konstatera att lokaliseringsuppgifter gör det möjligt att kartlägga en persons rörelse och kan således ge tämligen integritetskänslig information om en person. En kortare lagringstid bör därför föreskrivas för dessa uppgifter. En avvägning mellan den nytta uppgifterna innebär för de brottsbekämpande myndigheterna och det integritetsintrång uppgiften innebär leder till att, som utredningen föreslår, en lagringstid om två månader bör föreskrivas för lokaliseringsuppgifter, vilket tillstyrks av *Tele2 Sverige AB*.

Många uppgifter kopplade till internetåtkomst är inte särskilt integritets-känsliga eftersom de i sig inte innefattar uppgifter om kommunikation (t.ex. vem internetanvändaren har haft kontakt med). Uppgifter om ip-adresser och andra uppgifter som krävs för att identifiera abonnenten har ett tidsbegränsat användningsområde, eftersom uppgifterna ofta kan växla med korta mellanrum. 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. Även uppgifter om på- och avloggning i tjänsten som ger internetåtkomst krävs för att öka förståelsen och nyttan av de lagrade ip-adresserna. Som nämns i det föregående måste vissa av polisens utredningar 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. Sammanfattningsvis anser regeringen att en lagringstid om tio månader för uppgifter hänförliga till nu aktuella uppgifter utgör en rimlig avvägning mellan integritetsintresset och de brottsbekämpande myndigheternas behov. Som framgår av avsnitt 7 bedömer regeringen att Tele2-domen inte specifikt rör uppgifter om abonnemang

(såsom t.ex. ip-adresser) och att dessa uppgifter typiskt sett är mindre integritetskänsliga än t.ex. trafik- och lokaliseringsuppgifter (jfr EU-domstolens avgörande Ministerio Fiscal, dom den 2 oktober 2018, mål nr C-207/16 och Kammarrätten i Stockholm, dom den 14 december 2018, mål nr 2471-18). Regeringen anser därför, till skillnad från t.ex. *Svea hovrätt*, att EU-rätten inte utgör något hinder mot att föreskriva en längre lagringstid än nuvarande sex månader för abonnemangsuppgifter.

Uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten är, som både *Tele2 Sverige AB* och *Göteborgs tingsrätt* är inne på, 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 anses vara något mer känsliga än övriga uppgifter. En kortare lagringstid än tio månader bör därför föreskrivas. Sådana uppgifter bör i stället sparas i sex månader.

Sammanfattningsvis bör således lokaliseringsuppgifter vid telefonitjänst och meddelandehantering lagras i två månader. Uppgifter om internet-åtkomst, förutom uppgifter som identifierar utrustningen där kommunikationen slutligt avskiljs, bör lagras i tio månader och övriga uppgifter bör lagras i sex månader.

5.5 Uppgifter som omfattas av yrkesmässig tystnadsplikt

Regeringens bedömning: Det bör inte införas något undantag från lagring eller inhämtning av uppgifter om elektronisk kommunikation för personer med yrkesmässig tystnadsplikt. Det bör inte heller införas någon skyldighet att förstöra uppgifter som på grund av frågeförbudet enligt rättegångsbalken inte skulle ha kunnat inhämtas genom vittnesförhör i domstol.

Datalagringsutredningens förslag och bedömning överensstämmer delvis med regeringens. Datalagringsutredningen föreslår att det ska införas en förstörandeskyldighet för uppgifter som på grund av frågeförbudet enligt rättegångsbalken inte skulle ha kunnat inhämtas genom vittnesförhör i domstol.

Remissinstanserna: *Ekobrottsmyndigheten* och *Institutet för Juridik och Internet* instämmer i utredningens bedömning att det inte bör införas något förbud mot att inhämta uppgifter som kan vara skyddade på grund av yrkesmässig tystnadsplikt. *Utgivarna* anser att det bör införas ett undantag från lagringsskyldigheten som säkerställer meddelares anonymitet och att detta bör utredas närmare. Även *Sveriges advokatsamfund* efterlyser regler

som undantar uppgifter som kan vara föremål för t.ex. advokatsekretess från lagringsskyldigheter.

Institutet för Juridik och Internet, Tullverket, Göteborgs universitet (Juridiska institutionen), Stockholms universitet (Juridiska fakulteten), Tele2 Sverige AB, Svenska kyrkan, Sveriges kristna råd, Journalistförbundet, Tidningsutgivarna och *Föreningen för digitala fri- och rättigheter (DFRI)* ser positivt på eller har inget att invända mot att en förstörandeskyldighet införs. *Tele2 Sverige AB* och *Journalistförbundet* anser att det också bör säkerställas att berörda myndigheter upprättar interna rutiner för hur sådana ärenden ska identifieras och hanteras samt att de bör vara föremål för extern tillsyn. Journalistförbundet föreslår att även grundmaterialet som lagrats hos operatörerna ska förstöras. *Swedish Network Users' Society (SNUS)* anser att uppgifter som omfattas av sekretess eller tystnadsplikt, t.ex. uppgifter som faller under advokatsekretessen eller meddelarskyddet, måste hanteras på ett mycket mer adekvat sätt än vad utredningen föreslår.

Ekobrottsmyndigheten avstyrker förslaget om att införa en förstörandeskyldighet och pekar på vissa svårigheter med förslaget. T.ex. kan uppgifter som skulle förstöras kunna vara uppgifter som talar till den misstänktes fördel och således kunna innebära en kränkning av den misstänktes rätt till en rättvis rättegång om sådant material förstörs under utredningsstadiet. Myndigheten pekar också på vissa praktiska svårigheter vid bedömningen av vad som ska förstöras då frågeförbudet i rättegångsbalken är utformat efter vad som anförtrotts vissa befattningshavare i deras yrkesutövning eller vad dessa erfarit. Det är enligt myndigheten svårt att se hur det ska vara möjligt att bedöma detta när det gäller lagring av uppgifter som inte tar sikte på innehållet i kommunikationen. *Säkerhetspolisen* och *Polismyndigheten* är inne på samma linje och pekar på att rättssäkerheten för den misstänkte och utredningen i övrigt kan riskera lida skada av att uppgifter raderas. Att vissa uppgifter raderas kan också leda till att tillsynen av polisens verksamhet inte kan fullgöras på ett tillfredsställande sätt. *Utgivarna* anser att förslaget om en förstörandeskyldighet är otillräckligt eftersom skadan redan är skedd när informationen väl har uppfattats och anonymiteten brutits.

Statens inspektion för försvarsunderrättelseverksamheten bedömer att den föreslagna ändringen i rättegångsbalken inte kommer att påverka förstöringsskyldighetens omfattning enligt signalspaningslagen. *Göta hovrätt* har vissa lagtekniska påpekanden gällande förslagen om en förstörandeskyldighet.

Utredningens bedömning överensstämmer med regeringens bedömning vad gäller frågan om det bör införas ett undantag från lagringen för personer med tystnadsplikt. Enligt utredningen bör Datalagringsutredningens förslag om att införa en förstörandeskyldighet för uppgifter som omfattas av yrkesmässig tystnadsplikt övervägas.

Remissinstanserna: De flesta remissinstanser uttalar sig inte särskilt i denna fråga. *Åklagarmyndigheten* delar utredningens bedömning att det inte bör införas något undantag från lagringen för personer med tystnadsplikt. Myndigheten tillstyrker Datalagringsutredningens förslag om förstörandeskyldighet men har vissa lagtekniska påpekanden på förslaget. *Sveriges*

advokatsamfund anser att det bör införas en regel som undantar lagring av uppgifter som omfattas av advokatsekretess. Samfundet föreslår att det kan ske genom att de abonnemang eller andra elektroniska anslutningar som en advokat använder sig av i sin verksamhet anmäls i förväg. Om ett lagringsförbud inte kan införas förordar samfundet att det införs hinder mot att inhämta uppgifter som omfattas av tystnadsplikt och att en förstörandeskyldighet införs. *Svenska journalistförbundet* är kritiskt till att det inte föreslås ett undantag från lagringsskyldigheten för personer som omfattas av tystnadsplikt, såsom t.ex. journalister. Förbundet anser att man bortsett från det faktum att skadan redan är skedd i det ögonblick ett samtal mellan en källa och en journalist lagras.

Skälen för regeringens bedömning

Skyddet för yrkesmässig tystnadsplikt och frågeförbudet

Vissa person- eller yrkeskategorier är underkastade tystnadsplikt i fråga om uppgifter som de har erfarit i sin yrkesutövning. Exempelvis finns regler om tystnadsplikt för advokater i 8 kap. 4 § första stycket RB. Ett annat exempel är den tystnadsplikt som följer av reglerna om meddelarskydd enligt 3 kap. 3 § tryckfrihetsförordningen (TF) och 2 kap. 3 § yttrandefrihetsgrundlagen (YGL). Enligt dessa bestämmelser har den som tar befattning med tillkomsten eller utgivningen av tryckta skrifter eller framställningar som är avsedda att tas in i tryckta skrifter m.m. eller framställningar i radio och tv etc. som huvudregel tystnadsplikt för uppgifter som röjer identiteten hos den som lämnar uppgifter avsedda att offentliggöras i sådana medier. Tillämpningsområdet omfattar t.ex. journalister och andra som arbetar på en tidnings- eller tv-redaktion eller på företag där framställningar som skyddas av grundlagarna produceras. Tystnadsplikten gäller också för den som arbetar på en nyhetsbyrå och den som bedriver verksamhet på internet med s.k. frivilligt grundlagsskydd med stöd av ett utgivningsbevis enligt 1 kap. 4 § YGL. Tystnadsplikten gäller alltså för en relativt stor grupp av personer som inte alltid är helt lätt att definiera och avgränsa. Som ett ytterligare led i meddelarskyddet gäller ett principiellt efterforskningsförbud. Myndigheter och andra allmänna organ får som huvudregel inte efterforska vem som har lämnat meddelandet och som har rätt att vara anonym (3 kap. 5 § TF och 2 kap. 5 § YGL). Ytterligare exempel är den tystnadsplikt som gäller inom hälso- och sjukvården enligt 25 kap. offentlighets- och sekretesslagen (2009:400) och 6 kap. patientsäkerhetslagen (2010:659).

Det är en allmän medborgerlig plikt att inställa sig som vittne vid domstol och där avlägga vittnesmål. Vittnesplikten är av grundläggande betydelse för domstolarnas möjligheter att få ett fullgott underlag för prövningen av mål och ärenden. I flera fall får tystnadsplikten ge vika för vittnesplikten. I rättegångsbalken uppställs dock vissa begränsningar i vittnesplikten genom det s.k. frågeförbudet i 36 kap. 5 § andra–sjätte styckena. Bestämmelsen har tillkommit av hänsyn till enskildas personliga integritet och privatliv. Lagstiftaren har ansett att den enskilde som huvudregel ska kunna anförtro sig till vissa angivna personer inom dessas yrkesutövning utan rädsla för att

informationen ska föras vidare eller annars användas mot honom eller henne. Frågeförbudet innebär att personer inom vissa yrkeskategorier, t.ex. advokater och hälso- och sjukvårdspersonal, inte får höras som vittnen om något som på grund av deras ställning anförtrotts dem eller de i samband därmed på annat sätt erfarit, med mindre än att det är medgivet i lag eller den till vars förmån tystnadsplikten gäller samtycker (andra stycket). För rättegångsombud, biträden och försvarare gäller att de får höras som vittnen om vad som anförtrotts dem för uppdragets fullgörande endast om parten medger det (tredje stycket). Vissa begränsade undantag görs från frågeförbudet när det gäller de nu nämnda yrkeskategorierna (fjärde stycket). Den som är präst inom ett trossamfund eller den som i ett sådant samfund har motsvarande ställning får inte höras som vittne om något som han eller hon har erfarit under bikt eller enskild själavård (femte stycket). Vidare får den som har tystnadsplikt enligt 3 kap. 3 § TF eller 2 kap. 3 § YGL höras som vittne om förhållanden som tystnadsplikten avser endast i den mån det föreskrivs i nämnda paragrafer (sjätte stycket). Slutligen gäller enligt det sjunde stycket att, om någon inte får höras som vittne enligt paragrafen, så får vittnesförhör inte heller äga rum med den som under tystnadsplikt har biträtt med tolkning eller översättning.

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

Enligt 27 kap. 22 § RB får hemlig avlyssning av elektronisk kommunikation eller hemlig rumsavlyssning inte avse samtal, meddelanden eller annat tal där någon som yttrar sig på grund av bestämmelserna i 36 kap. 5 § andra–sjätte styckena RB inte skulle ha kunnat höras som vittne om det som har sagts eller på annat sätt kommit fram. Om det under avlyssningen kommer fram att det är fråga om ett sådant samtal, meddelande eller tal, ska avlyssningen omedelbart avbrytas. Detsamma gäller vid hemlig avlyssning av elektronisk kommunikation enligt preventivlagen (11 §). Bestämmelserna innebär att den som granskar material från hemlig avlyssning genast måste avbryta granskningen så fort det står klart att samtalet omfattas av avlyssningsförbud. Avlyssningsförbudet är utformat med utgångspunkt från bedömningen att uppgifter som på grund av hänsyn till enskildas personliga integritet inte får inhämtas genom vittnesförhör i domstol inte heller ska kunna inhämtas genom avlyssning (se prop. 2005/06:178 s. 68, prop. 2009/10:133 s. 24 och prop. 2013/14:237 s. 132).

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

Ett grundläggande krav för att tillstånd till hemlig övervakning av elektronisk kommunikation och inhämtning av uppgifter enligt inhämtningslagen ska kunna meddelas är att åtgärden är proportionerlig (27 kap. 1 § tredje stycket RB och 2 § inhämtningslagen). Vid bedömningen av om en åtgärd kan anses proportionerlig har det betydelse vilken typ av kommunikation uppgifterna avser. Bland annat ska det beaktas om åtgärden innebär intrång i ett rättsligt skyddat intresse, t.ex. meddelarskyddet enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen. Innebär inhämtningen ett kringgående av förbudet för massmedier att röja sina källor eller för det allmänna att efterforska vem som är meddelare, får inhämtning inte ske (prop. 2011/12:55 s. 122). Detta innebär alltså att risken för att uppgifter om skyddad kommunikation kommer att hämtas in då åtgärden verkställs ska beaktas vid tillståndsgivningen. Vidare gäller proportionalitetsprincipen under hela verkställighetsförfarandet och ska således, även sedan tillstånd har meddelats, beaktas av den verkställande myndigheten. Integritetsintrånget under verkställigheten kan bli så stort att åtgärden inte längre är tillåten, trots att rekvisiten för åtgärden fortfarande är uppfyllda (a. prop. s. 122). Trots att det inte finns något uttryckligt förbud är alltså möjligheten att hämta in uppgifter om elektronisk kommunikation avseende personer som omfattas av yrkesmässig tystnadsplikt begränsad jämfört med kommunikation som avser andra personer. Däremot kan det givetvis hända att en åtgärd som riktar sig mot någon som inte omfattas av yrkesmässig tystnadsplikt får till följd att även uppgifter om dennes kontakter med personer inom skyddade yrkeskategorier samlas in. Vidare kan uppgifter som avser personer inom skyddade yrkeskategorier komma att inhämtas genom t.ex. basstationstömningar.

Sammanfattningsvis är det i svensk rätt alltså huvudsakligen uppgiftens innehåll som avgör om uppgiften omfattas av skydd mot att de brottsbekämpande myndigheterna eller någon annan tar del av den. 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 (36 kap. 5 § RB, se även NJA 2010 s. 122, särskilt punkterna 8–9). Vid beslut om tillstånd till inhämtning av elektronisk kommunikation ska proportionalitetsprincipen beaktas.

Något undantag från lagring eller inhämtning av uppgifter för personer med yrkesmässig tystnadsplikt eller en förstörandeskyldighet bör inte införas

EU-domstolen noterar i Tele2-domen att den svenska lagstiftningen om datalagring inte innehåller något undantag för personer vilkas kommunikationer enligt nationell rätt omfattas av tystnadsplikt (punkt 105, jfr även Digital Rights-domen punkt 58). Däremot uppställer inte domstolen något krav på en sådan begränsning av lagringsskyldigheten. Mot bakgrund av domstolens konstaterande har fråga uppkommit om det finns anledning att göra nya överväganden om den svenska regleringen kring lagring, inhämtning eller förstörande av uppgifter gällande personer med tystnadsplikt.

Sveriges advokatsamfund, Svenska journalistförbundet och *Utgivarna* anser att det bör införas ett undantag från lagringsskyldigheten för personer som omfattas av tystnadsplikt, såsom t.ex. journalister och advokater. I likhet med utredningarna anser regeringen att det emellertid inte finns skäl att införa något sådant undantag när det gäller lagring av uppgifter om elektronisk kommunikation, dvs. uppgifter som visar att kommunikation har ägt rum men inte vad den innehöll. Som framgår ovan är det normalt uppgiftens innehåll som avgör om den omfattas av skydd mot att de brottsbekämpande myndigheterna tar del av uppgiften. Exempelvis är frågeförbudet i rättegångsbalken utformat efter vad som anförtrotts vissa befattningshavare i deras yrkesutövning eller vad dessa erfarit. När det gäller meddelarskyddet omfattas en person som har kommunicerat med en journalist av detta skydd endast i de fall då kommunikationen innebär att ett meddelande etc. lämnas för publicering. Anonymitetsskyddet, och därmed även tystnadsplikten, gäller däremot inte om en journalist söker upp en person för en intervju och denne svarar på frågor utan att ge uttryck för ett önskemål om att skyddas som journalistisk källa. Inte heller gäller anonymitetsskyddet för kontakter som en journalist har med någon som inte är medveten om att uppgifterna lämnas till en person som avser att publicera dem i ett grundlagsskyddat medium. Ett förbud mot att lagra uppgifter som enligt svensk rätt omfattas av tystnadsplikt skulle därför i många fall kräva att man undersöker syftet och omständigheterna kring kommunikationen eller tar del av innehållet i den. Att klarlägga omständigheterna kring kommunikationen torde ofta vara en svår uppgift i det skede inhämtningen av uppgifter sker och en kontroll av innehållet i kommunikationen skulle dessutom innebära ett ökat integritetsintrång. En sådan ordning är därför inte lämplig. Ett sätt att komma runt detta skulle vara att införa ett system där vissa yrkeskategorier i förväg undantas från lagringen genom ett anmälningsförfarande av t.ex. telefonnummer och annan elektronisk utrustning som används i yrkesverksamheten, såsom *Sveriges advokatsamfund* föreslår. Ett sådant system skulle dock vara administrativt svårt att genomföra, samtidigt som det inte skulle vara en önskvärd ordning. Även personer med tystnadsplikt kan misstänkas för brott och när de uppträder som brottsmisstänkta har de inte någon priviligierad ställning. Det är dock viktigt att notera att tystnadsplikten till förmån för klienten alltjämt gäller även i en sådan situation.

Mot bakgrund av att det normalt endast är en uppgifts innehåll som skyddas finns det inte heller skäl att införa ett förbud mot inhämtning av uppgifter om vissa yrkeskategoriers elektroniska kommunikation. Vid inhämtning av uppgifter om elektronisk kommunikation känner de brottsbekämpande myndigheterna normalt sett inte till innehållet i kommunikationen. Detta innebär att det inte går att avgöra vilka uppgifter som omfattas av tystnadsplikt. Ett förbud mot att hämta in sådana uppgifter skulle därför vara mycket svårt att tillämpa. Det är dock inte otänkbart att det i undantagsfall skulle kunna inträffa att en myndighet får kännedom om att de aktuella uppgifterna omfattas av yrkesmässig tystnadsplikt redan innan inhämtning sker. Så skulle t.ex. kunna vara fallet om hemlig övervakning av elektronisk kommunikation används tillsammans med hemlig avlyssning. I en sådan situation gäller

emellertid proportionalitetsprincipen som innebär att inhämtning inte får ske om det skulle innebära ett kringgående av tystnadsplikten eller efterforskningsförbudet (jfr prop. 2011/12:55 s. 122). Ett uttryckligt förbud mot inhämtning av uppgifter i sådana situationer skulle således vara av begränsat praktiskt värde.

I detta sammanhang bör även påpekas att det råder ett grundlagsskyddat förbud för det allmänna att efterforska vem som lämnat uppgifter till t.ex. en journalist. Regeringen instämmer dock i den bedömning som utredningarna gör att efterforskningsförbudet i sådana situationer överträds endast i den mån som syftet från det allmännas sida är att efterforska en författare, utgivare eller meddelare. När sådan information i stället råkar inhämtas av en myndighet som en icke avsedd bieffekt av annan verksamhet kan det således inte anses att efterforskningsförbudet överträds.

Datalagringsutredningen föreslår att uppgifter som omfattas av yrkesmässig tystnadsplikt ska förstöras i efterhand om de är sådana att de inte hade kunnat inhämtas genom vittnesförhör i domstol på grund av frågeförbudet i rättegångsbalken. Flera remissinstanser, såsom t.ex. *Institutet för Juridik och Internet, Tullverket, Tele2 Sverige AB* och *Svenska kyrkan*, tillstyrker förslaget eller har ingen invändning mot det. Som Datalagringsutredningen konstaterar skulle tillämpningen av en sådan regel normalt förutsätta att myndigheten efter att en inhämtning skett får reda på innehållet i kommunikationen och på så vis kan sluta sig till att uppgiften omfattas av yrkesmässig tystnadsplikt. Det är alltså här fråga om att uppgiften oavsiktligt kommit att röjas genom tvångsmedelsanvändningen (de s.k. bieffektsfallen). Som framgår ovan kan en sådan situation uppstå endast undantagsvis och det torde därför sällan bli aktuellt att tillämpa en sådan regel. Dessutom gäller även i denna situation proportionalitetsprincipen, som ger skydd mot obehörigt röjande av uppgifter (jfr prop. 1988/89:124 s. 36). En parallell kan här också dras till beslagsförbudet i 27 kap. 2 § RB som innebär att en skriftlig handling inte får tas i beslag när den innehåller skyddad information. Vad som gäller om ett beslag har skett i strid mot förbudet är inte lagreglerat. Enligt grunderna för bestämmelsen har det dock ansetts att myndigheten inte får använda den skyddade informationen och har att verka för att den inte finns bevarad inom myndigheten (NJA 2015 s. 631). Enligt riktlinjer för åklagararbetet framgår att dessa principer ska iakttas. Mot denna bakgrund kan det ifrågasättas om det finns ett så stort behov av en uttrycklig lagreglering om en förstörandeskyldighet. Till detta kommer att det finns vissa svårigheter med en sådan ordning, som också *Ekobrottsmyndigheten, Säkerhetspolisen* och *Polismyndigheten* påpekar. Exempelvis kan uppgifter som skulle omfattas av en förstörandeskyldighet kunna tala till den misstänktes fördel. Som ett exempel kan nämnas att uppgifter från hemlig övervakning av elektronisk kommunikation kan ge stöd för att den misstänkte inte var på t.ex. en brottsplats vid tidpunkten för samtalet. Europadomstolen har i ett par avgöranden fällt Finland för att material från hemliga tvångsmedel förstörts under utredningsstadiet (Janatuinen mot Finland, 8 december 2009, mål nr 28552/05, och Natunen mot Finland, 30 juni 2009, mål nr 21022/04). Europadomstolen fann att agerandet hade inneburit en kränkning

av den misstänktes rätt till en rättvis rättegång, eftersom besluten att förstöra materialet medfört att varken domstolen eller den misstänkte givits möjlighet att bedöma om materialet varit relevant eller inte. Att vissa uppgifter raderas kan också leda till att tillsynen av myndighetens verksamhet inte kan fullgöras på ett tillfredsställande sätt.

Sammantaget anser regeringen att det redan i dag finns ett fullgott skydd mot obehörigt röjande av uppgifter och att den föreslagna förstörande-skyldigheten för med sig sådana nackdelar att den inte bör genomföras.

Mot den angivna bakgrunden lämnar regeringen inget förslag på något undantag från lagring eller inhämtning av uppgifter från personer som har tystnadsplikt eller någon lagreglerad skyldighet att förstöra vissa uppgifter.

6 Tillgången till lagrade uppgifter

6.1 Nuvarande bestämmelser om tillgång till uppgifter om elektronisk kommunikation

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. Möjligheten att få tillgång till abonnemangsuppgifter regleras i lagen om elektronisk kommunikation, se avsnitt 7. Inhämtningen ger inte tillgång till uppgifter om innehållet i meddelanden. Hemlig övervakning av elektronisk kommunikation omfattar inhämtning av uppgifter från telefoni- och internetoperatörer. Tvångsmedlet kan användas också för att hindra meddelanden som överförs i ett elektroniskt kommunikationsnät från att nå fram.

Hemlig övervakning av elektronisk kommunikation får 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 narkotika-smuggling av normalgraden (27 kap. 19 § tredje stycket RB). Därutöver får tvångsmedlet användas vid förundersökning om vissa samhällsfarliga brott som bekämpas av Säkerhetspolisen, t.ex. sabotage, spioneri 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 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 RB 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 (överskotts-information) 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. Frågan om hur överskottsinformation ska få användas är föremål för överväganden (SOU 2018:61).

Inhämtningslagen

Inhämtningslagen reglerar Polismyndighetens, Säkerhetspolisens och Tull-verkets möjligheter att hämta in uppgifter om elektronisk kommunikation i underrättelseverksamhet. Lagen reglerar enbart inhämtning från den som enligt lagen om elektronisk kommunikation 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 kom-munikationsutrustning 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 ett lägre straffminimum, t.ex. sabotage och spioneri. Denna bestämmelse är tidsbegränsad och gäller till utgången av 2019. Regeringen föreslår nu att denna bestämmelse ska permanentas, se avsnitt 6.8.

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 tillämpnings-området för straffprocessuella tvångsmedel enligt rättegångsbalken, vilket beror på att inhämtningslagen är tillämplig redan på underrättelsestadiet.

Beslut om inhämtning fattas av myndigheten själv. Utgångspunkten är att det är myndighetschefen som ska besluta om inhämtningen. Myndighets-chefen får dock delegera rätten att fatta beslut till en annan anställd vid myndigheten som har den särskilda kompetens, utbildning och erfarenhet som behövs. Den som har fått sådan delegation får inte fatta beslut om inhämtning i operativ verksamhet som han eller hon själv deltar i (4 §).

Regeringen föreslår i avsnitt 6.5 att beslutsordningen ska ändras så att beslut framöver ska fattas av åklagare efter ansökan av myndigheten.

Säkerhets- och integritetsskyddsnämnden utövar tillsyn över inhämtningen. Samtliga beslut om inhämtning av uppgifter ska anmälas till nämnden när underrättelseärendet har avslutats (6 §). Inhämtade uppgifter får användas i en förundersökning endast efter tillstånd av domstol till hemlig övervakning av elektronisk kommunikation. Utan ett sådant tillstånd får dock inhämtade uppgifter ligga till grund för beslut om att inleda en förundersökning (8 §).

Preventivlagen

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 preventivlagen får tillstånd till bl.a. hemlig övervakning av elektronisk kommunikation meddelas om det finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som innefattar vissa särskilt angivna brott. Det rör sig främst om sådan samhällsfarlig brottslighet som bekämpas av Säkerhetspolisen, t.ex. sabotage, spionerі och terroristbrottslighet, men även vissa våldsbrott och brott mot frihet och frid som begås i syfte att påverka offentliga organ eller journalister (systemhotande brottslighet). Även om lagen främst rör brottslig verksamhet inom Säkerhetspolisens område kan också Polismyndigheten använda lagen. Det sker dock mycket sällan. Under 2015, 2016 och 2017 förekom ingen användning av hemliga tvångsmedel enligt preventivlagen i Polismyndighetens verksamhet (skr. 2017/18:69 s. 26 och skr. 2018/19:19 s. 26). Tillstånd får meddelas endast om åtgärden är proportionerlig och av synnerlig vikt för att förhindra sådan brottslig verksamhet (1 och 5 §§).

Hemlig övervakning enligt preventivlagen 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 Stockholms tingsrätt efter ansökan av åklagare (6 §). Tillståndet får – som för 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 rättegångsbalken 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 §).

Lagen om särskild utlänningskontroll

Enligt lagen (1997:572) om särskild utlänningskontroll (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 19–22 §§ LSU ska tillämpas på utlänningen. Detsamma gäller om det utvisningsbeslut som inte ska verkställas har fattats enligt 8 eller 8 a kap. utlänningslagen (2005:716) och det finns sådana omständigheter avseende utlänningen som nämns ovan (11 och 11 a §§ LSU).

Av 19 och 20 §§ LSU 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 om straff för terroristbrott och det finns synnerliga skäl.

Yrkande om tillstånd görs hos Stockholms tingsrätt av Säkerhetspolisen eller Polismyndigheten. 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 § LSU).

6.2 EU-domstolens uttalanden i Tele2-domen om tillgången till lagrade uppgifter om elektronisk kommunikation

Den andra tolkningsfrågan som EU-domstolen besvarade i Tele2-domen gäller frågan om de brottsbekämpande myndigheternas tillgång till lagrade uppgifter om elektronisk kommunikation. Enligt direktiv 2002/58 ska konfidentialitet säkerställas vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster (artikel 5). Enligt artikel 15.1 i direktivet får medlemsstaterna emellertid, under vissa förutsättningar, genom nationell lagstiftning vidta åtgärder som begränsar konfidentialiteten, t.ex. för brottsbekämpande syften. När det gäller de syften som kan motivera en

nationell lagstiftning som begränsar konfidentialiteten vid elektronisk kommunikation anför EU-domstolen följande (punkterna 115–121 i domen).

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 endast förebyggande, undersökning, avslöjande av och åtal för grov brottslighet som kan motivera en sådan tillgång. Vad gäller proportionalitetsprincipen fastslår EU-domstolen att en nationell lagstiftning måste garantera att tillgång inte ges utöver vad som är strängt nödvändigt.

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 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. 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. 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 vara grundad på objektiva kriterier som avgör under vilka omständigheter och på vilka villkor behöriga nationella myndigheter ska ges tillgång till uppgifter.

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 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.

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. Enligt EU-domstolen krävs vidare 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.

EU-domstolen kommer mot denna bakgrund till slutsatsen att EU-rätten utgör hinder för en nationell lagstiftning som – inom ramen för brottsbekämpning – inte begränsar tillgången till trafik- och lokaliseringsuppgifter till enbart åtgärder som syftar till att bekämpa grov brottslighet och inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet (punkt 125 i domen).

I det följande analyseras de svenska reglerna om tillgång till uppgifter om elektronisk kommunikation i ljuset av Tele2-domen.

6.3 Tillgång endast för att bekämpa grov brottslighet

Regeringens bedömning: Tillgång till lagrade trafik- och lokaliseringsuppgifter får endast ges för bekämpning av grov brottslighet. Reglerna i rättegångsbalken, preventivlagen, inhämtningslagen och lagen om särskild utlänningskontroll uppfyller EU-rättens krav i detta avseende.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna kommenterar inte utredningens bedömning.

Skälen för regeringens bedömning: Som anges i föregående avsnitt anför EU-domstolen att endast bekämpning av grov brottslighet kan motivera att brottsbekämpande myndigheter ges tillgång till lagrade uppgifter. Det finns dock 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 – anses som så allvarliga att de på olika 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/EU av den 27 april 2016 om användning av passageraruppgiftssamlingar (PNR-uppgifter) för att förebygga, förhindra, upptäcka, utreda och lagföra terroristbrott och grov brottslighet (PNR-direktivet) 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). Därutöver är direktivet tillämpligt på vissa terrorismrelaterade brott, trots att de har en straffskala som inte når upp till detta minimikrav. 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 har straffminimum på minst sex månaders fängelse (27 kap. 19 § RB). I den uppräkningen finns t.ex. narkotikabrott och barnpornografibrott.

Som framgår i avsnitt 6.1 kan hemlig övervakning av elektronisk kommunikation förekomma även inom ramen för förhindrande av vissa särskilt allvarliga brott. Bland de brott som kan berättiga till hemlig övervakning ingår de absolut grövsta brotten i vårt samhälle, som t.ex. mord, terroristbrott och spioneri (1 § preventivlagen).

Ytterligare ett exempel förekommer i inhämtningslagen. Inhämtning enligt den lagen 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 (2 §). Härutöver finns en uppräkning av vissa brott inom främst Säkerhetspolisens verksamhetsområde som t.ex. spioneri och brott mot medborgerlig frihet (3 § inhämtningslagen).

Enligt lagen om särskild utlänningskontroll finns möjligheter att tillgripa hemlig övervakning av elektronisk kommunikation vid misstankar om medverkan till terroristbrott enligt 2 § lagen om straff för terroristbrott eller försök, förberedelse eller stämpling till sådant brott (19 och 20 §§).

Den brottslighet som omfattas av de uppräknade tvångsmedelslagarna har lagstiftaren ansett vara så allvarliga att utredningsintresset väger tyngre än det integritetsintrång som drabbar dem som blir föremål för tvångsmedlet. I likhet med utredningen anser regeringen att det inte finns något i domstolens uttalanden i Tele2-domen som ger anledning att tro att de avvägningar som gjorts beträffande detta måste rubbas. Ingen remissinstans invänder mot detta. Mot denna bakgrund är det regeringens bedömning att de brott som ger rätt att använda tvångsmedel enligt rättegångsbalken, inhämtningslagen, preventivlagen och lagen om särskild utlänningskontroll är att betrakta som sådan grov brottslighet som enligt EU-domstolen kan motivera att brottsbekämpande myndigheter ges tillgång till lagrade uppgifter.

6.4 Tillgång till uppgifter om personer som är inblandade i allvarlig brottslighet

Regeringens bedömning: Tillgång till lagrade trafik- och lokaliseringsuppgifter bör som huvudregel endast gälla personer som på något sätt kan vara inblandade i allvarlig brottslighet. Reglerna i rättegångsbalken, preventivlagen, inhämtningslagen och lagen om särskild utlänningskontroll uppfyller EU-rättens krav i detta avseende.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna kommenterar inte utredningens bedömning.

Skälen för regeringens bedömning

Tillgång till uppgifter som rör personer som på något sätt kan vara inblandad i allvarlig brottslighet

Tillgång till lagrade uppgifter kan enligt EU-domstolen i princip bara beviljas för 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 t.ex. 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.

Inledningsvis kan noteras att det som huvudregel alltså krävs att personen på något sätt är inblandad i den allvarliga brottsligheten för att få hämta in uppgifter om elektronisk kommunikation om denna. Domstolen beskriver denna personkrets på samma sätt som Europadomstolen i målet Roman Zakharov mot Ryssland (4 december 2015, mål nr 47143/06, punkt 260), som EU-domstolen också hänvisar till. Därtill lägger EU-domstolen ”på något sätt inblandad”, vilket alltså innebär att personkretsen är vidare än endast misstänkta gärningsmän och medhjälpare. Detta stöds även av att Europadomstolen i samma dom (punkt 245) – med hänvisning till tidigare praxis (Greuter mot Nederländerna, den 19 mars 2002, mål nr 40045/98) – 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. I Greuter mot Nederländerna bedömdes det nämligen befogat att avlyssna en telefon tillhörande partnern till en dödad person, eftersom det fanns skäl att tro att gärningsmannen skulle kunna kontakta henne. I särskilda fall kan det alltså enligt EU-domstolen vara befogat att ge myndigheterna tillgång även till andra personers uppgifter. Det bör särskilt noteras att det 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.

I det följande beskrivs de svenska reglerna i fråga om vilken personkrets som tillgång kan beviljas och regeringens bedömning av om dessa regler uppfyller EU-rättens krav i detta avseende.

Hemlig övervakning av elektronisk kommunikation

Huvudsakligen beviljas åtkomst till lagrade uppgifter vid hemlig övervakning av elektronisk kommunikation 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 eller som kan antas ha använts eller komma att användas 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 kan ett tillstånd till nu nämnd övervakning begränsas till att endast avse inkommande samtal (prop. 2002/03:74 s. 38–39).

Som redogörs för ovan tillåter EU-rätten i viss utsträckning övervakning även mot andra än misstänkta. Mot denna bakgrund gör regeringen, i likhet med utredningen, bedömningen att den övervakning som regleras i 27 kap. 20 § första stycket är förenlig med de krav som EU-rätten uppställer. Ingen remissinstans invänder mot denna bedömning.

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, huvudsakligen brott med ett straffminimum på fängelse två år eller samhällsfarlig brottslighet såsom t.ex. spionerі, sabotage eller mordbrand (27 kap. 19 § fjärde stycket RB). Exempel på en sådan åtgärd är basstationstömning (masttömning) som utförs t.ex. om polisen hittar en mördad person och vill undersöka vilka som har befunnit sig vid platsen. En basstationstömning avser i bästa fall en eller flera misstänkta personer, men medför samtidigt att uppgifter inhämtas om personer som inte är misstänkta. Det har i förarbetena inte bedömts innebära ett betydande ingrepp i den enskildes privata sfär eftersom det normalt endast är fråga om en positionsbestämning vid ett specifikt tillfälle. En sådan inhämtning har därför inte ansetts innebära ett sådant betydande intrång i den personliga integriteten som avses i 2 kap. 6 § regeringsformen (prop. 2011/12:55 s. 97). Dessutom är personuppgifter som behandlas hos de brottsbekämpande myndigheterna omgärdade av integritetsskyddande lagstiftning, se lagen (2018:1697) om åklagarväsendets behandling av personuppgifter inom brottsdatalagens område (åklagarväsendets brottsdatalag), lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område (polisens brottsdatalag) och lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område (Tullverkets brottsdatalag). I fråga om uppgifter som rör meddelanden är inhämtningen dessutom begränsad till att enbart avse historiska uppgifter. Till det kommer att nu aktuell övervakning endast får utföras om det är av synnerlig vikt för utredningen. Det innebär att uppgifterna som tvångsmedlet förväntas leda till ska vara av viss kvalitet och inte inskränka sig till obetydliga detaljer. Däremot behöver uppgiften inte vara avgörande utan kan indirekt bidra till att föra förundersökningen framåt, t.ex. genom kartläggning av kontakter och förehavanden. I kravet på synnerlig vikt inryms också ett behovskrav. Det

man vill åstadkomma ska i princip inte vara åtkomligt med mindre ingripande metoder. Brottsutredningen ska som huvudregel inte kunna föras framåt med andra medel och det ska finnas skäl att räkna med att åtgärden verkligen kan få effekt (prop. 2013/14:237 s. 94–95). Genom kravet på synnerlig vikt för utredningen skapas därmed indirekt en koppling mellan de övervakade adresserna eller utrustningarna och brottet. Möjligheten att använda hemlig övervakning i detta syfte infördes främst för att det fanns ett stort behov av uppgifterna redan i ett tidigt skede av utredningen, innan det fanns någon misstänkt. I förarbetena till bestämmelsen anges det tydligt att regleringen inte skulle innebära någon utvidgning av möjligheterna att använda tvångsmedlet mot en skäligen misstänkt person. I motiven till bestämmelsen anges även att åklagare och domstol bör begränsa tillståndet så att mängden överskottsinformation minimeras (prop. 2011/12:55 s. 73–74 och 130). Detta följer också av proportionalitetsprincipen.

Utrymmet för att använda hemlig övervakning av elektronisk kommunikation för att utreda vem som är misstänkt är som beskrivs ovan 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 det finns en indirekt koppling till brottsligheten genom kravet på synnerlig vikt, att inhämtningen är begränsad (sett till de uppgifter som får inhämtas) och till att den brottslighet som berättigar till sådan övervakning är mycket allvarlig eller samhällsfarlig, delar regeringen utredningens bedömning att det utrymme som EU-domstolen ger är tillräckligt för att de svenska reglerna i detta hänseende ska lämnas oförändrade. Ingen remissinstans invänder mot denna bedömning. Reglerna om tillgång genom hemlig övervakning av elektronisk kommunikation uppfyller således de krav som EU-rätten ställer i detta avseende.

Inhämtningslagen

Enligt inhämtningslagen inhämtas uppgifter endast i underrättelseverksamhet. Inhämtning får ske om åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet för brott där det inte är föreskrivet lindrigare straff än fängelse i två år (2 §) eller vissa samhällsfarliga brott som t.ex. sabotage, spioneri eller grov terrorismrelaterad brottslighet (3 §).

På underrättelsestadiet saknas kunskap om ett specifikt brott. Av naturliga skäl blir det därmed svårt att tala om någon misstänkt person på det sätt som uttrycket används i rättegångsbalken. Även om underrättelseanalysen inte alltid kan peka ut ett specifikt brott eller en misstänkt person så inriktas underrättelsearbetet ändå 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 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 inte möjligt att precisera personkretsen mer. Kravet att åtgärden ska vara av

särskild vikt för att förebygga, förhindra eller upptäcka viss brottslig verksamhet innefattar dessutom både ett kvalitetskrav på de upplysningar som åtgärden kan ge och ett krav på behovet av inhämtningen i det enskilda fallet. Bedömningen får inte bygga enbart på spekulationer eller allmänna antaganden utan måste grundas på faktiska omständigheter. Det kan således inte bli fråga om att rutinmässigt inhämta uppgifter i syfte att kartlägga personer enbart på grund av att de är kriminellt belastade eller ingår i en viss grupp eller ett visst nätverk (prop. 2011/12:55 s. 121). På samma sätt som beskrivs ovan angående hemlig övervakning av elektronisk kommunikation enligt rättegångsbalken finns det således indirekt en koppling mellan de övervakade adresserna eller utrustningarna och brottet. Brottsligheten det är fråga om är dessutom av mycket allvarlig art eller samhällsfarlig. Regeringen delar utredningens bedömning att de svenska reglerna får anses uppfylla de villkor som har uppställts av EU-domstolen. Ingen remissinstans invänder mot denna bedömning.

Preventivlagen

Som anges i avsnitt 6.1 får tillstånd till hemlig övervakning av elektronisk kommunikation enligt preventivlagen endast ges om det finns en påtaglig risk för att en person kommer att utöva brottslig verksamhet som avser en rad närmare preciserade allvarliga eller samhällshotande brott såsom t.ex. mord, människorov, terroristbrott eller sabotage (1 § första stycket).

Tillstånd får också ges om det finns påtaglig risk för att det inom en organisation eller grupp kommer att utövas sådan brottslig verksamhet som omfattas av lagen och det kan befaras att en person som tillhör eller verkar för organisationen eller gruppen medvetet kommer att främja denna verksamhet (1 § andra stycket). Även om det inte uttryckligen framgår av bestämmelsens ordalydelse så är det endast mot den personen som medvetet kommer att främja den brottsliga verksamheten som den hemliga tvångsåtgärden får riktas (prop. 2013/14:237 s. 108). Det krävs inte någon precisering av den eller de personer inom gruppen som risken ska knytas till, men det ska finnas en koppling mellan gruppen eller organisationen och den brottsliga verksamheten. Bedömningen av om det kan befaras att en person medvetet kommer att främja den brottsliga verksamheten ska grundas på konkreta omständigheter. Sådana omständigheter kan i vissa fall vara personens ställning i gruppen, liksom om personen tidigare dömts för brottslighet som är relevant i sammanhanget. Det ska finnas objektivt fastställbara tecken på att personen kommer att vidta någon åtgärd som innebär ett främjande. Endast medlemskap i organisationen är inte tillräckligt. Med främjande avses detsamma som i medverkansbestämmelserna i brottsbalken, även om gärningen inte behöver konkretiseras närmare (prop. 2013/14:237 s. 109 och 196).

Tillstånd får vidare 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 (2 §).

Regleringen innebär alltså att personkretsen som kan komma att bli utsatt för tvångsåtgärder enligt preventivlagen är begränsad och kan hänföras till en förmodad brottslig verksamhet. Bedömningen ska bygga på faktiska omständigheter och inte på antaganden. Dessutom ska den övervakade adressen på ett visst sätt vara knuten till den person som tvångsmedelsbeslutet avser. Av samma skäl som tillgångsreglerna vid hemlig övervakning av elektronisk kommunikation bedöms förenliga med EU-rätten gör regeringen, i likhet med utredningen, bedömningen att även preventivlagen uppfyller EU-rättens krav i detta hänseende.

Lagen om särskild utlänningskontroll

Som framgår i avsnitt 6.1 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 om straff för terroristbrott och det finns synnerliga skäl (19 och 20 § lagen om särskild utlänningskontroll).

Av samma skäl som tillgångsreglerna vid hemlig övervakning av elektronisk kommunikation bedöms förenliga med EU-rätten delar regeringen utredningens bedömning att även lagen om särskild utlänningskontroll uppfyller EU-rättens krav i detta hänseende.

6.5 Förhandskontroll av domstol eller oberoende myndighet

Regeringens förslag: Åklagare vid Åklagarmyndigheten ska besluta om tillstånd för inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet enligt inhämtningslagen.

Ansökan ska göras av Polismyndigheten, Säkerhetspolisen respektive Tullverket.

Skyldigheten att omedelbart häva ett beslut som det inte finns skäl för och skyldigheten att underrätta Säkerhets- och integritetsskyddsnämnden om ett beslut om inhämtning enligt inhämtningslagen ska även fortsättningsvis vila på Polismyndigheten, Säkerhetspolisen respektive Tullverket. Detta ska tydliggöras i lagtexten.

Regeringens bedömning: Beslut om tillstånd för inhämtning enligt inhämtningslagen bör inte kunna överklagas. Det finns inte heller behov av interimistiska beslut enligt inhämtningslagen. Det behövs ingen uttrycklig bestämmelse i inhämtningslagen om att underrättelseskyldigheten till Säkerhets- och integritetsskyddsnämnden ska fullgöras genom att beslutet lämnas till nämnden.

Reglerna i rättegångsbalken, preventivlagen och lagen om särskild utlänningskontroll uppfyller EU-rättens krav på att inhämtning av lagrade uppgifter ska beslutas av domstol eller en oberoende myndighet.

Datalagringsutredningens förslag överensstämmer inte med regeringens. Utredningen föreslår att det ska framgå av lagtexten att underrättelseskyldigheten om ett beslut om inhämtning till Säkerhets- och integritetsskyddsnämnden ska fullgöras genom att beslutet lämnas till nämnden.

Remissinstanserna: De flesta remissinstanser kommenterar inte förslaget särskilt. *Tele2 Sverige AB* och *Sveriges advokatsamfund* tillstyrker förslaget.

Utredningens förslag och bedömning överensstämmer med regeringens.

Remissinstanserna: *Hovrätten för Övre Norrland, Stockholms tingsrätt, Säkerhetspolisen, Datainspektionen, Sveriges advokatsamfund* och *Tele2 Sverige AB* tillstyrker eller har ingen invändning mot att beslut om inhämtning enligt inhämtningslagen ska fattas av åklagare. *Stockholms tingsrätt* anser att utredningens resonemang om varför allmänna domstolar inte bör fatta beslut enligt inhämtningslagen framstår som väl underbyggt. Om en ordning med domstolsprövning skulle införas, finns det dock ingen invändning mot att Stockholms tingsrätt blir exklusivt forum. *Tele2 Sverige AB* poängterar att det måste säkerställas att de åklagare som tilldelas beslutsbehörighet genomgår relevant utbildning och att beslutsbehörigheten inte sprids bland de olika åklagarkamrarna, utan tilldelas en centralt placerad grupp med särskild kompetens. *Telia Sverige AB* anser att det är väsentligt att det finns förhandsbeslut av domstol eller oberoende myndighet för att få tillgång till lagrade uppgifter.

Åklagarmyndigheten, Polismyndigheten och *Tullverket* delar utredningens bedömning att den nuvarande beslutsordningen i inhämtningslagen behöver ändras. Myndigheterna anser dock att man bör överväga andra alternativ än åklagare för beslutsfattandet. De anför bl.a. att åklagares objektivitetsplikt gör att de bör hålla distans till underrättelseverksamheten. *Åklagarmyndigheten* anser att det måste krävas starka skäl för att åklagare ska tilldelas en roll i polisens allmänna underrättelsearbete, men har förståelse för de argument som utredningen har för valet av åklagare eftersom det är den enda befintliga myndighet som har de praktiska förutsättningarna att möta de krav som bör ställas på en beslutsmyndighet enligt inhämtningslagen. Om åklagare utses till beslutsfattare kommer det kräva en särskild organisation inom myndigheten där ett begränsat antal åklagare bör involveras i beslutsfattandet. *Polismyndigheten* anser att det bör säkerställas att åklagare har tillräcklig kunskap för att skydda underrättelseuppgifter och att det finns en systematik för att hålla underrättelseuppgifter skilda från förundersökningsmaterial.

Svea hovrätt anser att beslutsfattandet enligt inhämtningslagen bör flyttas till en oberoende myndighet och att den lämpligaste lösningen vore en särskild inrättad nämnd. Åklagare skulle, enligt hovrätten, kunna fylla funktionen men av samma skäl som utredningen anför beträffande allmän domstol framstår det inte som en lämplig ordning. *Malmö tingsrätt* anser att

det kan ifrågasättas om åklagare uppfyller EU-rättens krav på oberoende och anser att en särskild nämnd skulle vara mer lämpad för uppgiften. *Göteborgs tingsrätt* efterfrågar en mer utförlig analys av om Åklagarmyndigheten kan anses utgöra en oberoende myndighet såsom EU-rätten föreskriver. Bl.a. *Dataskydd.net* och *Föreningen för Digitala fri- och rättigheter (Dfri)* är kritiska till förslaget och anser att åklagare inte kan anses vara oberoende eftersom de är en del av brottsbekämpningen.

Skälen för regeringens förslag och bedömning

Domstolsbeslut krävs redan för inhämtning enligt rättegångsbalken, preventivlagen och lagen om särskild utlänningskontroll

Som framgår i avsnitt 6.2 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.

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.

Även enligt preventivlagen krävs som huvudregel domstolsbeslut innan tillstånd till tvångsmedel kan ges (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 dock tillstånd till åtgärden ges av åklagaren i avvaktan på rättens beslut. Ett sådant beslut ska underställas rättens prövning (6 a §).

Domstolsbeslut krävs också för tillstånd till hemlig övervakning av elektronisk kommunikation enligt lagen om särskild utlänningskontroll (21 §). Någon möjlighet till interimistiska beslut finns inte enligt denna lag.

Utredningen bedömer att reglerna om domstolsprövning i rättegångsbalken, preventivlagen och lagen om särskild utlänningskontroll lever upp till EU-rättens krav. Ingen remissinstans invänder mot detta. Regeringen instämmer i utredningens bedömning.

Beslutsordningen enligt inhämtningslagen bör ändras

Inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamhet enligt inhämtningslagen får beslutas av Polismyndigheten, Säkerhetspolisen och Tullverket. Datalagringsutredningen bedömer att det inte finns skäl att göra några förändringar i beslutsordningen. Bedömningen var föremål för sedvanligt remissförfarande. Därefter meddelades Tele2-domen. Mot bakgrund av uttalandena i Tele2-domen bedömer Utredningen om datalagring och EU-rätten att beslutsordningen i inhämtningslagen bör ändras. Remissinstanserna delar denna bedömning eller har ingen invändning

mot den. I likhet med utredningen och remissinstanserna anser regeringen att beslutsfattandet enligt inhämtningslagen bör ändras och anförtros en domstol eller annan oberoende myndighet. Regeringen väljer mot denna bakgrund att inte redogöra för de remissvar som lämnats med anledning av Datalagringsutredningens betänkande i denna fråga.

Frågan är då vilken myndighet som bör anförtros beslutsfattandet enligt inhämtningslagen. För den här typen av beslutsfattande om hemliga tvångsmedel står valet mellan allmän domstol, särskild nämnd eller åklagare. Dessa olika alternativ behandlas nedan. En utgångspunkt för regeringen är att verksamhet, om möjligt, bör organiseras inom ramen för den befintliga myndighetsorganisationen. En ny myndighet bör inrättas bara om det är nödvändigt med hänsyn till EU-rättens krav.

Allmän domstol fattar beslut om inhämtning av elektronisk kommunikation i förundersökningsverksamhet. 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. I underrättelseverksamheten är dock situationen en annan. Som anfördes i förarbetena till inhämtningslagen (prop. 2011/12:55 s. 88–89) och som båda utredningarna konstaterar finns det nackdelar med att låta domstolar ha en roll som beslutsorgan enligt inhämtningslagen. Beslut enligt lagen fattas i underrättelseverksamhet, där andra intressen gör sig gällande än under en förundersökning. Underrättelseverksamheten är nämligen främst inriktad mot att, utifrån en mer övergripande ansats, studera och kartlägga en befarad brottslig verksamhet för att förebygga eller förhindra att brottsligheten genomförs, till skillnad från förundersökningen som inriktar sig mot ett redan begånget konkret brott och vem som kan misstänkas för det. Integritetsaspekten präglas i underrättelseskedet mer av ett medborgarperspektiv än av ett sådant tvåpartsförfarande som särskilt lämpar sig för rättslig prövning i allmän domstol. Trots att beslutsfattande enligt preventivlagen ligger på domstol så är underrättelseverksamhet typiskt sett främmande för de allmänna domstolarna. I preventivlagens fall är det dessutom så att den huvudsakligen tillämpas i situationer när en förundersökning är nära förestående, vilket inte kan sägas vara fallet när det gäller inhämtningslagen. Slutligen är inte domstolsväsendet ordnat på så sätt att det kan erbjuda det snabba beslutsfattande som kan behövas i ärenden enligt inhämtningslagen. Regeringen, liksom *Stockholms tingsrätt,* delar därför utredningens bedömning att allmän domstol inte bör utses som beslutsorgan.

Utredningen överväger om Säkerhets- och integritetsskyddsnämnden (SIN) skulle kunna fatta beslut enligt inhämtningslagen men kommer fram till att detta vore olämpligt dels mot bakgrund av myndighetens uppdrag att utöva tillsyn över verksamheten, dels då SIN inte är organiserad för en sådan beredskap som skulle behövas för att kunna fatta de snabba beslut som ibland behövs i underrättelseverksamhet. Regeringen delar den bedömningen.

Av redan existerande myndigheter återstår då att överväga om åklagare bör bli beslutsfattare enligt inhämtningslagen. Åklagare utgör en central del i rättskedjan. Trots att 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 förundersökningsstadiet) som ett ärende befinner sig i. Trots att åklagarnas kärnverksamhet är förundersökningsverksamheten och rollen som processförare i domstol, finns det redan i dag i viss utsträckning åklagare som har uppgifter inom ramen för underrättelseverksamhet. Det rör sig här främst om tillämpningen av preventivlagen. Därutöver har åklagare i viss begränsad utsträckning en roll i polisens regionala underrättelsecenter (RUC). Åklagare utför således i dag arbetsuppgifter på relevant område för inhämtningslagen. Även om just dessa arbetsuppgifter inte är särskilt spridda i organisationen kan det 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. Regeringen anser därför att den omständigheten att beslutsfattandet rör ett område utanför kärnverksamheten inte i sig bör utgöra något hinder mot en ordning med åklagare som beslutsfattare.

Både utredningen och några remissinstanser, t.ex. *Åklagarmyndigheten, Polismyndigheten, Tullverket* och *Malmö tingsrätt*, tar upp frågan om åklagares objektivitet skulle kunna ifrågasättas om de skulle ha till uppgift att pröva och godkänna olika åtgärder i underrättelseverksamheten. Åklagarmyndigheten påpekar att objektivitetsplikten gör att åklagare bör hålla distans till underrättelseverksamheten och att det kan uppstå svårigheter i avgränsningen mellan förundersökning och underrättelseverksamhet. Enligt regeringen är det viktigt att åklagarnas objektivitetsplikt inte på något sätt urholkas av föreslagna förändringar. Frågan är då om det kan finnas en risk för att enskildas förtroende för åklagarnas objektivitetsplikt skulle kunna undergrävas genom att åklagare skulle kunna förmodas hålla kvar ett ärende i underrättelsestadiet för att därigenom lättare få tillgång till uppgifter om elektronisk kommunikation enligt inhämtningslagen i stället för att behöva vända sig till domstol och söka ett tillstånd till hemlig övervakning av elektronisk kommunikation. Regeringen kan konstatera att en åklagares objektivitetsplikt inte bara gäller under förundersökningen utan även i underrättelsestadiet (23 kap. 4 § tredje stycket RB). Enligt regeringen finns det inte något som talar i riktning mot att åklagare skulle frestas att hålla kvar ett ärende i underrättelsestadiet.

Göteborgs tingsrätt efterfrågar en mer utförlig analys av om Åklagarmyndigheten kan anses utgöra en oberoende myndighet såsom EU-rätten föreskriver. *Dataskydd.net* och *Föreningen för Digitala fri- och rättigheter (Dfri)* anser att åklagare inte kan anses uppfylla kraven på oberoende eftersom de är en del av brottsbekämpningen precis som polisen. Som utredningen konstaterar innebär den svenska förvaltningsmodellen att åklagare, i likhet med andra myndigheter, vid sitt beslutsfattande är helt självständiga. Av 12 kap. 2 § regeringsformen framgår att ingen myndighet får bestämma hur en annan förvaltningsmyndighet i ett särskilt fall ska besluta i ett ärende som rör myndighetsutövning mot en enskild. Åklagarna är alltså självständiga i sitt beslutsfattande både i förhållande till andra

myndigheter, som t.ex. Polismyndigheten och Säkerhetspolisen, och i förhållande till den verkställande makten, dvs. regeringen. Även inom myndigheten är åklagare helt självständiga i sitt beslutsfattande. När en åklagare fattar beslut i den brottsbekämpande verksamheten är det åklagaren personligen som har rätt att besluta och som därmed bär tjänsteansvaret. Även om åklagarväsendet är hierarkiskt uppbyggt får inte en högre åklagare ge bindande instruktioner till en lägre åklagare om vilka beslut han eller hon ska fatta. En annan sak är att en högre åklagare kan överta en arbetsuppgift av en lägre åklagare (7 kap. 5 § RB). Ytterligare en komponent i frågan om oberoende är anställningsformen. Här finns skäl att lyfta fram en rapport från Venedigkommissionen (en rådgivande kommission till Europarådet i konstitutionella frågor) som handlar om åklagares oberoende (European Standards as regards the independence of judicial system: Part II – The Prosecution Service, European Comission for Democracy Through Law, [Venice Commission], december 2010). Riksåklagaren har som landets högsta allmänna åklagare ett förstärkt anställningsskydd och anställs som en av få myndighetschefer med fullmakt (7 kap. 3 § RB). Även vice riksåklagaren har samma anställningsskydd. En sådan anställning går mycket väl i linje med kommissionens rekommendationer i rapporten (punkt 37). Möjligheten att skilja riksåklagaren från ämbetet är klart definierade i 4 § lagen (1994:261) om fullmaktsanställning, vilket även det går väl i linje med rekommendationerna från Venedigkommissionen (punkt 39). Övriga åklagare har dock inte samma starka anställningsskydd som riksåklagaren och vice riksåklagaren. De allra flesta åklagare är dock anställda tills vidare och omfattas därigenom av det starka svenska anställningsskyddet. Det innebär att åklagare som utgångspunkt är anställda till dess att de går i pension, vilket också är en rekommendation av kommissionen (punkt 50). Mot bakgrund av det anförda anser regeringen att åklagare uppfyller det EU-rättsliga kravet på oberoende myndighet.

Åklagare har som utgångspunkt generell befogenhet att utöva sitt ämbete, 6 § åklagarförordningen (2004:1265). Regeringen delar dock *Åklagarmyndighetens, Polismyndighetens* och *Tele2 Sverige AB:s* inställning att det kan finnas skäl att inrätta en särskild organisation inom Åklagarmyndigheten där ett begränsat antal åklagare involveras i nu aktuellt beslutsfattande, bl.a. för att upprätthålla förtroendet för åklagarnas objektivitet och för att kunna säkerställa kunskapsnivån hos beslutsfattarna.

Om åklagare får en roll som beslutsfattare enligt inhämtningslagen 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 polisens brottsdatalag och åklagarväsendets brottsdatalag. Härutöver finns bestämmelser om sekretess i offentlighets- och sekretesslagen (2009:400), OSL. Enligt regeringens 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. Åklagarväsendets brottsdatalag 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. OSL.

Sammanfattningsvis leder det sagda till slutsatsen att i valet mellan de olika alternativ som finns för beslutsfattande enligt inhämtningslagen, framstår åklagare som det bästa alternativet av redan befintliga myndigheter. Enligt regeringens bedömning bör därför åklagare vid Åklagarmyndigheten anförtros uppgiften att fatta beslut om inhämtning enligt inhämtningslagen.

Några remissinstanser – *Svea hovrätt, Malmö tingsrätt* och *Tullverket* – förordar att en särskild nämnd ska stå för beslutsfattandet. Även utredningen för ett sådant resonemang utan att lämna något förslag i den delen. Polismetodutredningen föreslår i sitt betänkande Särskilda spaningsmetoder (SOU 2010:103) att det bör inrättas en särskild nämnd som ska 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. Det förslaget bereds alltjämt i Regeringskansliet, vilket innebär att någon sådan nämnd inte finns för närvarande. Det går därför inte att bedöma om en sådan nämnd skulle kunna vara mer lämpad än åklagare att besluta om tillstånd till inhämtning enligt inhämtningslagen. Enligt regeringens bedömning kan det – om Polismetodutredningens förslag genomförs i denna del – finnas skäl att överväga att lägga beslutsbefogenheten på denna nämnd i stället för på åklagare.

Ansökan om tillstånd enligt inhämtningslagen bör upprättas av Polismyndigheten, Säkerhetspolisen respektive Tullverket

Eftersom inhämtningslagen föreskriver att myndigheterna själva får fatta beslut om inhämtning finns det av uppenbara skäl inga regler i inhämtningslagen om vilken myndighet som ska upprätta ansökningar om tillstånd. När nu beslutsbehörigheten föreslås placeras på åklagare måste det dock införas sådana regler. Eftersom inhämtning enligt inhämtningslagen görs i Polismyndighetens, Säkerhetspolisens respektive Tullverkets intresse bör det enligt regeringen föreskrivas att ansökningarna upprättas av respektive myndighet. Ingen remissinstans invänder mot förslaget i denna del.

Det finns inte skäl att införa en möjlighet till interimistiska beslut i inhämtningslagen

EU-rätten lämnar ett utrymme för interimistiska beslut i brådskande fall. En sådan ordning skulle kunna ge Polismyndigheten, Säkerhetspolisen och Tullverket rätt att i brådskande fall själva besluta om inhämtning, med en efterföljande prövning av beslutet av åklagare.

En sådan ordning är dock inte helt oproblematisk. I princip samtliga beslut enligt inhämtningslagen avser uppgifter i förfluten tid. När prövningen sedan ska göras av åklagare skulle således uppgifter i de flesta fallen redan ha levererats till myndigheten. Det skulle alltså behövas regler om vad följden blir om åklagaren upphäver beslutet om inhämtning, i likhet med vad som gäller för interimistiska beslut om hemliga tvångsmedel under en förundersökning (jfr 27 kap. 21 a § RB). Att föreskriva att sådana uppgifter inte får användas i en förundersökning är logiskt eftersom uppgifterna då inte kan användas som bevisning. I underrättelseverksamheten är det emellertid mer oklart vad en sådan bestämmelse skulle få för praktiska följder. En bestämmelse som t.ex. innebär att myndigheten skulle bortse från information som den redan känner till och som exempelvis skulle kunna användas för att förhindra grova brott framstår inte som en lämplig ordning.

Dessutom synes behovet av att kunna fatta interimistiska beslut inte heller vara särskilt påtagligt om beslutsfattandet ligger hos åklagare, eftersom det för dem finns rutiner för jour- och beredskapstjänstgöring (13 § åklagarförordningen [2004:1265]).

Regeringen anser därför, i likhet med utredningen, att det inte bör införas någon interimistisk beslutsmöjlighet. Ingen remissinstans invänder mot denna bedömning.

Beslut enligt inhämtningslagen bör inte kunna överklagas

Åklagarbeslut är som huvudregel inte överklagbara. Regeringen instämmer i utredningens bedömning att det inte har framkommit något skäl att behandla beslut om inhämtning enligt inhämtningslagen på annat sätt. Ingen remissinstans invänder mot denna bedömning. 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.

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).

Skyldigheten att omedelbart häva beslut enligt inhämtningslagen bör ligga hos den ansökande myndigheten

I ett beslut om inhämtning ska det bl.a. anges vilken tid 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 (5 §). Även om det initiala beslutet nu föreslås fattas av åklagare anser regeringen, i likhet med utredningen, att skyldigheten att häva beslutet fortfarande bör vila på Polismyndigheten, Säkerhetspolisen och Tullverket. Skälet till det är att de nämnda myndigheterna har bäst förutsättningar att bedöma om det inte längre finns 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. Ingen remissinstans invänder mot denna bedömning.

Underrättelse till Säkerhets- och integritetsskyddsnämnden bör göras av den ansökande myndigheten

Säkerhets- och integritetsskyddsnämnden (SIN) har i uppdrag att utöva tillsyn över bl.a. de brottsbekämpande myndigheternas användning av hemliga tvångsmedel och därmed sammanhängande verksamhet (1 § lagen [2007:980] om tillsyn över viss brottsbekämpande verksamhet). Att tillsynen även avser med tvångsmedelsanvändningen sammanhängande verksamhet innebär att både själva övervakningen och den vidare hanteringen av uppgifterna omfattas, t.ex. hantering av överskottsinformation och att reglerna om underrättelseskyldighet följs.

Polismyndigheten, Säkerhetspolisen och Tullverket har alltså en skyldighet att bl.a. underrätta SIN om ett beslut om inhämtning enligt inhämtningslagen. Underrättelsen ska lämnas senast en månad efter det att ärendet om inhämtning avslutades (6 §). Även om beslutsrätten enligt inhämtningslagen 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. Ingen remissinstans invänder mot denna bedömning. Att underrättelseskyldigheten ska fullgöras av den ansökande myndigheten bör framgå av lagtexten.

Datalagringsutredningen föreslår att det i lagtexten även bör tydliggöras att underrättelseskyldigheten till SIN ska fullgöras genom att själva beslutet lämnas till nämnden. Av vad som upplysts till utredningen uppfyller de flesta sin underrättelseskyldighet genom att sända en kopia av besluten till SIN, men det har dock hänt att SIN underrättats om fattade beslut på annat sätt, t.ex. genom en särskild skrivelse som sannolikt inte utgör beslutet, och i vissa fall uppkommer frågan om SIN verkligen fått del av beslutet. Enligt SIN bör problemet dock inte överdrivas. Regeringen instämmer i att det bör vara själva beslutshandlingen som tillställs SIN, vilket också är det underrättelsesätt som använts i praktiken i huvuddelen av fallen. Regeringen anser dock inte att det finns ett behov av en särskild föreskrift om detta i lagen. SIN har dessutom rätt att få de uppgifter och det biträde som nämnden begär (4 § lagen om tillsyn över viss brottsbekämpande verksamhet). För det fall SIN anser att underlaget som lämnas till nämnden inte är komplett eller oklart, finns det således möjlighet att påpeka detta och få de kompletteringar som behövs.

6.6 Information till berörda om att inhämtning skett

Regeringens bedömning: Reglerna i rättegångsbalken, preventivlagen och inhämtningslagen om information till berörda om att inhämtning skett uppfyller EU-rättens krav. Avsaknaden av regler om information till berörda i lagen om särskild utlänningskontroll är förenlig med EU-rätten.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanser kommenterar inte bedömningen särskilt. *Civil Rights Defenders* ställer sig tveksamma till de undantag från underrättelseskyldigheten som går längre än att endast skjuta upp en underrättelse till de berörda.

Skälen för regeringens bedömning

Informationsskyldigheten och EU-rättens krav

EU-domstolen slår fast att EU-rätten kräver att de myndigheter som har beviljats tillgång till lagrade uppgifter, enligt tillämpliga nationella förfaranden, informerar de berörda personerna om det så snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar (punkt 121 i Tele2-domen). 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. Motsvarande informationsskyldighet till berörda personer gäller som huvudregel även enligt Europakonventionen (se t.ex. Roman Zakharov mot Ryssland, 4 december 2015, mål nr 47143/06, punkterna 287–288).

Syftet med underrättelseskyldigheten är alltså 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 görs 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.

Det har emellertid ansetts nödvändigt att förena underrättelseskyldigheten med vissa undantag, däribland möjligheten att skjuta upp eller avstå från en underrättelse för att inte skada den brottsutredande verksamheten eller intresset av att inte behöva avslöja verksamhetens inriktning eller arbetsmetoder överlag. Europadomstolen har mot den bakgrunden i vissa fall godtagit att någon underrättelse inte lämnats till den berörda om det finns andra kontrollsystem att tillgripa, t.ex. möjligheter att begära ett tillsynsorgans kontroll av om en person varit föremål för en hemlig tvångsåtgärd i strid med lag (se t.ex. Kennedy mot Förenade Kungariket, 18 maj 2010, mål nr 26839/05, punkt 167 och Roman Zakharov mot Ryssland, 4 december 2015, mål nr 47143/06, punkt 288).

Hemlig övervakning av elektronisk kommunikation

Den som har varit utsatt för hemliga tvångsmedel enligt rättegångsbalken ska som huvudregel underrättas om detta så snart det kan ske utan men för utredningen, dock senast inom en månad efter att förundersökningen avslutades (27 kap. 31 § RB). Det finns vissa möjligheter att skjuta upp underrättelsen om de uppgifter som den ska innehålla omfattas av vissa former 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 Säkerhets- och integritetsskyddsnämnden (SIN) underrättas om beslutet att avstå från underrättelse (14 b § andra stycket förundersökningskungörelsen [1947:948]). Vissa brott som faller inom Säkerhetspolisens ansvarsområde, i fråga om utredningar om sabotagebrott, brott mot rikets inre och yttre säkerhet samt terroristbrott, är helt undantagna från underrättelseskyldigheten (27 kap. 33 § tredje stycket RB).

Om övervakningen 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 underrättelse inte lämnas (27 kap. 31 § andra stycket RB). Någon underrättelse behöver inte heller lämnas till den som redan fått del av eller tillgång till uppgifterna eller om underrättelsen med hänsyn till omständigheterna uppenbart är utan betydelse (27 kap. 31 § femte stycket RB).

Vid användningen av hemlig övervakning av elektronisk kommunikation finns det alltså föreskrivet en underrättelseskyldighet gentemot den enskilde. EU-domstolen anger att risk för skada för utredningen kan motivera en uppskjuten underrättelse till den enskilde. De svenska bestämmelserna ger större möjligheter 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 § OSL). 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 inte vara rimligt om skydd för landets försvar inte skulle få åberopas medan det är möjligt att skjuta upp en underrättelse för att skydda en brottsutredning. Även sekretess för att skydda polisens arbetsmetoder bör rimligen få åberopas till stöd för att skjuta upp underrättelse (18 kap. 1 § OSL). I likhet med utredningen anser regeringen att de svenska reglerna för att kunna skjuta upp underrättelse bör kunna bibehållas.

Civil Rights Defenders ställer sig tveksamma till undantag från underrättelseskyldigheten som går längre än att endast skjuta upp en underrättelse till de berörda. EU-domstolen gör emellertid ingen bedömning av den situationen att det är fråga om att helt avstå från en underrättelse till den enskilde. Domstolen berör endast uppskjuten underrättelse. Att den svenska rättsordningen i vissa fall föreskriver en möjlighet att helt avstå från underrättelse till den enskilde bedömer regeringen inte stå i strid med EU-rätten. Endast i de fall tvångsmedelsanvändningen avser vissa brott som

utreds av Säkerhetspolisen kan underrättelse underlåtas helt och hållet. Utrymmet för staten att avvika från skyddsreglerna för att värna sina vitala intressen är också något som bejakas av domstolen (punkt 119). Dessutom säkerställs att tvångsmedelsanvändningen har skett på ett korrekt sätt genom att SIN underrättas i de fall den enskilde inte underrättas på grund av sekretess (14 b § förundersökningskungörelsen).

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 regeringen finns det två skäl som talar för att EU-rätten inte utgör hinder för att en sådan ordning bibehålls. Det första är att EU-domstolen ger medlemsstaterna visst nationellt handlingsutrymme i denna fråga genom att hänvisa till ”tillämpliga nationella förfaranden”. 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. 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. Något egentligt behov av en rättslig prövning torde således inte uppstå för dessa personer. Det ska även i sammanhanget noteras att den behandling av de icke misstänktas person-uppgifter som utförs hos polisen och Tullverket är kringgärdad av ett integritetsskyddande regelverk i form av bl.a. polisens brottsdatalag och Tullverkets brottsdatalag.

Utöver att de brottsbekämpande myndigheterna ska underrätta SIN i de fall den enskilde inte underrättas, kan en enskild själv begära att SIN ska 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 (3 § lagen [2007:980] om tillsyn över viss brottsbekämpande verksamhet). Det finns inget krav på att den enskilde ska ange något skäl för sin begäran eller att det ska finnas en konkret misstanke om att personen är föremål för en hemlig tvångsåtgärd. Den enskilde ska underrättas om att kontrollen har utförts. Om SIN bedömer att det förekommit felaktigheter som kan medföra skadeståndsansvar för staten gentemot den enskilde ska det anmälas till Justitiekanslern. Om SIN i stället bedömer att det förekommit felaktigheter som innefattar misstanke om brott ska ärendet anmälas till Åklagarmyndigheten eller annan behörig myndighet. Vidare har nämnden en viss anmälningsskyldighet till Datainspektionen i fråga om brister vid behandling av personuppgifter (20 § förordningen [2007:1141] med instruktion för Säkerhets- och integritetsskyddsnämnden). Därutöver kan Justitiekanslern och Riksdagens ombudsmän på eget initiativ eller efter klagomål från enskilda utöva tillsyn över verksamheten. Justitiekanslern kan också besluta om skadestånd till enskilda t.ex. på grund av myndighets-utövning som innefattar olaglig användning av hemliga tvångsmedel. Även Datainspektionen kan ta emot och undersöka klagomål gällande person-uppgiftsbehandling.

Europadomstolen har godtagit att underrättelse inte lämnas till den berörde när liknande kontrollsystem funnits att tillgå (jfr. Kennedy mot Förenade kungariket, 18 maj 2010, mål nr 26839/05, punkt 167 och Roman Zakharov mot Ryssland, 4 december 2015, mål nr 47143/06, punkt 288).

Regeringen gör mot den angivna bakgrunden bedömningen att rättegångsbalkens regler om uppskjuten och underlåten underrättelse är förenliga med de krav som EU-rätten uppställer.

Inhämtningslagen

När det gäller inhämtning av uppgifter i underrättelseverksamhet enligt inhämtningslagen finns ingen motsvarighet till rättegångsbalkens krav på underrättelse till enskild. För inhämtningslagen 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 § inhämtningslagen).

Frågan om ett krav på underrättelse till enskild borde införas övervägdes i samband med att lagen infördes. Regeringen uttalade då att en skyldighet att underrätta enskilda om inhämtning av uppgifter i underrättelseverksamhet, med hänsyn till verksamhetens framåtblickande perspektiv och övergripande natur, skulle riskera att motverka huvudsyftet med underrättelseverksamheten. 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 skulle kunna 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 rättegångsbalken bli tillämpliga (prop. 2011/12:55 s. 107).

Det bör också noteras att i vissa fall är identiteten på den som omfattas av inhämtning enligt inhämtningslagen 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 inhämtningslagen omfattas uppgifterna av sekretess – företrädelsevis enligt 18 kap. 1 och 2 §§ OSL som bl.a. avser skydd för uppgifter i underrättelseverksamhet och i verksamhet för att förebygga, uppdaga, utreda eller beivra brott – som är särskilt viktig att bibehålla. Det är här fråga om den av typ av sekretess som till och med innebär att tystnadsplikten för uppgift om brottsbekämpande myndigheters inhämtning av uppgifter om elektronisk kommunikation i underrättelseverksamheten har företräde framför rätten att meddela och offentliggöra uppgifter enligt tryckfrihetsförordningen eller yttrandefrihetsgrundlagen, den s.k. meddelarfriheten (se 18 kap. 19 § och 44 kap. 4 § OSL, prop. 2011/12:55 s. 115–116). Dessutom är den brottslighet som är aktuell vid inhämtning enligt inhämtningslagen mycket angelägen att bekämpa effektivt. Det rör sig

nämligen om allvarlig brottslighet, antingen sett till de straff som kan utdömas (2 §) eller sett till att brotten riktar sig mot centrala delar av samhället och staten (3 §).

Som framgår ovan när det gäller hemlig övervakning av elektronisk kommunikation anser regeringen att det finns ett visst utrymme att avstå från underrättelse. Enligt regeringens bedömning inbegriper detta en ordning där information till de berörda över huvud taget inte föreskrivs vid inhämtning av uppgifter i underrättelseverksamheten. Regeringen beaktar vid denna bedömning 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 inhämtningslagen och om inhämtningen och behandlingen av uppgifterna varit lagenlig (3 § lagen om tillsyn över viss brottsbekämpande verksamhet). SIN underrättas också om beslut om inhämtning av uppgifter enligt inhämtningslagen (6 §) och utövar tillsyn över verksamheten. Som framgår i föregående avsnitt finns också andra effektiva rättsmedel i form av de verktyg som Justitiekanslern, Riksdagens ombudsmän och Datainspektionen har till sitt förfogande. Regeringen delar därför, till skillnad från *Civil Rights Defenders*, utredningens bedömning att inhämtningslagens regler i detta avseende är förenliga med EU-rätten.

Preventivlagen

Enligt preventivlagen ska en underrättelse lämnas till den som blivit utsatt för inhämtning av uppgifter om brottslig verksamhet som innefattar mord, dråp, grov eller synnerligen 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. Om sekretess hindrar underrättelse i ett år behöver någon underrättelse inte lämnas (17 §).

För övrig brottslig verksamhet för vilken inhämtning kan ske enligt preventivlagen, föreskrivs ingen underrättelseskyldighet.

Underrättelseskyldigheten ska fullgöras av åklagare. Om sekretess hindrar underrättelse ska i stället SIN underrättas (förordningen [2007:1144] om fullgörande av underrättelseskyldighet enligt lagen [2007:979] om åtgärder för att förhindra vissa särskilt allvarliga brott).

Den som varit utsatt för övervakning enligt preventivlagen avseende vissa brott som huvudsakligen utreds av Polismyndigheten ska alltid underrättas om tvångsmedelsanvändningen. Underrättelseskyldigheten gäller dock inte

för de brott som huvudsakligen utreds av Säkerhetspolisen. Reglerna kring detta är utformade på motsvarande sätt som för underrättelse vid hemlig övervakning av elektronisk kommunikation enligt rättegångsbalken. De skäl som redovisas ovan till stöd för regeringens uppfattning att underrättelsereglerna i rättegångsbalken är förenliga med EU-rätten har giltighet även vid bedömningen av underrättelseskyldigheten enligt preventivlagen. Regeringen anser därför, i likhet med utredningen, att underrättelseskyldigheten enligt preventivlagen är förenlig med EU-rätten.

Lagen om särskild utlänningskontroll

I lagen om särskild utlänningskontroll föreskrivs ingen skyldighet att underrätta enskild som har utsatts för hemliga tvångsmedel. Tvångsmedelsanvändning enligt lagen kan endast avse en utlänning som enligt ett redan fattat beslut ska utvisas av hänsyn till rikets säkerhet eller för att det kan befaras att utlänningen kommer att begå eller medverka till terroristbrott enligt 2 § lagen om straff för terroristbrott. Domstol får i sådant fall lämna tillstånd att använda tvångsmedel för att ta reda på om utlänningen eller en organisation eller grupp som han eller hon tillhör eller verkar för, planlägger eller förbereder 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. Regeringen gör därför, i likhet med utredningen, 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 (jfr skr. 2017/18:57 s. 4).

6.7 Uppgifter för operatörernas egna ändamål

Regeringens bedömning: De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation bör även fortsättningsvis 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.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Åklagarmyndigheten, Säkerhetspolisen, Tullverket, Post- och telestyrelsen, Ecpat Sverige, Rädda barnen, Rättighetsalliansen, Dataspelsbranschen, Sveriges Biografägareförbund, Musikförläggarna Sveriges filmuthyrareförening, Film- och TV-branschens samarbetskommitté* och *Sveriges Videodistributörers förening* är positiva till att tillgången även

fortsättningsvis ska omfatta sådana uppgifter som operatörerna lagrar för egna ändamål.

Rättighetsalliansen, Dataspelsbranschen, Sveriges Biografägareförbund, Musikförläggarna Sveriges filmuthyrareförening, Film- och TV-branschens samarbetskommitté och *Sveriges Videodistributörers förening* anser att det bör införas ett juridiskt ansvar för operatörernas påstående huruvida informationen finns eller inte.

Telia Sverige AB anser att tillgången till uppgifter endast bör avse de uppgifter som sparas enligt datalagringsreglerna. Polisens möjlighet att få del av uppgifter bör inte vara beroende av hur mycket eller hur länge en operatör lagrar data för egna behov. Tillgång bör dessutom, enligt bolaget, bara ges till uppgifter som är strikt nödvändiga och proportionerliga, varför det inte är rimligt att reglerna om tillgång medger polisen en vidare tillgång än vad som följer av datalagringsbestämmelserna.

Post- och telestyrelsen anser att det vore mer ändamålsenligt om ersättningen vid utlämnande av uppgifter som operatörerna själva lagrat för egna ändamål också skulle fastställas av föreskrifter meddelade av myndigheten. *Ecpat Sverige* anför att operatörernas prissättning för att lämna ut uppgifter som inte omfattas av lagringsskyldigheten är otillfredsställande och anser att detta bör ses över.

Skälen för regeringens bedömning: 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 uppgifter som enligt direktivet får sparas för operatörernas egna ändamål ska uppgifter även lagras 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 §§ lagen om elektronisk kommunikation. Av dessa bestämmelser kan utläsas att de trafikuppgifter som lagras för brottsbekämpande ändamål endast får behandlas vid tillämpning av reglerna om hemliga tvångsmedel. Det innebär att om Polismyndigheten efterforskar en försvunnen person (utan misstanke om brott) eller Skatteverket behöver uppgifter i ett ärende om kontroll av skatt får myndigheten inte tillgång till de uppgifter som är lagrade för brottsbekämpande ändamål, men däremot till de uppgifter som finns lagrade för operatörens eget behov (6 kap. 22 § jämförd med 16 a och 16 c §§).

Det står alltså klart att det endast är de brottsbekämpande myndigheterna som har rätt att få tillgång till de uppgifter som är föremål för lagring enligt datalagringsreglerna och att tillgång ges endast för brottsbekämpande ändamål. Vid det omvända förhållandet – dvs. att de brottsbekämpande myndigheterna vill få åtkomst till uppgifter som lagras av operatörerna för eget behov – finns inga begränsningar i lagen om elektronisk kommunikation. 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.

Regeringen anser, till skillnad från *Telia Sverige AB*, att det inte finns skäl att ändra regleringen gällande tillgången till uppgifter som operatörerna sparar för egna ändamål. En motsatt ordning skulle vara ett främmande inslag i det straffprocessuella regelsystemet. För att illustrera det kan en jämförelse med beslag göras. Om en bokföringsskyldig t.ex. har bevarat mer material än vad som behövs enligt bokföringsreglerna finns det givetvis inget som hindrar polisen från att ta detta i beslag om övriga förutsättningar för det är uppfyllda. Ett förbud mot tillgång till annat än uppgifter som lagras enligt datalagringsreglerna, synes inte heller ge någon större integritetsvinst eftersom uppgifterna ändå lagras av operatören. Bedömningen att tillgången till uppgifter även fortsatt ska avse de uppgifter som operatörerna sparar för egna ändamål stöds också av flertalet remissinstanser, bl.a. *Åklagarmyndigheten, Säkerhetspolisen, Tullverket, Post- och telestyrelsen, Rädda barnen, Rättighetsalliansen* och *Musikförläggarna.*

Flera organisationer inom film-, tv- och musikbranschen, t.ex. *Rättighetsalliansen, Film- och TV-branschens samarbetskommitté* och *Sveriges Videodistributörers förening,* anser att det bör införas ett juridiskt ansvar för operatörernas påstående om huruvida informationen finns eller inte. Regeringen anser att det inom ramen för detta lagstiftningsprojekt inte finns skäl att överväga en sådan regel, utan förutsätter att operatörerna följer det regelverk som finns. Om motsatsen skulle framkomma kan det dock finnas anledning att återkomma i frågan.

Den som är skyldig att lagra uppgifter enligt 6 kap. 16 a § lagen om elektronisk kommunikation har rätt till ersättning för kostnader som uppstår när lagrade uppgifter lämnas ut (6 kap. 16 e §). Det är Post- och telestyrelsen som bestämmer ersättningens storlek när det gäller sådana uppgifter som omfattas av lagringsskyldigheten. När det gäller utlämning av uppgifter som lagras för operatörernas egna ändamål finns inte någon motsvarande reglering av vilken ersättning som ska utgå. Ersättningsnivåerna bestäms efter förhandlingar mellan de brottsbekämpande myndigheterna och berörda operatörer. Såsom utredningen konstaterar innebär detta att ersättningsnivåerna kan variera mellan olika operatörer. Utredningens uppfattning är att denna ordning inte är helt tillfredsställande och därför bör ändras. Utredningen lämnar dock inget sådant förslag. Utredningens uppfattning delas av *Post- och telestyrelsen* och *Ecpat Sverige.* Post- och telestyrelsen anser att det vore mer ändamålsenligt att reglera prissättningen på samma sätt som i dag gäller för utlämnande av uppgifter som omfattas av lagringsskyldigheten och att myndigheten bör ges mandat att fastställa även denna ersättning. Regeringen konstaterar att en ändring av denna reglering skulle kräva vissa lagändringar och att det inte finns något beredningsunderlag för att genomföra en sådan ändring i detta lagstiftningsärende. Det kan dock finnas anledning för regeringen att återkomma i frågan.

6.8 Säkerhetspolisens inhämtning i underrättelseverksamhet för viss samhällsfarlig brottslighet

Regeringens förslag: Inhämtningslagens tidsbegränsade bestämmelse om inhämtning av uppgifter om elektronisk kommunikation för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar vissa brott med lägre minimistraff än fängelse i två år ska göras permanent.

Möjligheten att hämta in uppgifter ska utvidgas till att gälla även vid misstanke om

- statsstyrt företagsspioneri
- grov misshandel och olaga frihetsberövande som begås i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller i avsikt att hämnas en åtgärd.

Datalagringsutredningens förslag överensstämmer med regeringens.

Remissinstanserna: Endast ett fåtal remissinstanser yttrar sig särskilt i denna del. *Åklagarmyndigheten, Försvarsmakten, Juridiska institutionen på Handelshögskolan vid Göteborgs universitet* och *Stockholms universitet (Juridiska fakulteten)* tillstyrker eller har ingen invändning mot förslaget. *Malmö tingsrätt* ifrågasätter om det finns ett reellt behov av att utvidga möjligheten att hämta in uppgifter om brottslig verksamhet enligt 3 § inhämtningslagen till att även omfatta statsstyrt företagsspioneri samt grov misshandel och olaga frihetsberövande som begås i vissa syften. Förslaget kan enligt tingsrätten även leda till tillämpningsproblem. *Svenska Tidningsutgivareföreningen (TU)* och *Journalistförbundet* anför att hoten mot massmedier ökar, men att de inte kan tillstyrka åtgärder som riskerar att negativt påverka meddelares anonymitet. De anser att det finns en risk att anonyma källor röjs i samband med kartläggning av misstänkt brottslig verksamhet mot en journalist eller redaktion.

Polismyndigheten och *Tullverket* vill att det införs en straffvärdesventil för att bättre kunna bekämpa bl.a. grov organiserad brottslighet. *Ekobrottsmyndigheten* vill av samma skäl att även t.ex. grovt bokföringsbrott och grovt skattebrott ska omfattas av lagen. Enligt *Försäkringskassan* bör även grovt bidragsbrott omfattas.

Skälen för regeringens förslag

Säkerhetspolisens möjlighet att hämta in uppgifter om elektronisk kommunikation är tidsbegränsad

Säkerhetspolisens uppdrag är främst inriktat på att förhindra brott, och i mindre utsträckning på att utreda brott som redan har begåtts. Flera av de brott som Säkerhetspolisen bekämpar har lägre minimistraff än fängelse i två år och inhämtningslagens huvudregel kan då inte tillämpas. Det innebär att brott som exempelvis sabotage, spioneri, s.k. terrorismfinansiering (grovt

brott) och s.k. terrorismrekrytering (grovt brott) faller utanför huvudregelns tillämpningsområde. För att kunna upptäcka och förhindra även sådana brott får, enligt en särskild bestämmelse i 3 § inhämtningslagen, uppgifter om elektronisk kommunikation hämtas in vid brottslig verksamhet som innefattar vissa särskilt angivna brott med ett lägre straffminimum än fängelse i två år.

När bestämmelsen trädde i kraft gavs den begränsad giltighetstid till utgången av 2013. Skälet som regeringen angav för den begränsade giltighetstiden var att både lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott var tidsbegränsade till utgången av 2013 och föremål för utvärdering. Därför borde bestämmelsen i inhämtningslagen tills vidare ges samma giltighetstid som dem. Det angavs också att frågan om Säkerhetspolisens fortsatta tillgång till uppgifter om elektronisk kommunikation för tiden efter utgången av 2013 borde övervägas i det sammanhang då man överväger en framtida reglering av hemliga tvångsmedel för särskilt allvarlig eller samhällsfarlig brottslighet (prop. 2011/12:55 s. 87).

Sådana överväganden har gjorts, och resulterade i att bestämmelserna i de tidsbegränsade lagarna om hemliga tvångsmedel permanentades (prop. 2013/14:237). Under det pågående lagstiftningsarbetet förlängdes giltighetstiden för 3 § inhämtningslagen till utgången av 2014 (prop. 2012/13:180, bet. 2013/14:JuU7, rskr. 2013/14:38). När lagstiftningsärendet sedan slutfördes förlängdes giltighetstiden – trots förslag om att permanenta bestämmelsen – ytterligare en gång, till utgången av 2016. Som skäl för förlängningen angav regeringen att den hittillsvarande tillämpningen av inhämtningslagen borde kartläggas och analyseras ytterligare innan slutlig ställning togs till hur Säkerhetspolisens behov av uppgifter om elektronisk kommunikation i underrättelseverksamhet borde tillgodoses (prop. 2013/14:237 s. 116).

En sådan utvärdering av inhämtningslagen har gjorts av Datalagringsutredningen. Utredningen förslår att bestämmelsen i 3 § inhämtningslagen ska gälla permanent. Innan slutlig ställning tas till en permanentning av 3 § har regeringen velat avvakta utgången av processen i EU-domstolen om den svenska datalagringsregleringen. För att inte bestämmelsen ska upphöra att gälla har giltighetstiden därför förlängts ytterligare två gånger, först till utgången av 2017 och sedan till utgången av 2019 (prop. 2015/16:177, bet. 2015/16:JuU35, rskr. 2015/16:320 och prop. 2016/17:186, bet. 2016/17:JuU28, rskr. 2016/17:343).

Säkerhetspolisens möjlighet att hämta in uppgifter om elektronisk kommunikation bör gälla permanent

Bestämmelsen i 3 § inhämtningslagen upphör alltså att gälla vid årsskiftet 2019/2020. Förslaget om att bestämmelsen ska gälla permanent tar avstamp i en ingående kartläggning av den hittillsvarande tillämpningen av lagen.

Utredningen har tittat på dels vilket behov som finns av tvångsmedelsanvändning enligt lagen, dels vilken nytta den har inneburit för den brottsbekämpande verksamheten. Även frågan om vilken inverkan lagen har haft på enskildas personliga integritet har utvärderats. Av kartläggningen framgår att tillämpningen av lagen har lett till beaktansvärd nytta i samband med underrättelsearbete avseende brottslig verksamhet som innefattar flera av de brott som för närvarande omfattas av den tidsbegränsade bestämmelsen. Flera av brotten anses dessutom regelmässigt vara svåra att kartlägga. Behovet av att använda olika hemliga tvångsmedel har därför ansetts vara särskilt stort (se t.ex. prop. 2013/14:237 s. 81). Enligt utredningen leder lagen dock även till integritetsintrång, både för personer som ärendena avser och de personer som dessa har kontakt med. Genom inhämtning av uppgifter om elektronisk kommunikation kan t.ex. uppgifterna användas för att kartlägga personernas kontakter och rörelsemönster.

De brott som omfattas av den tidsbegränsade bestämmelsen riktar sig på olika sätt mot samhällsstrukturen och Sveriges säkerhet. Sådana brott är särskilt angelägna att upptäcka och förhindra. Det finns ingenting som tyder på att Säkerhetspolisens behov av en särskild inhämtningsmöjlighet skulle minska inom överskådlig tid. Tvärtom talar den senaste utvecklingen i omvärlden, men även i Sverige, för att det behövs effektiva och ändamålsenliga verktyg för att förebygga, förhindra och upptäcka brottslighet som direkt eller indirekt hotar vitala samhällsintressen. En försämring i det avseendet skulle kunna medföra allvarliga risker för Sveriges säkerhet. Det har inte heller i övrigt kommit fram något som ger skäl att anta att de sakförhållanden som ligger till grund för regeringens bedömning är av tillfällig natur. Enligt regeringen väger samhällets och medborgarnas intresse av att den aktuella brottsligheten upptäcks och förhindras tyngre än integritetsintresset för dem som kan komma att bli föremål för tvångsmedlet. Möjligheten att hämta in uppgifter om elektronisk kommunikation om brott med lägre minimistraff än två års fängelse bör alltså finnas kvar och bör inte längre vara tidsbegränsad. Remissinstanserna motsätter sig inte heller detta. Bestämmelsen bör alltså göras permanent. Liksom utredningen föreslår, och som ingen remissinstans invänder mot, bör bestämmelsen även i fortsättningen gälla de brott som den omfattar i dagsläget. Av lagtekniska skäl bör dock nuvarande föreskrifter i 3 § arbetas in i 2 § inhämtningslagen.

Bör bestämmelsen omfatta fler brott?

Datalagringsutredningen föreslår att den brottskatalog som finns i 3 § inhämtningslagen ska utvidgas till att omfatta vissa ytterligare brott. Det handlar dels om s.k. statsstyrt företagsspioneri, dels om grov misshandel och olaga frihetsberövande som begås i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller i avsikt att hämnas en åtgärd.

Vid utvidgning av området för ett hemligt tvångsmedel måste behovet och nyttan av att använda tvångsmedlet alltid vägas mot det integritetsintrång som åtgärden kan innebära. Vid en sådan avvägning får brottets allvar en stor

betydelse. Detta kan mätas främst genom brottets straffskala eller förväntade straffvärde. I tidigare lagstiftningsärenden har dock även styrkan i det skyddsintresse som motiverar kriminaliseringen beaktats. Vissa brott har då, utan att detta direkt avspeglats i straffskalan, betecknats som särskilt allvarliga eftersom de har ansetts som samhällsfarliga (prop. 2007/08:163 s. 29–30 och prop. 2013/14:237 s. 78).

Statsstyrt företagsspionerі innebär att främmande makt bedriver spionage mot svenska företag med avsikt att få tillgång till företagshemligheter. Till skillnad från traditionellt spionage, som syftar till att underminera ett lands säkerhet, är företagsspioneriets motiv främst att skaffa ekonomisk vinning och inhämta teknisk kunskap. Sådant spionerі kan få allvarliga konsekvenser för svenska företag och i förlängningen kan viktiga svenska samhällsintressen som är avgörande för vårt välstånd drabbas. Brottsligheten kan även försämra förutsättningarna att utveckla och upprätthålla skyddet för landets säkerhet. Civil forskning har fått allt större betydelse för att driva teknikutvecklingen och även för att ta fram teknik som kan användas i militära syften. Exempel på detta är bioteknisk forskning som kan användas för att utveckla och tillverka biologiska och kemiska massförstörelsevapen. Eftersom resultaten av sådan forskning kan missbrukas är det av stor vikt att den skyddas. Även här står alltså stora samhällsvärden på spel. Vidare är de personer som deltar i spioneriverksamhet ofta välutbildade underrättelse-officerare som tränats och dessutom understöds av främmande makt. Dessa personer är i allmänhet mycket säkerhetsmedvetna vilket gör brottsligheten svår att upptäcka och förhindra.

Bland annat av dessa skäl har regeringen gjort bedömningen att statsstyrt företagsspionerі är så allvarligt att hemlig rumsavlyssning – som ur ett integritetsperspektiv typiskt sett anses som det mest ingripande tvångsmedlet – bör tillåtas för att bekämpa brottet, låt vara att det är begränsat till brott som inte kan antas leda till endast böter (27 kap. 20 d § 3 RB, prop. 2013/14:237 s. 89–90). Av samma skäl har brottet även lagts till i brottskatalogen i preventivlagen (1 § första stycket 5, prop. 2013/14:237 s. 114–115). Redan i skedet innan en förundersökning har inletts är det alltså möjligt att använda de betydligt mer integritetskänsliga tvångsmedlen hemlig avlyssning av elektronisk kommunikation och hemlig kameraövervakning. Det kan ur ett systematiskt perspektiv anses rimligt och logiskt att statsstyrt företags-spionerі även omfattas av den särskilda inhämtningsmöjligheten enligt inhämtningslagen.

En fråga som emellertid kan ställas är om Säkerhetspolisens behov av uppgifter om elektronisk kommunikation i underrättelseverksamheten i tillräcklig utsträckning tillgodoses genom möjligheten till hemlig övervakning av elektronisk kommunikation enligt preventivlagen. Som utredningen konstaterar skiljer sig emellertid rekvisiten för att få tillgång till information väsentligt mellan de två lagarna. En viktig skillnad är att det i inhämtningslagen inte finns något krav på att inhämtningen ska kunna kopplas till en viss person. Enligt utredningen är informationsinhämtning utan ett krav på koppling till en viss person särskilt ägnad att tillgodose vissa behov hos Säkerhetspolisen, t.ex. att identifiera det okända hotet genom att

identifiera okända aktörer och bedöma vilket hot de utgör. Preventivlagen är inte heller något allmänt underrättelseverktyg, utan när den lagen tillämpas är det uteslutande i situationer där det handlar om att förhindra att en på visst sätt konkretiserad risk förverkligas. Utredningen bedömer mot den bakgrunden att behovet av en möjlighet att hämta in uppgifter enligt inhämtningslagen inte påverkas i någon större utsträckning av att preventivlagen innehåller en möjlighet att använda hemlig övervakning av elektronisk kommunikation beträffande det aktuella brottet. Regeringen har ingen annan uppfattning. Inte heller remissinstanserna framför några synpunkter i den delen.

Sammanfattningsvis anser regeringen, till skillnad från *Malmö tingsrätt*, att det står klart att det finns ett reellt behov av att kunna inhämta uppgifter enligt inhämtningslagen beträffande brottslig verksamhet som innefattar statsstyrt företagsspionerі. Behovet och den förväntade nyttan av att använda tvångsmedlet kan antas överväga de integritetsintrång som tvångsmedlet kan innebära. Regeringen föreslår därför att den utökade möjligheten att använda tvångsmedel enligt inhämtningslagen även ska omfatta statsstyrt företagsspionerі.

När det sedan gäller grov misshandel och olaga frihetsberövande som begås i s.k. systemhotande syfte framgår av Säkerhetspolisens uppgifter till utredningen att ett relativt stort antal brott begås mot förtroendevalda, myndighetspersoner och journalister. Sådan brottslighet syftar till att påverka den allmänna åsiktsbildningen, inkräkta på handlingsfriheten inom viss politisk organisation eller till att påverka eller hämnas framtida eller genomförda myndighetsbeslut. Det saknas enligt regeringen anledning att ifrågasätta att Säkerhetspolisen har ett stort behov av att kunna kartlägga grupperingar som har avsikt och förmåga att begå sådan brottslighet. Brottsligheten är också mycket allvarlig eftersom den syftar till att påverka de aktuella personerna i utövandet av deras uppdrag. På så sätt utgör brottsligheten ett hot mot demokratin.

Även dessa brott omfattas av brottskatalogen i preventivlagen. I likhet med vad som gäller för statsstyrt företagsspionerі finns det även avseende dessa brott vissa systematiska skäl för att de ska läggas till i brottskatalogen i inhämtningslagen. Vad som anförs ovan om möjligheten att enligt preventivlagen använda tvångsmedel som från integritetsperspektiv typiskt sett är mer ingripande än inhämtning av uppgifter om elektronisk kommunikation enligt inhämtningslagen har alltså relevans även här. Detsamma gäller vad som anförs om behovet av en möjlighet att hämta in uppgifter enligt inhämtningslagen även om preventivlagen innehåller en möjlighet att använda hemlig övervakning av elektronisk kommunikation beträffande samma brott.

Malmö tingsrätt påpekar att ändringen kan komma att innebära avsevärda tillämpningssvårigheter eftersom gränsdragningen mellan misshandel av normalgraden och grov misshandel inte torde vara möjlig att göra på underrättelsestadiet. Regeringen delar dock inte den farhågan. Situationen är nämligen inte unik för grov misshandel. Redan i dag omfattar brottskatalogen i 3 § inhämtningslagen i flera fall grovt brott, och där det kan uppkomma

frågor om gränsdragning i förhållande till brott av normalgraden. Utredningens kartläggning ger inte anledning att anta att detta har varit ett problem hittills. Säkerhets- och integritetsskyddsnämnden, som utövar tillsyn över tvångsmedelsanvändning enligt lagen, har inte heller lyft frågan i sitt remissvar. En osäkerhet om brottet i fråga är grovt ska givetvis resultera i att något beslut om tvångsmedel inte fattas.

Svenska Tidningsutgivareföreningen (TU) och *Journalistförbundet* påpekar att det kan finnas en risk att anonyma källor röjs i samband med kartläggning av misstänkt brottslig verksamhet mot en journalist eller redaktion och avstyrker därför förslaget. Regeringen anser emellertid att denna farhåga inte bör överdrivas. Såsom regeringen redogör närmare för i avsnitt 5.4 tar anonymitetsskyddet sikte på situationer där kommunikationen innebär att ett meddelande eller liknande lämnas för publicering. För det fall myndigheten undantagsvis i förväg skulle känna till att kommunikationen i ett visst fall omfattas av anonymitetsskyddet gäller proportionalitetsprincipen som innebär att inhämtning inte får ske om det skulle innebära ett kringgående av tystnadsplikten eller efterforskningsförbudet. Som framgår ovan är inhämtning av uppgifter om elektronisk kommunikation för denna typ av brottslighet redan möjlig enligt preventivlagen. Det har inte framkommit att det vid tillämpningen av den lagen uppstått problem vad gäller anonymitetsskyddet.

Sammanfattningsvis väger alltså intresset av att även kunna förebygga, förhindra och upptäcka nu aktuell brottslighet tungt. Regeringen anser att behovet, och den förväntade nyttan, av tvångsmedlet i detta fall väger tyngre än integritetsintresset hos dem som kan bli föremål för tvångsmedelsanvändningen. De aktuella brotten hör utan tvekan till kategorin grova brott, som enligt Tele2-domen är de enda som kan berättiga att myndigheterna får tillgång till uppgifterna, se avsnitt 6.3. Regeringen föreslår därför att brottskatalogen utvidgas till att även omfatta grov misshandel och olaga frihetsberövande som begås i systemhotande syfte. Olaga frihetsberövande som är mindre grovt ska dock inte omfattas.

Några remissinstanser, bl.a. *Ekobrottsmyndigheten, Polismyndigheten* och *Tullverket*, anser att inhämtningslagens tillämpningsområde är för begränsat och att delar av den grova organiserade brottsligheten faller utanför. De föreslår att en straffvärdesventil införs för att även t.ex. grov stöld, grovt häleri, grovt bokföringsbrott och narkotikasmuggling av normalgraden ska omfattas. Förslaget tar alltså inte sikte på den utökade möjligheten till tvångsmedelsanvändning för vissa samhällsfarliga brott inom Säkerhetspolisens ansvarsområde, utan på en möjlighet att utvidga lagens tillämpningsområde för att bekämpa grov organiserad brottslighet. Från ett brottsbekämpningsperspektiv går det givetvis att ha förståelse för dessa synpunkter. En möjlighet att hämta in uppgifter enligt inhämtningslagen skulle säkert kunna vara till nytta i myndigheternas verksamhet. Frågor om hur intresset av en effektiv brottsbekämpning bör balanseras mot integritetsintresset kräver emellertid noggranna överväganden. Det finns inte något beredningsunderlag för förslaget. Frågan får därför analyseras i ett annat sammanhang.

7 Uppgifter om abonnemang

Regeringens bedömning: Tele2-domen rör framför allt trafikuppgifter och lokaliseringsuppgifter och inte specifikt uppgifter om abonnemang. Regleringen gällande uppgifter om abonnemang är förenlig med EU-rätten.

Det finns inte skäl att i författning definiera uttrycket uppgift om abonnemang.

Utredningens bedömning överensstämmer i sak med regeringens.

Remissinstanserna: *Åklagarmyndigheten, Säkerhetspolisen, Ekobrottsmyndigheten, Polismyndigheten, Tullverket, Ecpat Sverige, Rättighetsalliansen, Dataspelsbranschen, Sveriges Biografägareförbund, Musikförläggarna, Sveriges filmuthyrareförening, Film- och TV-branschens samarbetskommitté* och *Sveriges Videodistributörers förening* instämmer i utredningens bedömning att abonnemangsuppgifter, inklusive ip-adresser, inte omfattas av Tele2-domen. *Åklagarmyndigheten* poängterar att en motsatt tolkning skulle innebära att flera brott, som inte är grova men där tillgången till abonnemangsuppgifter är en förutsättning för en framgångsrik brottsbekämpning, i praktiken skulle bli omöjliga att utreda och lagföra och därmed bli straffria. En sådan ordning skulle strida mot Europakonventionen. *Ecpat Sverige* understryker vikten av abonnemangsuppgifter för att kunna utreda och lagföra sexualbrott mot barn. Utan tillgång till abonnemangsuppgifter skulle flera sexualbrott mot barn som inte rubriceras som grova brott, som t.ex. köp av sexuell handling av barn eller kontakt för att träffa ett barn i sexuellt syfte, bli långt mer svårutredda. *Säkerhets- och integritetsskyddsnämnden* ifrågasätter inte utredningens bedömning, men anser att det bör bringas klarhet ifråga om vilka uppgifter som utgör abonnemangsuppgifter och att begreppet bör definieras i författningstext. *Stiftelsen för internetinfrastruktur (Internetstiftelsen)* påpekar att det finns en risk för överutnyttjande av inhämtning av abonnemangsuppgifter om det inte finns en tydlig definition av begreppet i svensk lag.

Svea hovrätt, Hovrätten för övre Norrland, Datainspektionen, Post- och telestyrelsen och *Com Hem AB* anser att det behövs en närmare analys av frågan. *Datainspektionen* och *Com Hem AB* delar inte utredningens slutsats att abonnemangsuppgifter inte är lika integritetskänsliga som trafik- och lokaliseringsuppgifter och anför att definitionen av abonnemangsuppgifter kommer från en tid långt före den tekniska utvecklingen och innebär att de uppgifter som idag sorteras under abonnemangsuppgifter är betydligt fler och mer integritetskänsliga än när begreppet infördes.

Bahnhof AB, Tele2 Sverige AB, Com Hem AB och *Civil Rights Defenders* anser att ip-adresser omfattas av Tele2-domen. Någon uppdelning mellan abonnemangsuppgifter och trafik- och lokaliseringsuppgifter görs inte i direktiv 2002/58. Det viktiga är i stället om uppgiften kan klassificeras som en konfidentiell personuppgift som i så fall skyddas av direktivet och därmed av EU-domstolens krav. Tele2-domen måste läsas i ljuset av Digital Rights-

domen och bestämmelserna i det upphävda datalagringsdirektivet som omfattade ip-adresser. Därför måste också Tele2-domen anses omfatta ip-adresser. Kammarrättens dom omfattar dessutom samtliga datalagringsbestämmelser, inklusive ip-adresser. Ip-adresser är långt mer integritetskänsliga än uppgifter om t.ex. vem som står bakom ett mobiltelefonnummer.

Post- och Telestyrelsen, Netnod Internet Exchange i Sverige AB och *RISE SICS AB* påpekar att användningen av dynamiska ip-adresser och NAT-teknik 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. Detta innebär att de uppgifter man måste behandla sammantaget kan lämna mycket exakt information om abonnenternas internetkommunikation och därmed vara mer integritetskänslig.

Skälen för regeringens bedömning

Vad innefattas i uttrycket uppgift om abonnemang?

Med uppgift om abonnemang i 6 kap. 20 § lagen om elektronisk kommunikation avses t.ex. uppgifter om abonnentens nummer, namn, titel och adress (prop. 1992/93:200 s. 310). Vidare har det ansetts innefatta såväl fasta som dynamiska ip-adresser och IMSI-nummer (ett nummer som är kopplat till abonnentens simkort och därmed telefonnummer) (se t.ex. prop. 2011/12:55 s. 101 och Kammarrätten i Stockholms dom den 19 januari 2010 i RK 2010:1). I de bakomliggande EU-direktiven till lagen om elektronisk kommunikation anges inte uppgifter om abonnemang som en särskild kategori uppgifter. I motsats till vad som gäller i fråga om trafik- och lokaliseringsuppgifter ger EU-rätten därför inte någon direkt ledning för hur uppgift om abonnemang ska definieras, se vidare nedan.

I likhet med utredningen anser regeringen att det kan ifrågasättas om det är lämpligt eller ens möjligt att definiera uppgifter om abonnemang endast utifrån vilken uppgift det är fråga om. I stället är det mer relevant att som utgångspunkt definiera uppgifter om abonnemang 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. Med en sådan definition utgör t.ex. uppgift om vilken abonnent som är kopplad till ett visst IMSI-nummer en uppgift om abonnemang, medan information om vilka andra nummer eller adresser som ett visst IMSI-nummer har kommunicerat med inte gör det.

Ett annat exempel är ip-adresser. En ip-adress är en adress som en dator eller ett lokalt nätverk tilldelas för att datapaket (en datamängd som behandlas som en enhet när data skickas från sändare till mottagare över datornät) ska kunna skickas och tas emot över internet genom den tekniska kommunikationsstandarden Internet Protocol. Ip-adressen kan därför, något förenklat, liknas vid en postadress 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 till något särskilt 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). Det förtjänar också att påpekas att uppgifter som går utöver vad som kan anses som identitetsuppgifter, t.ex. vilka andra ip-adresser som innehavaren har kommunicerat med, vilka webbplatser som en viss ip-adress har besökt och liknande uppgifter inte omfattas (prop. 2011/12:55 s. 102). Att ip-adresser, oavsett om de är fasta eller dynamiska, är att anse som uppgift om abonnemang har också bekräftats av Kammarrätten i Stockholm i en dom den 14 december 2018 (mål nr 2471-18), se vidare nedan.

Den beskrivna definitionen av uppgifter om abonnemang kan också sägas vara i linje 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). Vid denna tid användes emellertid annan teknik och enskildas kommunikationsmönster var annorlunda. Kammarrätten i Stockholm har dock i domen RK 2010:1, i överensstämmelse med den angivna definitionen, uttalat att uppgifter som syftar till att identifiera ett abonnemang eller en abonnent i princip avser uppgifter om abonnemang.

Enligt *Säkerhets- och integritetsskyddsnämnden* och *Stiftelsen för internetinfrastruktur (Internetstiftelsen)* bör begreppet abonnemangsuppgifter definieras i författningstext. Av beskrivningen ovan framgår vad som enligt förarbeten och praxis anses utgöra en uppgift om abonnemang. Det saknas beredningsunderlag för att författningsreglera vad som faller under begreppet. Mot denna bakgrund ser regeringen ingen möjlighet och inte heller något omedelbart behov av en författningsreglering.

Regleringen om de brottsbekämpande myndigheternas tillgång till uppgifter om abonnemang

En operatör som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har tystnadsplikt för bl.a. uppgifter om abonnemang (6 kap. 20 § första stycket 1 lagen om elektronisk kommunikation). Uppgifter om abonnemang 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 §). 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, såsom t.ex. ip-adresser.

Uppgifter om abonnemang är typiskt sett mindre integritetskänsliga än t.ex. trafik- och lokaliseringsuppgifter. Uppgifter om abonnemang i sig går enbart i mer begränsad utsträckning att använda för det slags ingående kartläggning av enskilda personer som EU-domstolen anser utgör en mycket ingripande begränsning av enskildas rättigheter enligt stadgan.

Enligt nuvarande regelverk har tillgången till uppgifter om abonnemang inte bedömts utgöra ett hemligt tvångsmedel och regleras direkt i lagen om elektronisk kommunikation. Operatörerna är skyldiga att på begäran lämna ut uppgifter om abonnemang till de brottsbekämpande myndigheterna om det finns misstanke om brott (6 kap. 22 § första stycket 2 lagen om elektronisk kommunikation). Det krävs inte att brottet är av visst allvar. När tillgångsbestämmelserna i 6 kap. 22 § första stycket 2 lagen om elektronisk kommunikation 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 ett allt vanligare fenomen. Vid bedömningen av integritetsintrånget när abonnemangsinformation om ip-adresser lämnas ut beaktades att privatpersoner ofta använder dynamiska ip-adresser. Det gjordes en avvägning mellan det integritetsintrång som ett utlämnande av uppgifter om abonnemang 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) Användandet av internet och telekommunikation har därefter fortsatt att växa och det finns ingenting som talar för att användningen av it-verktyg och elektronisk kommunikation vid brottslighet avtar eller att behovet av uppgifter om abonnemang för brottsbekämpningen minskar. Avvägningarna framstår därmed fortfarande som giltiga.

Eftersom tillgång till abonnemangsuppgifter inte utgör en hemlig övervakningsåtgärd och ingreppet i privatlivet är begränsat i jämförelse med tillgång till trafik- och lokaliseringsuppgifter, finns det inte något krav på förhandskontroll av domstol eller annan oberoende myndighet, eller på underrättelse till de berörda. Vid en jämförelse med t.ex. husrannsakan, som normalt får beslutas av undersökningsledaren, är inhämtning av uppgifter om abonnemang 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 innehavaren av ett visst bankkort eller ännu mer integritetskänslig information, såsom hur bankkortet har använts, 1 kap. 10–12 §§ lagen (2004:297) om bank- och finansieringsrörelse. Enligt denna reglering krävs inte beslut av domstol och bestämmelserna ger undersökningsledare eller åklagare möjlighet att besluta att kreditinstitutet, dess styrelseledamöter eller anställda inte får röja för kunden eller för någon utomstående att uppgifter har lämnats eller att det pågår en förundersökning.

Några remissinstanser, t.ex. *Post- och Telestyrelsen, Netnod Internet Exchange i Sverige AB* och *RISE SICS AB*, påpekar 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. Remissinstanserna anser därför att de uppgifter man måste behandla sammantaget kan lämna mycket exakt information om abonnenternas internetkommunikation och därmed vara mer integritetskänslig. Enligt regeringens mening torde det ur integritetssynpunkt dock inte vara någon större skillnad mellan att kartlägga någon via en fast ip-adress, via en dynamisk ip-adress eller via en ip-adress där trafiken styrs av NAT-teknik. Inte i något fall lagras vilka webbplatser som användaren har besökt eller annan motsvarande information. Det finns inte heller någon 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.

Den svenska regleringen om abonnemangsuppgifter är förenlig med EU-rätten

Med anledning av EU-domstolens dom i Tele2-målet har frågan väckts om uppgifter om abonnemang, och i synnerhet ip-adresser, omfattas av domen eller inte. Bedömningen av denna fråga får bl.a. betydelse för vilka regler som ska gälla för de brottsbekämpande myndigheternas möjlighet att få tillgång till dessa uppgifter. Om uppgifter om abonnemang (inkluderat ip-adresser) skulle anses omfattas av de uttalanden som görs om trafik- och lokaliseringsuppgifter i Tele2-domen skulle det innebära att domstolens uttalanden om bl.a. föregående kontroll av en domstol eller annan oberoende myndighet för att få tillgång till uppgifterna skulle bli tillämpliga. Även uttalandena om att tillgång endast ska kunna ges de brottsbekämpande myndigheterna vid grova brott skulle behöva beaktas.

Utredningen bedömer att EU-domstolens avgörande i Tele2-domen inte berör uppgifter om abonnemang. Remissinstanserna har olika uppfattningar i frågan där bl.a. *Polismyndigheten, Åklagarmyndigheten, Säkerhetspolisen* och *Säkerhets- och integritetsskyddsnämnden* delar utredningens bedömning, medan flera operatörer och föreningar, såsom *Bahnhof AB, Tele2 Sverige AB* och *Civil Rights Defenders,* är av motsatt uppfattning. En del remissinstanser, t.ex. *Svea hovrätt, Hovrätten för övre Norrland, Datainspektionen* och *Post- och telestyrelsen,* efterlyser en närmare analys av frågan. Den analys som behövs för detta ställningstagande redogörs för nedan. Det bör dock redan nu påpekas att det efter att utredningen lämnat sitt betänkande och remiss-instanserna inkommit med sina remissvar har tillkommit ny rättspraxis som gör att frågeställningarna numera är bättre belysta och i stort får anses klargjorda, vilket regeringen återkommer till nedan.

Direktiv 2002/58 syftar till att harmonisera nationella bestämmelser för att säkerställa ett likvärdigt skydd för de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet (som bl.a. följer av artikel 7 och 8 i EU:s stadga) när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation (artikel 1). Direktivet syftar även till att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom unionen. Direktivet definierar trafikuppgifter och lokaliseringsuppgifter (artikel 2), men inte uppgifter om abonnemang. I det numera upphävda datalagringsdirektivet gjordes emellertid en distinktion mellan trafik- och lokaliseringsuppgifter och de uppgifter som är nödvändiga för att identifiera en abonnent eller en användare (jfr. artikel 1, 2 och 5 i direktiv 2006/24).

Enligt artikel 5 i direktiv 2002/58 ska medlemsstaterna genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. 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 som behandlas och lagras av en leverantör utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra kommunikation.

I Tele2-domen uttalar sig EU-domstolen om hur artikel 15.1 i direktiv 2002/58 ska tolkas i förhållande till artiklarna 7, 8, 11 och 52.1 i EU:s rättighetsstadga. Artikel 15.1 reglerar när undantag får göras från bl.a. bestämmelsen om konfidentialitet i artikel 5 och förstörandeskyldigheten i artikel 6. 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. Som framgår i avsnitt 4.2 kommer EU-domstolen fram till att artikel 15.1 i direktiv 2002/58 jämförd med ovannämnda grundläggande rättigheter enligt EU:s rättighetsstadga utgör hinder för en nationell lagstiftning som inte begränsar behöriga nationella myndigheters tillgång till lagrade uppgifter till åtgärder som syftar till att bekämpa grov brottslighet och inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet.

I förhandsavgörandet uttalar sig domstolen generellt om helheten i det svenska systemet kring lagring och tillgång till uppgifter om elektronisk kommunikation. De uttalanden som domstolen gör tar i första hand sikte på de mer integritetskänsliga trafik- och lokaliseringsuppgifterna. EU-domstolen har inte gjort uttalanden som specifikt handlar om regleringen kring uppgifter om abonnemang. EU-domstolens uttalanden i Tele2-domen ger således t.ex. inte ledning i frågan om vilka krav som ska uppställas vid utlämnande av enbart uppgifter om abonnemang. Det går alltså inte att, med hänvisning till Tele2-domen, dra slutsatsen att de svenska bestämmelserna

om lagring och tillgång till uppgifter om abonnemang står i strid med EU-rätten.

I linje med detta har EU-domstolen i förhandsavgörandet i Ministerio Fiscal (dom den 2 oktober 2018, mål nr C-207/16) slagit fast att tillgång till vissa typer av abonnemangsuppgifter (identitetsuppgifter för innehavare av SIM-kort som aktiverats med en stulen mobiltelefon, såsom för- och efternamn och adress) visserligen utgör ett ingrepp i berörda personers grundläggande rättigheter enligt artikel 7 och 8 EU:s rättighetsstadga, men att ingreppet inte är så allvarligt att tillgången till uppgifterna i samband med brottsbekämpning måste begränsas till kampen mot allvarlig brottslighet (punkt 63). EU-domstolen konstaterar att domstolens tidigare uttalanden i Tele2-domen om att endast kampen mot allvarlig brottslighet kan motivera att myndigheterna får tillgång till lagrade uppgifter, avser sådana uppgifter som sammantagna kan göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter lagrats. Denna tolkning motiveras med att syftet med en lagstiftning måste stå i rimlig proportion till hur allvarligt ingrepp åtgärden innebär. I enlighet med proportionalitetsprincipen kan ett allvarligt ingrepp i samband med brottsbekämpning endast motiveras av syftet att bekämpa brottslighet, som då också måste kvalificeras som allvarlig. När det ingrepp som en tillgång innebär däremot inte är allvarligt, kan det dock motiveras av syftet att förebygga, utreda, upptäcka och lagföra brott i allmänhet (punkterna 54–57). Eftersom det i det aktuella fallet var fråga om uppgifter som inte gjorde det möjligt att dra precisa slutsatser om privatlivet för de personer vars uppgifter berörs, var ingreppet inte så allvarligt att tillgången till dessa uppgifter behövde begränsas till allvarlig brottslighet (punkterna 60–62).

Kammarrätten i Stockholm har därefter tagit ställning i frågan om uppgift om abonnemang i den svenska lagstiftningen (dom den 14 december 2018, mål nr 2471-18). Kammarrätten konstaterar att uppgifter om abonnemang enligt 6 kap. 20 § första stycket 1 lagen om elektronisk kommunikation utgörs av exempelvis uppgifter om namn, adress, abonnentnummer och uppgifter om ip-adress som kan användas för att identifiera en abonnent. Kammarrätten pekar vidare på att det i förarbetena (prop. 2011/12:55 s. 102) har framhållits att uppgifter som går utöver vad som kan anses som identitetsuppgifter – t.ex. vilka andra ip-adresser som innehavaren har kommunicerat med, vilka hemsidor som en viss ip-adress har besökt och liknande uppgifter – inte omfattas. De uppgifter som de brottsbekämpande myndigheterna därmed kan få tillgång till utgör enligt kammarrätten en begränsad kategori uppgifter som inte i sig kan användas för omfattande kartläggning av personers privatliv och som dessutom i många fall finns allmänt tillgängliga. Kammarrätten anser därför att sådana uppgifter kan sägas vara av samma slag som den typ av uppgifter som EU-domstolen hade att bedöma i Ministerio Fiscal. Den behandling av personuppgifter som innebär att de brottsbekämpande myndigheterna ges tillgång till uppgifter om abonnemang kan därför inte anses vara särskilt integritetskänslig. Det ingrepp i rättigheterna enligt artiklarna 7 och 8 i EU:s rättighetsstadga som det är fråga om bedöms därför inte vara av allvarlig art. Lagstiftningen som ger tillgång till uppgifter om

abonnemang behöver därför inte begränsas till att endast gälla situationer då det rör sig om att utreda allvarliga brott och tillgången till uppgifterna behöver inte heller vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet.

Kammarrätten konstaterar avslutningsvis att bestämmelserna om tillgång till abonnemangsuppgifter har funnits under en lång tid och motiverats med att de brottsbekämpande myndigheterna, för att det ska vara möjligt att utreda brott, har ett stort intresse av att få tillgång till uppgifterna. Kammarrätten anser därför att intresset att ge de brottsbekämpande myndigheterna tillgång till uppgifter om abonnemang i brottsbekämpningssyfte väger tyngre än enskildas integritetsintresse. Skyldigheten att lämna ut uppgifter om abonnemang, inklusive ip-adresser, till brottsbekämpande myndigheter bedömdes därför vara förenlig med EU-rätten.

Den bedömning som kammarrätten nu har gjort gällande tillgången till abonnemangsuppgifter ligger också i linje med Sveriges internationella förpliktelser enligt bl.a. artikel 8 i Europakonventionen. Staten har enligt denna artikel ett ansvar för att skydda enskildas privatliv och personliga integritet mot intrång som begås av andra enskilda. En förutsättning för att staten ska kunna leva upp till kravet på att upprätthålla rättstryggheten för enskilda är att det finns en väl fungerande och effektiv brottsbekämpning. Ett rättsfall som är av särskilt intresse i detta sammanhang är Europadomstolens dom K.U. mot Finland (dom den 2 december 2008, mål nr 2872/02). I detta avgörande ansågs Finland kränka rätten till privatliv enligt artikel 8 i och med att det enligt finsk rätt inte var möjligt för brottsbekämpande myndigheter att från en operatör få ut uppgift om vem som använt en viss ip-adress i ett fall då ett barn via internet utsatts för förtal eller möjligen sexuellt ofredande genom att någon lagt ut en påhittad kontaktannons av sexuell natur i barnets namn. Det kan alltså sägas att Europakonventionen inte bara tillåter en rättsordning där de brottsbekämpande myndigheterna i någon form ges tillgång till uppgifter om abonnemang, den påbjuder en sådan ordning. Utrymmet för Sverige att ha ett regelverk som inte tillåter de brottsbekämpande myndigheterna att komma åt sådana uppgifter är således tämligen begränsat.

I linje med de nya avgöranden i frågan som redogörs för ovan är det sammanfattningsvis regeringens bedömning att nuvarande reglering av tillgången till abonnemangsuppgifter är förenlig med EU-rätten och Sveriges internationella åtaganden i övrigt. Det finns således inte skäl att förändra förutsättningarna för de brottsbekämpande myndigheternas tillgång till uppgifter om abonnemang.

I kammarrättens dom konstateras också att behandling av personuppgifter måste vila på en laglig grund, dvs. varje behandling måste uppfylla de förutsättningar som anges i lagstiftningen för att anses tillåten. Eftersom de nuvarande svenska reglerna om lagringsskyldighet i 6 kap. 16 a § lagen om elektronisk kommunikation har funnits oförenliga med EU-rätten konstaterar kammarrätten att uppgifter som lagrats med stöd av den nu underkända lagstiftningen inte behöver lämnas ut till polisen. I och med de justeringar av regleringen som regeringen föreslår i avsnitt 5, bedömer regeringen att

lagringsskyldigheten kommer vara förenlig med EU-rätten. Skyldigheten att lagra uppgifter för brottsbekämpande ändamål kommer, när författningsändringarna träder i kraft, utgöra laglig grund att behandla uppgifterna och alltså vara en tillåten behandling av uppgifterna.

8 Lagring av data inom EU och övriga skydds- och säkerhetsnivåer

8.1 Nuvarande skydds- och säkerhetsnivåer uppfyller EU-rättens krav

Regeringens bedömning: De svenska reglerna om skydds- och säkerhetsnivåer och om utplåning av uppgifter uppfyller de krav som EU-rätten ställer. Även reglerna om tillsyn uppfyller EU-rättens krav.

Utredningens bedömning överensstämmer med regeringens.
Remissinstanserna kommenterar inte bedömningen särskilt.

Skälen för regeringens bedömning

EU-domstolens uttalanden i Tele2-domen om skydd och säkerhet för lagrade uppgifter

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 4.1 a i direktivet. De 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, att dessa är av känslig natur och 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 (punkt 122 i domen).

Medlemsstaterna måste vidare 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 EU:s rättighetsstadga 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 (punkt 123 i domen).

Skydds- och säkerhetsnivåer

Enligt EU-domstolen måste leverantörerna av elektroniska kommunikationstjänster alltså garantera en särskilt hög skydds- och säkerhetsnivå för trafik- och lokaliseringsuppgifter genom lämpliga tekniska och organisatoriska åtgärder.

Av 6 kap. 3 a § lagen om elektronisk kommunikation framgår att den som är lagringsskyldig enligt 6 kap. 16 a § ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. I förarbetena anges att det därav följer att bestämmelsen, till skillnad från vad som gäller enligt 6 kap. 3 §, 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 bemyndigas regeringen eller den myndighet regeringen bestämmer att komplettera lagbestämmelsen med ytterligare föreskrifter om säkerheten. Detta har regeringen gjort i 37 § förordningen (2003:396) om elektronisk kommunikation. Av bestämmelsen, som har godkänts av riksdagen (bet. 2011/12:JuU26, skr. 2011/12:288), 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. Post- och Telestyrelsen (PTS) får efter att ha hört Polismyndigheten, Säkerhetspolisen och Datainspektionen meddela närmare föreskrifter om de åtgärder som ska vidtas. PTS har med stöd av 37 § i förordningen meddelat sådana föreskrifter (PTSFS 2012:4). Dessa går i korthet ut på att den lagringsskyldige ska bedriva ett kontinuerligt och systematiskt säkerhetsarbete med beaktande av de särskilda risker lagringsskyldigheten medför (3 §). Rutiner ska finnas som säkerställer att bara personal med särskild behörighet har tillgång till lagrade uppgifter och de system som hanterar uppgifterna (4 §). Den utrustning som används för att lagra uppgifter ska också placeras i ett särskilt skyddat utrymme för att förhindra förlust av eller otillåten tillgång till uppgifterna (5 §). Vidare ska all behandling av lagrade uppgifter loggas i krypterad form och på ett sådant sätt att det går att se vem som har haft tillgång till uppgifterna och vid vilken tidpunkt (6 §). Lagrade uppgifter ska också säkerhetskopieras (7 §).

Utredningen anser att de ovan beskrivna svenska reglerna om skydds- och säkerhetsnivåer uppfyller de krav som EU-rätten ställer. Ingen remissinstans invänder mot det. Regeringen delar denna bedömning.

Utplåning av uppgifter

EU-domstolen har fastslagit att EU-rätten kräver att uppgifter som är föremål för datalagring oåterkalleligen ska förstöras när deras lagringstid har gått ut.

I 6 kap. 6 d § lagen om elektronisk kommunikation föreskrivs att den lagringsskyldige genast ska utplåna uppgifterna vid lagringstidens utgång. Om uppgifterna har begärts utlämnade före utgången av lagringstiden men innan uppgifterna har hunnit lämnas ut, följer dock av bestämmelsen att leverantören ska fortsätta lagra uppgifterna till dess ett utlämnande har skett. Därefter ska leverantören genast utplåna dem. Regeringen delar utredningens bedömning att den svenska regleringen är i överensstämmelse med EU-rättens krav.

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.

PTS utövar tillsyn över verksamhet som bedrivs med stöd av lagen om elektronisk kommunikation. Myndighetens tillsyn omfattar en kontroll av att lagen och de beslut om skyldigheter eller villkor som har meddelats med stöd av lagen följs (7 kap. 1 §). För att kunna utöva en effektiv tillsyn har PTS en rad befogenheter till sitt förfogande. PTS har rätt att för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av lagen bedrivs (7 kap. 2 §). Vidare får PTS förelägga en leverantör att tillhandahålla myndigheten de upplysningar och handlingar som behövs för kontrollen (7 kap. 3 §). Finner PTS skäl att misstänka att den som bedriver verksamhet enligt lagen om elektronisk kommunikation inte följer lagen eller de föreskrifter som har meddelats med stöd av lagen, ska myndigheten underrätta den som bedriver verksamheten om detta förhållande och ge denne möjlighet att yttra sig (7 kap. 4 §). PTS får också meddela de förelägganden och förbud som behövs för att rättelse av en överträdelse ska ske omedelbart eller inom skälig tid. Ett sådant föreläggande eller förbud får förenas med vite. Om föreläggandet inte följs, får PTS återkalla ett tillstånd, ändra tillståndsvillkor eller ytterst besluta att den som har åsidosatt en skyldighet helt eller delvis ska upphöra med verksamheten (7 kap. 5 §). PTS beslut får överklagas hos allmän förvaltningsdomstol (8 kap. 19 §).

Vad gäller tillsynen över personuppgiftsbehandling generellt är Datainspektionen tillsynsmyndighet. Dessutom har Säkerhets- och integritetsskyddsnämnden en tillsynsroll när det gäller den personuppgifts-behandling som utförs i polisens brottsbekämpande verksamhet. Att de tre myndigheter som har tillsynsansvar på området har en tillräcklig grad av oberoende följer av 12 kap. 2 § regeringsformen.

I likhet med utredningen anser regeringen att det finns en tillräcklig grad av oberoende tillsyn för att det svenska regelverket ska vara förenligt med EU-rätten.

8.2 Lagringen bör ske inom EU

Regeringens bedömning: Eftersom det i den svenska regleringen saknas regler om var lagring av uppgifter som omfattas av lagringsskyldigheten får ske, uppfyller den inte EU-rättens krav. Lagring av uppgifter bör ske inom EU. Detta bör regleras i förordning.

Utredningens bedömning och förslag överensstämmer delvis med regeringens. Utredningen föreslår att uppgifter som omfattas av lagringsskyldigheten inte ska få lagras utanför Sverige.

Remissinstanserna: *Åklagarmyndigheten, Ekobrottsmyndigheten, Säkerhetspolisen, Tullverket, Datainspektionen, Post- och telestyrelsen (PTS)* och *Hovrätten för Övre Norrland* tillstyrker förslaget att lagringen av uppgifter ska ske i Sverige. *Tullverket* anser att det kan behöva belysas ytterligare hur lagringen i praktiken ska kunna genomföras hos berörda operatörer. *PTS* anser att en lagring i Sverige kommer ge bättre möjligheter att rent faktiskt kontrollera att lagringen sker i enlighet med gällande regler. Myndigheten framför vidare att lagring i utlandet skulle kunna medföra betydande risker för nationell säkerhet, t.ex. genom möjligheten för utländska aktörer att bedriva inhämtning av uppgifter som ett led i underrättelseverksamhet mot Sverige eller svenska intressen.

Säkerhets- och integritetsskyddsnämnden (SIN) och *Stockholms tingsrätt* ifrågasätter om en lagringsskyldighet i Sverige är förenlig med EU-rätten och vill att frågan analyseras vidare. *Skatteverket* påpekar att förslaget, i den mån ett sådant krav inte kan anses berättigat av hänsyn till allmän säkerhet, kan komma att påverkas av ett antagande av förslag till förordning om en ram för det fria flödet av icke-personuppgifter i EU.

Tele2 Sverige AB, Colt Technology Services AB och *the Business Carrier Coalition (BCC)* avstyrker förslaget och anser att utredningens argument för en lagring i Sverige strider mot grundprinciperna i EU-rätten om fri rörlighet inom unionen, om etableringsfriheten, det fria tillhandahållande av tjänster och det fria flödet av personuppgifter som garanteras i EU:s allmänna dataskyddsförordning (dataskyddsförordningen) och i direktiv 2002/58. Förslaget skulle innebära att operatörer skulle kunna tvingas sätta upp separata lagringssystem i uppemot 28 länder, och riskerar därmed skapa ytterligare barriärer mot förverkligandet av en digital inre marknad. Det är vanligt att lagring sker utanför Sverige eftersom det är kostnadseffektivt, lättare att administrera och att skydda data. Genom centralisering finns bättre möjligheter till att ha ett utbyggt skalskydd, bättre säkerhetsrutiner, bemanning och kontroll. Förslaget skulle minska operatörernas möjligheter att bedriva en kostnadseffektiv lagring. Dessa remissinstanser ifrågasätter vidare att tillsynen skulle bli mer kraftfull med en lagring i Sverige.

Skälen för regeringens bedömning: EU-domstolen anger i Tele2-domen att den nationella lagstiftningen måste föreskriva att datalagrade uppgifter inte ska få lagras utanför unionen. 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 som

gjordes av Datalagringsutredningen bedömdes att det inte borde införas något uttryckligt förbud mot att uppgifter som lagras enligt de svenska datalagringsreglerna fördes över till tredjeland (SOU 2015:31 s. 178). Genom EU-domstolens tydliga ställningstagande i Tele2-domen blir den sistnämnda bedömningen inte längre hållbar. Eftersom det i dag inte finns några regler som anger var lagring får ske uppfyller den svenska regleringen således inte EU-rättens krav. I likhet med vad utredningen anför bör det därför införas ett förbud mot att lagra de nu aktuella uppgifterna utanför EU. Mot bakgrund av bedömningen att lagring inte bör tillåtas i tredjeland, dvs. utanför EU, väljer regeringen att inte redovisa de remissvar som kommit in gällande Datalagringsutredningens bedömning i denna fråga.

Enligt 6 kap. 3 a § lagen om elektronisk kommunikation får regeringen meddela föreskrifter om skyddsåtgärder för att skydda de lagrade uppgifterna vid behandling. I likhet med utredningen anser regeringen att föreskrifterna om var lagringen får ske bör meddelas i förordningen om elektronisk kommunikation. Även om det alltså är regeringen som har det slutgiltiga ansvaret för att det svenska regelverket lever upp till EU-rättens krav finns det ändå anledning att övergripande beskriva hur regeringen ser på frågan om var lagringen bör ske.

Utredningen anser att regleringen om var lagringen ska ske bör gå ännu längre än vad EU-domstolen har uttalat och föreslår att lagringen endast ska få ske i Sverige. Utredningen anser att en sådan reglering skulle förstärka den tillsyn som PTS bedriver och att konfidentialiteten skulle skyddas på ett bättre sätt om uppgifter endast lagras i Sverige. Flera remissinstanser, t.ex. *Åklagarmyndigheten, Säkerhetspolisen, Datainspektionen, PTS* och *Hovrätten för Övre Norrland*, tillstyrker förslaget, främst eftersom det skulle innebära en förbättrad tillsynsmöjlighet. Det finns emellertid flera remissinstanser som avstyrker förslaget eller har invändningar mot det, bl.a. *SIN, Stockholms tingsrätt, Tele2 Sverige AB* och *the Business Carrier Coalition (BCC)*. Dessa remissinstanser ifrågasätter bl.a. förslagets förenlighet med EU-rätten.

När det gäller frågan om tillsyn kan det inledningsvis konstateras att enligt svensk rätt gäller leverantörens skyldigheter om hur lagringsskyldigheten ska fullgöras även om lagringen förläggs utomlands, t.ex. vad gäller de krav som rör säkerheten för de lagrade uppgifterna (prop. 2010/11:46 s. 60). Detta måste särskilt beaktas av leverantörerna om de överväger att lagra uppgifter utomlands. Det ingår i PTS ansvar att kontrollera att leverantörerna följer regleringen i lagen om elektronisk kommunikation och de föreskrifter som har meddelats med stöd av lagen. Även detta ansvar gäller oberoende av var leverantörerna väljer att lagra uppgifter. Som framgår i föregående avsnitt har PTS en rad befogenheter till sitt förfogande för att kontrollera att leverantörerna följer skydds- och säkerhetsreglerna. Regeringen bedömde när datalagringsdirektivet genomfördes att de befogenheter PTS har är tillräckliga för att myndigheten ska 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 lagen om elektronisk kommunikation bedrivs, kan dock i praktiken utövas

endast i Sverige. I detta avseende skulle en lagringsskyldighet i Sverige underlätta tillsynen, såsom t.ex. *PTS* påpekar. Däremot påverkas 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 denna bakgrund bedömer regeringen – i likhet med sitt tidigare ställningstagande och i enlighet med vad *Tele2 Sverige AB* framhåller – att PTS:s möjligheter att bedriva en aktiv och ändamålsenlig tillsynsverksamhet får anses vara tillfyllest även gentemot leverantörer som väljer att lagra uppgifter utanför Sverige, men inom EU. Det kan i sammanhanget också påpekas att leverantörernas tystnadsplikt och deras skyldighet att se till att beslut om inhämtning av uppgifter kan verkställas inte påverkas av var uppgifterna lagras. Även om uppgifterna lagras inom EU har leverantörerna således en skyldighet att se till att verkställigheten sker på ett sådant sätt att den inte röjs. Dessutom är de personuppgifter som behandlas också omgärdade av integritetsskyddande lagstiftning genom i första hand direktiv 2002/58.

Flera remissinstanser, bl.a. *SIN, Stockholms tingsrätt, Tele2 Sverige AB* och *BCC,* invänder mot förslagets förenlighet med EU-rätten. Bl.a. Tele2 Sverige AB och BCC anser att en begränsning till Sverige skulle strida mot grundprinciperna i EU-rätten om fri rörlighet inom unionen, om etableringsfriheten, det fria tillhandahållande av tjänster och det fria flödet av personuppgifter som stadgas i dataskyddsförordningen och i direktiv 2002/58. *Skatteverket* hänvisar till Europaparlamentets och rådets förordning 2018/1807 av den 14 november 2018 om en ram för det fria flödet av andra data än personuppgifter i Europeiska unionen (i det följande dataflödesförordningen). Dataflödesförordningen, som antogs i början av november 2018, gäller i situationer då det inte är fråga om personuppgiftsbehandling. Den innehåller bl.a. bestämmelser om att en medlemsstat inte får föreskriva att en viss typ av uppgifter endast ska få lagras i just den medlemsstaten förutsatt att ett sådant förbud inte motiveras av allmän säkerhet (artikel 4). Förordningen är inte tillämplig på verksamhet som inte omfattas av unionsrättens tillämpningsområde och det konstateras att den nationella säkerheten är varje medlemsstats eget ansvar (artikel 2.3 och beaktandesats 12).

Regeringen konstaterar att ovannämnda EU-rättsliga principer och den reglering om det fria flödet av uppgifter (personuppgifter respektive andra data än personuppgifter) som finns både i dataskyddsförordningen, i direktiv 2002/58 och i dataflödesförordningen, skulle kunna utgöra ett hinder mot att förbjuda att lagring sker i andra unionsländer. Samtidigt går det inte att bortse från den farhåga som *PTS* framför om att lagring i utlandet skulle kunna medföra risker för nationell säkerhet. Enligt 6 kap. 19 § lagen om elektronisk kommunikation ska operatörerna bedriva sin verksamhet så att beslut om hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs. Detta krav gäller oavsett om verkställandet omfattar uppgifter som rör Sveriges säkerhet eller inte. Den 1 april 2019 träder dessutom en ny säkerhetsskyddslag (2018:585) och säkerhetsskyddsförordning (2018:658) i kraft. Alla verksamhetsutövare som omfattas av

lagen blir då enligt 2 kap. 1 § säkerhetsskyddslagen skyldiga att genom en säkerhetsskyddsanalys utreda behovet av säkerhetsskydd för den aktuella verksamheten. Med utgångspunkt i analysen ska verksamhetsutövaren bl.a. vidta åtgärder som förebygger att säkerhetsskyddsklassificerade uppgifter obehörigen röjs, ändras, görs otillgängliga eller förstörs. Säkerhetsskyddsklassificerade uppgifter definieras i 1 kap. 2 § andra stycket som uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig. Därigenom klargörs att lagstiftningen gäller för såväl offentliga som privata aktörer. Förordningen innehåller bestämmelser som begränsar utlämnandet av säkerhetsskyddsklassificerade uppgifter till utländska aktörer (3 kap. 9 § andra stycket). Enligt denna bestämmelse får säkerhetsskyddsklassificerade uppgifter inte lämnas till en utländsk leverantör om inte Sverige har ingått en överenskommelse om säkerhetsskydd med den andra staten och leverantören har godkänts genom en kontroll enligt den andra statens säkerhetsskyddslagstiftning. Det finns också bestämmelser i 2 kap. 6 § förordningen som begränsar möjligheten för statliga myndigheter att genom utkontraktering lämna ut uppgifter till utländska aktörer. Regeringen kan således konstatera att alla privata aktörer, även t.ex. teleoperatörer, i enlighet med säkerhetsskyddsregleringen behöver analysera och bedöma om det i verksamheten finns säkerhetsskyddsklassificerade uppgifter som behöver skyddas på något särskilt vis. En sådan analys kan mynna ut i att lagringen av uppgifterna behöver ske i Sverige för att säkerhetsskyddet ska kunna tillgodoses. I sammanhanget förtjänas också att nämnas att även verksamheter som hanterar större mängder av uppgifter som inte är säkerhetsskyddsklassificerade, t.ex. sammanställningar av information, kan bedömas vara av betydelse för Sveriges säkerhet. Det innebär att hantering, lagring eller andra åtgärder som ger aktörer utanför Sverige tillgång till uppgifterna i vissa fall kan vara direkt olämpliga ur säkerhetsskyddssynpunkt (se prop. 2017/18:89 s. 45). Tillsyn över att kraven i den nya säkerhetsskyddslagstiftningen följs kommer att utövas av PTS och Säkerhetspolisen.

Utredningens förslag skulle dock innebära en skyldighet att lagra alla uppgifter, oavsett dess relevans för nationell säkerhet, i Sverige. Mot ett sådant generellt krav på lagring av uppgifter i Sverige talar bl.a., såsom bl.a. *Colt Technology Services AB* påpekar, att en sådan begränsning skulle innebära att leverantörer som har verksamhet i flera länder inom EU inte kan centralisera sin verksamhet, vilket kan försämra möjligheterna till att bedriva en kostnadseffektiv lagring. Mot denna bakgrund anser regeringen att utredningens förslag om att all lagring bör begränsas till Sverige kan ifrågasättas. Det finns därför starka skäl att i stället föreskriva att lagringen inte får ske utanför EU.

9 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Lagändringarna ska träda i kraft den 1 oktober 2019.

Regeringens bedömning: Lagändringarna medför inget behov av några övergångsbestämmelser.

Datalagringsutredningens förslag överensstämmer inte med regeringens. Utredningen föreslår att regleringen ska träda i kraft den 1 juli 2016.

Remissinstanserna yttrar sig inte särskilt i denna fråga.

Utredningens förslag överensstämmer inte med regeringens. Utredningen föreslår att regleringen ska träda i kraft den 1 december 2018.

När det gäller föreslagen ändring i förordningen om elektronisk kommunikation som gäller lagringsskyldigheten för annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare vid internetåtkomst, föreslår utredningen att den bestämmelsen inte ska behöva tillämpas förrän den 1 april 2019.

Remissinstanserna: *Säkerhetspolisen* understryker att det är av största vikt att de nya bestämmelserna om datalagring träder i kraft så snart som möjligt. *Post- och telestyrelsen (PTS)* anser att utredningens förslag om att förordningsändringen som gäller lagringsskyldigheten för annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare vid internetåtkomst, ska träda i kraft den 1 april 2019 innebär en ytterst begränsad tid för PTS att hinna ta fram föreskrifter i frågan. Myndigheten påpekar också att det kan antas att berörda tillhandahållare kommer att få ont om tid att hinna genomföra nödvändiga tekniska anpassningar innan ändringarna träder i kraft. I övrigt lämnar remissinstanserna inte några synpunkter gällande ikraftträdande- eller övergångsbestämmelser.

Skälen för regeringens bedömning och förslag: Lagändringarna bör träda i kraft så snart som möjligt. Regeringen föreslår att beslutsordningen enligt inhämtningslagen ändras på så vis att Säkerhetspolisen, Polismyndigheten och Tullverket framöver inte själva kommer att fatta beslut om tillgång till uppgifter, utan i stället kommer behöva ansöka om tillstånd hos åklagare. En viss förberedelsetid behövs för den nya beslutsordningen. När det gäller de förändringar som avser lagringsskyldighetens omfattning är det också rimligt att operatörerna får en viss tid på sig att göra de förändringar som krävs i sina datalagringssystem. Mot den bakgrunden och med hänsyn till den tid som de olika leden i lagstiftningsprocessen förväntas ta bedömer regeringen att den 1 oktober 2019 är den tidigaste möjliga tidpunkten för ikraftträdande av de av de författningsändringar som föreslås.

I likhet med vad utredningen och *PTS* påpekar finns det dock ett behov av ytterligare förberedelsetid när det gäller lagringsskyldigheten för annan uppgift som är nödvändig för att identifiera abonnent och registrerad användare vid internetåtkomst (s.k. NAT-teknik). Det bör därför inte finnas någon lagringsskyldighet i denna del före den 1 april 2020.

10 Konsekvenser

Regeringens bedömning: En lagringsskyldighet som är begränsad till ett antal uppgiftsslag, förbud mot lagring utanför EU och förslaget att åklagare ska fatta beslut enligt inhämtningslagen förväntas stärka integritets- och personuppgiftsskyddet.

En begränsad lagringsskyldighet kan minska möjligheterna att bekämpa brott men behöver inte innebära att brottsligheten kommer att öka. Förslaget om möjligheten att hämta in uppgifter i underrättelseverksamhet om brottslig verksamhet som innefattar statsstyrt företagsspioneri och vissa s.k. systemhotande brott, innebär att dessa brott mer effektivt kommer att kunna förebyggas, förhindras och upptäckas.

De tekniska anpassningar som behövs för en förändrad lagringsskyldighet leder till kostnadsökningar för operatörerna.

Förslaget att åklagare ska fatta beslut enligt inhämtningslagen bedöms leda till ökade kostnader för Åklagarmyndigheten. Finansieringen av dessa kostnader sker genom en omfördelning mellan myndigheterna inom utgiftsområde 4 Rättsväsendet.

Förslagen bedöms inte få några effekter på miljön eller för jämställdheten mellan kvinnor och män.

Datalagringsutredningens bedömning överensstämmer med regeringens.

Remissinstanserna uttalar sig inte särskilt om utredningens bedömning.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: *Polismyndigheten, Åklagarmyndigheten, Ekobrottsmyndigheten, Säkerhetspolisen, Tullverket* och *Ecpat Sverige* framhåller att varje begränsning av lagringsskyldigheten kommer att få allvarliga konsekvenser för myndigheternas förmåga att upptäcka, förhindra, bekämpa, utreda och lagföra brott.

Bahnhof AB, Com Hem AB, RISE SICS AB, Colt Technology Services AB, Dataskydd.net, Svenska stadsnätsföreningen, Föreningen Digitala fri- och rättigheter (Dfri), Stiftelsen för Internetsinfrastruktur och *IT&Telekomföretagen* anser att det finns en risk att återigen hamna i en rättslig osäkerhet där företag åläggs nya skyldigheter som driver kostnader och blockerar utvecklingsresurser, tills det sannolikt kommer att konstateras att lagringsskyldigheten bryter mot EU-rätten och måste rivas upp. *Svenska stadsnätsföreningen, RISE SICS AB, Colt Technology Services AB, The Business Carrier Coalition (BCC)* och *Dataskydd.net* påpekar att en förändrad lagringsskyldighet för de operatörer som använder NAT-teknik kommer att innebära att dessa behöver anpassa sina system och lagra många fler uppgifter än förut, vilket innebär stora kostnadsökningar.

Åklagarmyndigheten anser att ett större årligt resurstillskott än vad utredningen beräknat kommer att krävas för uppgiften att vara beslutsfattande myndigheten enligt inhämtningslagen. *Polismyndigheten, Säkerhetspolisen* och *Tullverket* påpekar att även om beslutsfattandet flyttar kommer det inte

per automatik innebära att kostnaderna minskar för myndigheterna. Snarare torde nya moment som beredning av underlag, föredragning m.m. i förhållande till en ny myndighet tillkomma.

Skälen för regeringens bedömning

Inledande utgångspunkter

Som framgår av tidigare avsnitt (avsnitt 5, 6 och 8) innebär förslagen att det i lag och förordning görs vissa anpassningar för att få regelverket i överensstämmelse med EU-rätten. Konsekvensbedömningarna i detta avsnitt bygger både på förslagen om anpassningar i lagstiftningen och på de anpassningar som regeringen i förordning avser genomföra.

Som framgår av avsnitt 5 är området för elektronisk kommunikation i ständig förändring med nya kommunikationstjänster som tillkommer samtidigt som andra tjänster försvinner eller används mindre, vilket leder till nya kommunikationsmönster hos användarna. Det kan i sin tur få till följd att bedömningen av vad som bör lagras förändras över tid. Frågan om hur EU-rätten ska tolkas är också föremål för prövning av EU-domstolen (t.ex. Privacy International m.fl., Ordre des barreaux francophones et germanophone m.fl. samt förenade målen La Quadrature du Net m.fl. och French Data Network m.fl., se vidare avsnitt 5.1). Inom EU-kretsen pågår också arbete i frågan, bl.a. diskussioner om det bör införas ett nytt EU-regelverk för datalagring på det brottsbekämpande området. Mot denna bakgrund anser regeringen att det, senast fyra år efter ikraftträdandet, kan finnas anledning att utvärdera de ändringar som nu föreslås.

Samhällspolitiska konsekvenser

De förändringar i lagringsskyldigheten som nu föreslås syftar till att stärka skyddet för den enskildes privatliv och kommunikation, då såväl intrånget som risken för intrång minskar med en begränsning av lagringsskyldigheten. Om färre uppgifter lagras om människors elektroniska kommunikationer, lagras mindre information som gör det möjligt att dra slutsatser om individers vanor och företeelser. Skyddet för känsliga uppgifter förstärks också genom att ett förbud mot att lagra uppgifterna utanför EU införs. Skyddet ökar vidare genom att det inte längre blir möjligt för myndigheterna att få tillgång till de lagrade trafik- och lokaliseringsuppgifterna utan en förhandsprövning av en oberoende myndighet eller domstol. Härigenom omgärdas uppgifterna av ytterligare en rättssäkerhetsgaranti. Det kan därigenom antas att förtroendet för statens tvångsmedelsanvändning kan komma att öka.

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 vissa fall leda till att mer integritetskränkande tvångsmedel måste användas i stället. Sammantaget bedöms dock reformen innebära integritetsvinster.

Såsom bl.a. *Polismyndigheten, Åklagarmyndigheten, Säkerhetspolisen* och *Ecpat Sverige* framhåller kommer en begränsad lagringsskyldighet minska möjligheterna att bekämpa brott. Effekten av hemlig övervakning av elektronisk kommunikation, som är beroende av tillgång till lagrade uppgifter, förväntas därför att minska vilket kan påverka brottsuppklaringen på ett negativt sätt. Det bör dock noteras att de brottsbekämpande myndigheterna fortfarande kommer att ha tillgång till den uppgiftsmängd som sparas för operatörernas egna ändamål. Det innebär att vissa uppgifter som inte omfattas av lagringsskyldigheten ändå kommer att finnas tillgängliga hos vissa operatörer och därmed kan begäras ut av de brottsbekämpande myndigheterna. Därtill kan det antas att andra informationskällor kan komma att användas i högre utsträckning i förundersökningar och därmed minska de negativa effekterna av en minskad lagring. I underrättelseverksamheten saknas det emellertid i princip straffprocessuella tvångsmedel som kan kompensera för sänkt effektivitet i de hemliga tvångsmedlen enligt inhämtningslagen och preventivlagen. De försämringar i underrättelseverksamheten som blir följden av en minskad lagringsskyldighet förväntas således inte kunna kompenseras med andra åtgärder i någon större utsträckning. Påverkan på underrättelseverksamheten kommer därför sannolikt att bli större än på förundersökningsverksamheten.

I motsatt riktning verkar utredningens förslag om att NAT-teknik inte längre kommer att hindra en meningsfull inhämtning av uppgifter. Såsom utredningen påpekar skulle hemlig övervakning av elektronisk kommunikation vad avser internetrelaterad brottslighet i praktiken kunna bli helt meningslös på grund av NAT-tekniken. Som regeringen anför i avsnitt 5.2 bör detta problem nu åtgärdas och det kan då förväntas vara en tämligen verkningsfull förstärkning av de brottsbekämpande myndigheternas förmåga att klara upp brott som begåtts med hjälp av internet.

Den minskade brottsuppklaring som kan bli följden av en förändrad lagringsskyldighet bedöms sammantaget inte påverka brottsligheten i samhället i stort.

Förslaget i fråga om inhämtning av uppgifter om brottslig verksamhet som innefattar statsstyrt företagsspioneri och vissa systemhotande brott leder till att sådan brottslighet mer effektivt kommer att kunna förebyggas, förhindras och upptäckas.

Vad gäller de politiska målen för sektorn elektronisk kommunikation förväntas förslagen i denna lagrådsremiss, såsom nedan utvecklas närmare, leda till ökade kostnader för lagring för tillhandahållare av elektroniska kommunikationstjänster. Kostnaderna har inte varit möjliga att kvantifiera fullt ut, men de bedöms för vissa aktörer inte försumbara. Ökade kostnader för tillhandahållarna kan leda till minskade investeringar och därmed sämre kvalitet i tjänsterna. Sammantaget bedöms dessa samhällspolitiska konsekvenser emellertid uppvägas av de vinster som förväntas i brotts-bekämpningen.

Regeringen bedömer att förslagen inte kommer att få några negativa effekter på miljön eller för jämställdheten mellan kvinnor och män.

Konsekvenser för företagen

För de lagringsskyldiga inom sektorn för elektronisk kommunikation kommer en förändrad lagringsskyldighet innebära att datasystemen behöver anpassas till de nya förutsättningarna. Detta är en kostnadsdrivande faktor för företagen. Såsom utredningen och några remissinstanser, bl.a. *Svenska stadsnätsföreningen, RISE SICS AB, Colt Technology Services AB* och *Dataskydd.net,* påpekar bedöms en förändrad lagringsskyldighet för de operatörer som använder NAT-teknik innebära att de kommer att behöva anpassa sina system och lagra fler uppgifter än förut, vilket innebär kostnadsökningar. Dels krävs en engångsinvestering i form av ombyggnad av systemen för en del operatörer, dels krävs större kapacitet vad gäller lagringsutrymme vid en mer omfattande lagring. Hur stora kostnadsökningar det kan bli fråga om har operatörerna enligt utredningen inte kunnat kvantifiera. Remissvaren ger inte heller någon mer information i detta avseende. Å ena sidan har några operatörer uppgett för utredningen att en sådan förändring skulle medföra att kostnaderna skulle skjuta i höjden och hamna på helt orimliga nivåer. 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 det alltså är svårt att kvantifiera hur stora kostnaderna kan komma att bli, delar regeringen utredningens bedömning att kostnaderna bedöms öka, i varje fall för de operatörer som använder sig av NAT-teknik.

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. I förarbetena anges t.ex. arbetsgivares skyldighet att uppbära, redovisa och inbetala preliminär skatt för anställda och miljöfarlig verksamhet där företagen måste investera stora summor för att minimera de skador som kan följa med verksamheten (prop. 1995/96:180 s. 32–36 och prop. 2010/11:46 s. 66–68). Regeringen menade att det inte fanns någon avgörande principiell skillnad mellan dessa förpliktelser och en förpliktelse att på egen bekostnad anpassa telesystemen så att möjligheterna till hemlig teleavlyssning och hemlig teleövervakning bibehålls. Regeringen anförde vidare att hemlig teleavlyssning och hemlig teleövervakning inte kunde sägas inta någon särställning i detta hänseende endast på den grunden att det rörde sig om brottsbekämpande verksamhet. I stället framhölls att televerksamheten är så speciell att det är oundvikligt att ett relativt stort samhällsansvar måste följa med verksamheten. Regeringen uttryckte också att det redan fanns lagstadgade skyldigheter för företag att vidta vissa åtgärder för att underlätta den brottsbekämpande verksamheten. Som exempel nämndes bankernas skyldigheter enligt dåvarande lagen om åtgärder mot penningtvätt. Skyldigheterna för fysiska och juridiska personer att vidta vissa åtgärder för

att förebygga, upptäcka och förhindra penningtvätt och finansiering av terrorism och på så sätt underlätta den brottsbekämpande verksamheten har därefter skärpts (se t.ex. prop. 2016/17:173).

Förutom att vila på ovannämnda principiella ställningstagande har den nuvarande modellen 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). Regeringen finner inte skäl att nu ändra denna bedömning. Eftersom ingen av de förändringar som föreslås rubbar de ovan redovisade utgångspunkterna eller fördelarna med systemet, bör den gällande modellen för kostnadsfördelning inte frångås. Det innebär att operatörerna alltjämt ska stå för kostnader för anpassning, drift och underhåll samtidigt som det allmänna ska ersätta operatörerna för de kostnader som hänför sig till utlämnande av uppgifter i enskilda ärenden.

I likhet med utredningen bedömer regeringen att både små och stora företag kommer att ha i vart fall delvis liknande förutsättningar att kunna anpassa sig till ett förändrat regelverk. Förslagen bedöms således inte få någon avgörande konkurrenspåverkan inom gruppen av tillhandahållare av elektroniska kommunikationstjänster.

Flera remissinstanser, t.ex. *Bahnhof AB, Com Hem AB, Föreningen Digitala fri- och rättigheter (Dfri), Stiftelsen för Internetsinfrastruktur* och *IT&Telekomföretagen,* reser farhågor om att företagen åläggs nya skyldigheter som driver kostnader och blockerar utvecklingsresurser som riskerar att förloras om det framöver skulle konstateras att lagrings-skyldigheten alltjämt bryter mot EU-rätten och således måste rivas upp. Såsom framgår i denna lagrådsremiss anser regeringen att den reform som nu bör genomföras medför att regleringen blir förenlig med EU-rätten och således kan förväntas stå sig över tid.

Konsekvenser för myndigheter

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 § lagen om elektronisk kommunikation). Hur stor denna ersättning är bestäms av Post- och telestyrelsen (46 § förordningen om elektronisk kommunikation). Vid en minskad lagrings-skyldighet kan det 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 som 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 regeringen, i likhet med utredningen, bedömningen att kostnaderna som uppstår för myndigheterna när lagrade uppgifter begärs ut inte kommer att påverkas på något märkbart sätt.

Åklagare föreslås få en roll vid beslutsfattande enligt inhämtningslagen. Som utredningen och *Åklagarmyndigheten* anför innebär förslaget att myndigheten kommer att få ökade kostnader, dels i form av ökade löpande kostnader för personal, dels i form av engångskostnader för it-anpassningar och utbildningar. Utredningen bedömer att den nya beslutsordningen innebär vissa besparingar för Polismyndigheten, Säkerhetspolisen och Tullverket och föreslår att medel ska flyttas från dessa myndigheter till Åklagarmyndigheten. Denna bedömning delas inte av *Polismyndigheten, Säkerhetspolisen* och *Tullverket* som anför att även om beslutsfattandet flyttar kommer det inte per automatik innebära att kostnaderna minskar för myndigheterna. Snarare torde nya moment som beredning av underlag, föredragning m.m. i förhållande till en ny myndighet tillkomma. Regeringen delar utredningens och Åklagarmyndighetens bedömning att förslaget kommer innebära ökade kostnader för Åklagarmyndigheten. Finansieringen av kostnaderna kan ske genom en omfördelning mellan myndigheterna inom utgiftsområde 4 Rättsväsendet. Regeringen föreslog därför i budgetpropositionen för 2019 att Åklagarmyndighetens anslag ökas med 3 000 000 kronor för 2019 samt med 1 000 000 kronor från och med 2020. Ökningen finansieras genom en minskning av Polismyndighetens och Säkerhetspolisens anslag (prop. 2018/19:1, utgiftsområde 4 avsnitt 2.7.3). Riksdagen har beslutat i enlighet med förslaget (bet. 2018/19:JuU1, rskr. 2018/19:73).

Förslaget om möjligheten att hämta in uppgifter i underrättelseverksamhet om brottslig verksamhet som innefattar statsstyrt företagsspionerі och vissa s.k. systemhotande brott innebär att utredning och hantering av tillstånd enligt inhämtningslagen kan förväntas öka något. I likhet med vad Datalagringsutredningen anför bedömer regeringen att denna förändring inte kan förväntas leda till annat än rent marginella kostnadsökningar för berörda myndigheter.

För att säkerställa att otillbörliga rättighetskränkningar inte sker och att principen om icke-diskriminering följs i de fall personuppgifter som har varit föremål för datalagring behandlas av de brottsbekämpande myndigheterna är det nödvändigt att säkerställa integritetsskyddet, bl.a. genom kontinuerlig kompetensutveckling. Detta bör ske som en del av den ordinarie kompetensutveckling som erbjuds personal inom berörda myndigheter, framför allt Polismyndigheten. Av 3 kap. 2 § brottsdatalagen (2018:1177) följer också att lämpliga tekniska och organisatoriska åtgärder ska vidtas för att säkerställa och kunna visa att behandlingen av personuppgifter är författningsenlig och att den registrerades rättigheter skyddas. Genom t.ex. tillämpning av principerna inbyggt dataskydd och dataskydd som standard (se 3 kap. 3 och 4 §§ brottsdatalagen, prop. 2017/18:232 s. 174–175) ska integritetsperspektivet genom rutiner utgöra en integrerad del i den löpande verksamheten och beaktas redan vid utformningen av behövliga it-stöd.

11 Författningskommentar

11.1 Förslaget till lag om ändring i lagen (2003:389) om elektronisk kommunikation

6 kap.

16 a § Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § är skyldig att lagra sådana uppgifter som avses i 20 § första stycket 1 och 3 som är nödvändiga för att spåra och identifiera kommunikationskällan, *målet* för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning vid kommunikationens början och slut.

Skyldigheten att lagra uppgifter enligt första stycket omfattar uppgifter som genereras eller behandlas vid telefonitjänst *och* meddelandehantering *via mobil nätanslutningspunkt samt vid* internetåtkomst. Även vid *en* misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas.

Den som är skyldig att lagra uppgifter enligt denna paragraf får uppdra åt någon annan att utföra lagringen.

Regeringen eller den myndighet som regeringen bestämmer *kan med stöd av 8 kap. 7 § regeringsformen meddela* närmare föreskrifter om vilka uppgifter som ska lagras enligt denna paragraf.

Paragrafen innehåller grundförpliktelsen för operatörerna i fråga om datalagring. Övervägandena finns i avsnitt 5.3.

Ändringen i *första stycket* innebär att uppgift om slutmålet för kommunikationen, dvs. vilket nummer ett samtal styrts till, inte längre ska omfattas av lagringsskyldigheten. Uppgift om vilket nummer ett samtal vidarekopplats till ska alltså inte längre lagras.

Ändringarna i *andra stycket* innebär att endast uppgifter som genereras eller behandlas via en mobil nätanslutningspunkt ska omfattas av lagringsskyldigheten när det gäller telefonitjänst- och meddelandehantering. Med mobil nätanslutningspunkt avses t.ex. en mobiltelefon som kopplar upp sig mot en mobilmast eller mot ett trådlöst lokalt nätverk (wifi) som tillhandahålls av någon som omfattas av lagringsskyldigheten, men inte en mobiltelefon som ansluter till ett privat trådlöst nätverk. En operatör som endast tillhandahåller fast telefoni kommer således inte att omfattas av lagringsskyldigheten. Om ett samtal går från en fast telefon till en mobiltelefon (eller tvärtom) omfattas endast mobiltelefonoperatören av lagringsskyldigheten. Vidare innebär ändringarna att tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform) inte längre ska omfattas av lagringsskyldigheten.

Ändringen i *fjärde stycket* är endast redaktionell.

16 d § Uppgifter som avses i 16 a § ska lagras *enligt följande:*

– Uppgifter som genereras eller behandlas vid telefonitjänst och meddelandehantering via mobil nätanslutningspunkt ska lagras i sex månader. Lokaliseringsuppgifter ska dock endast lagras i två månader.

– Uppgifter som genereras eller behandlas vid internetåtkomst ska lagras i tio månader. Om uppgifterna identifierar den utrustning där kommunikationen slutligt avskiljs från den lagringsskyldige till den enskilda abonnenten ska de dock endast lagras i sex månader.

Lagringstiden räknas från den dag kommunikationen avslutades.

När lagringstiden löpt ut ska den lagringsskyldige genast utplåna uppgifterna. Om en begäran om utlämnande har kommit in innan lagringstiden löpt ut, ska den lagringsskyldige dock fortsätta lagra uppgifterna till dess att de lämnats ut. Efter utlämnandet ska uppgifterna genast utplånas.

Regeringen eller den myndighet som regeringen bestämmer kan med stöd av 8 kap. 7 § regeringsformen meddela närmare föreskrifter om lagringstiden enligt första stycket.

Paragrafen innehåller bestämmelser om hur länge uppgifter som lagras enligt 6 kap. 16 a § ska bevaras. Övervägandena finns i avsnitt 5.4.

Uppgifter om telefonsamtal och meddelanden via en mobil nätanslutningspunkt (t.ex. en mobiltelefon) ska enligt *första stycket första strecksatsen* lagras i sex månader. Sådana uppgifter kan vara telefonnummer, abonnemangsidentitet, utrustningsidentitet, abonnent och tid för samtalet eller meddelandet. Även tid och plats för den första aktiveringen av en förbetald anonym tjänst (kontantkort) omfattas.

Lokaliseringsuppgifter, dvs. uppgifter som visar den geografiska positionen för terminalutrustningen för en användare, ska endast lagras i två månader.

Av *första stycket andra strecksatsen* följer att uppgifter som rör internetåtkomst ska lagras i tio månader. Sådana uppgifter kan vara ip-adress, uppgift om abonnent och datum för på- och avloggning i den tjänst som ger internetåtkomst. Uppgifter som identifierar den utrustning där kommunikationen slutligt avskiljs till en abonnent ska dock lagras i endast sex månader. Vid internetåtkomst via en mobiltelefon avskiljs kommunikationen slutligt vid basstationen.

Andra stycket om att lagringstiden ska räknas från den dag kommunikationen avslutades motsvarar hittillsvarande första stycket första meningen. Ändringarna är endast redaktionella.

Tredje stycket motsvaras till sitt innehåll av hittillsvarande första stycket andra meningen och andra stycket. Ändringarna är endast redaktionella.

I *fjärde stycket* upplyses om att regeringen eller den myndighet som regeringen bestämmer kan meddela verkställighetsföreskrifter.

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

2 § Uppgifter får hämtas in om omständigheterna är sådana att *åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar*

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

2. *sabotage enligt 13 kap. 4 § brottsbalken,*

3. kapning, sjö- eller luftfartssabotage eller flygplatssabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,

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

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

6. företagsspionerі enligt 26 § lagen (2018:558) om företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understödjs av en främmande makt eller av någon som agerar för en främmande makts räkning,

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

8. grov misshandel eller olaga frihetsberövande enligt 3 kap. 6 § eller 4 kap. 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

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

Paragrafen innehåller förutsättningarna för att de uppgifter som anges i 1 § ska få hämtas in. Övervägandena finns i avsnitt 6.8.

Paragrafen ändras på så sätt att hittillsvarande 2 och 3 §§ slås ihop. Ändringen beror på att möjligheten att hämta in uppgifter om brottslig verksamhet som innefattar vissa brott med lägre minimistraff än fängelse två år, enligt hittillsvarande 3 §, inte längre ska vara tidsbegränsad.

Inledningen av *första stycket punkt 1* flyttas till inledningen av paragrafen. Ändringen är endast redaktionell.

Första stycket punkt 2–5 och *7* motsvarar hittillsvarande 3 §. *Punkt 6* och *8* är nya och genom dem införs en möjlighet att hämta in uppgifter om brottslig verksamhet som innefattar statsstyrt företagsspionerі samt grov misshandel eller olaga frihetsberövande i systemhotande syfte. Brotten finns sedan tidigare i brottskatalogen i lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott och har samma innebörd som i den lagen (se prop. 2005/06:177 s. 83–84 och prop. 2013/14:237 s. 194–196).

Paragrafens *andra stycke* motsvaras av hittillsvarande punkt 2.

3 § Beslut om inhämtning av uppgifter fattas av *åklagare vid Åklagarmyndigheten efter ansökan av Polismyndigheten, Säkerhetspolisen eller Tullverket.*

Paragrafen innehåller bestämmelser om vem som fattar beslut om inhämtning av uppgifter. Övervägandena finns i avsnitt 6.5.

Hittills har myndigheterna själva fattat beslut om inhämtning. Ändringen innebär att åklagare vid Åklagarmyndigheten ska fatta beslut om inhämtning av uppgifter. Enligt paragrafen ska en ansökan göras av Polismyndigheten, Säkerhetspolisen eller Tullverket.

4 § I ett beslut om inhämtning av uppgifter ska det anges vilken brottslig verksamhet och vilken tid beslutet avser samt vilket telefonnummer eller *vilken* annan adress, vilken elektronisk kommunikationsutrustning eller vilket geografiskt område beslutet avser. Tiden får inte bestämmas längre än nödvändigt och får, när det gäller tid som infaller efter beslutet, inte överstiga en månad från dagen för beslutet.

Om det inte längre finns skäl för ett beslut om inhämtning av uppgifter, ska beslutet omedelbart hävas *av den ansökande myndigheten*.

Paragrafen reglerar vad som ska ingå i ett beslut om inhämtning och när ett sådant beslut ska hävas. Övervägandena finns i avsnitt 6.5.

Ändringen i *första stycket* är redaktionell.

Andra stycket ändras som en följd av att åklagare ska fatta beslut om inhämtning av uppgifter. Genom ändringen klargörs att det fortfarande är Polismyndigheten, Säkerhetspolisen och Tullverket som är skyldiga att fortlöpande bevaka behovet av en inhämtning och omedelbart häva beslutet om åtgärden inte längre behövs.

5 § *Den ansökande myndigheten ska underrätta Säkerhets- och integritetsskyddsnämnden* om ett beslut om inhämtning av uppgifter enligt denna lag. Underrättelsen ska lämnas senast en månad efter det att ärendet om inhämtning avslutades.

Paragrafen reglerar underrättelseskyldigheten till Säkerhets- och integritetsskyddsnämnden. Övervägandena finns i avsnitt 6.5.

Genom ändringen klargörs att det alltjämt är Polismyndigheten, Säkerhetspolisen och Tullverket som har ansvar för att Säkerhets- och integritetsskyddsnämnden underrättas om ett beslut om inhämtning. Underrättelseskyldigheten bör fullgöras genom att en kopia av beslutet lämnas till Säkerhets- och integritetsskyddsnämnden.

11.3 Förslaget till lag om ändring i lagen (2017:718) om ändring i lagen (2012:279) om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet

Härigenom föreskrivs att lagen (2017:718) om ändring i lagen (2012:279) om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska ha följande lydelse.

3 § lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet ska upphöra att gälla vid utgången av september 2019.

Ändringen innebär att den tidsbegränsade bestämmelsen i 3 § upphör att gälla vid utgången av september 2019 i stället för vid utgången av 2019. Föreskrifterna i den upphävda 3 § arbetas in i 2 § inhämtningslagen (se författningskommentaren till den paragrafen) och permanentas därmed. Övervägandena finns i avsnitt 6.8.

Sammanfattning av betänkandet Datalagring och integritet (SOU 2015:31)

Vårt uppdrag

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

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

Bakgrund

Skyddet för privatlivet m.m.

I betänkandets bakgrundsavsnitt redogör vi för de regler om skydd för enskildas privatliv som finns i regeringsformen, Europakonventionen och EU:s rättighetsstadga. Där behandlas också vissa bestämmelser om skydd för enskildas personuppgifter. Vidare innehåller bakgrundsavsnittet beskrivningar av de brottsbekämpande myndigheternas verksamhet och de bestämmelser som reglerar dessa myndigheters möjligheter att få tillgång till vissa uppgifter om elektronisk kommunikation som behövs i verksamheten.

Datalagring

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

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

Vilka uppgiftskategorier ska lagras?

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

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

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

Krav på lagring inom EU?

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

Vi har mot den bakgrunden övervägt om det bör införas ett förbud mot att uppgifter som lagras enligt de svenska reglerna förs över till ett s.k.

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

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

Inhämtning av abonnemangsuppgifter

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

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

Vi har mot den bakgrunden övervägt ett flertal olika åtgärder som skulle kunna bidra till att stärka kontrollen över de brottsbekämpande myndigheternas tillämpning av reglerna om inhämtning av abonnemangsuppgifter. Bland annat har vi övervägt om ett tillsynsorgan bör få i uppgift att utöva tillsyn som specifikt tar sikte på tillämpningen av dessa regler. Vi gör dock bedömningen att nackdelarna med en sådan ordning överväger fördelarna. Däremot föreslår vi att beslut om inhämtning av abonnemangsuppgifter ska få fattas endast av vissa särskilt utpekade befattningshavare inom den myndighet som begär uppgifterna. Vidare föreslår vi att beslut om inhämtning av sådana uppgifter ska dokumenteras på visst sätt. Dessa åtgärder bedöms kunna bidra till högre kvalitet i beslutsfattandet och till att den tillsyn som bedrivs av JO, JK, Datainspektionen och SIN blir mer effektiv. Vidare lämnar vi förslag på vissa förtydliganden i bestämmelsen om inhämtning av abonnemangsuppgifter. Syftet är att göra det tydligt att bestämmelsen kan tillämpas i de brottsbekämpande myndigheternas underrättelseverksamhet.

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

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

Inhämtningslagen

Kartläggningen

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

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

Inhämtningslagens beslutsordning

EU-domstolen pekade i datalagringsdomen på att direktivet inte föreskrev att de behöriga nationella myndigheternas tillgång till lagrade uppgifter skulle vara underkastad någon förhandskontroll utförd av en domstol eller oberoende myndighet. Vi har därför, och i enlighet med våra direktiv, övervägt bl.a. om allmän domstol bör anförtros uppgiften att fatta beslut om inhämtning av uppgifter. Emellertid har vi funnit att frågor om inhämtning av uppgifter i underrättelseverksamhet lämpar sig mindre väl för prövning i allmändomstol. I underrättelseverksamheten, som är skild från och ligger i tiden före en förundersökning, är syftet att genom en bred informations- och kunskapsinsamling ge underlag för bearbetning och analys. Utgångspunkten för underrättelseverksamheten är, ofta utifrån en mer övergripande ansats, att studera och kartlägga en befarad brottslig verksamhet för att förebygga eller förhindra att brottsligheten genomförs. Eftersom verksamheten inte som i en förundersökning, är inriktad mot någon specifik brottslig gärning – och ofta inte heller mot någon särskild utpekad person – gör sig partsintresset inte heller gällande på samma sätt i underrättelseverksamheten som under en förundersökning. Integritetsaspekten i underrättelseskedet präglas därför mer av ett medborgarperspektiv än av ett sådant tvåpartsförfarande som lämpar sig för prövning i allmän domstol. Det finns också anledning att vara tveksam till om domstolarna skulle ha möjlighet att tillgodose behovet av snabba beslut.

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

Åtgärder inom ramen för den befintliga beslutsordningen

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

Inom både Polismyndigheten och Tullverket finns numera centralt placerade enheter som har ett övergripande ansvar för att skapa enhetliga riktlinjer för handläggningen av ärenden enligt inhämtningslagen och följa upp hur denna verksamhet hanteras inom respektive myndighet. Vi bedömer att detta med stor sannolikhet kommer att bidra till att höja och garantera kvaliteten i beslutsprocessen hos myndigheterna. Vidare arbetar såväl Polismyndigheten som Tullverket f.n. med att utarbeta nya system för delegation av beslutsbeslutsbefogenhet enligt lagen. Vi anser oss kunna utgå från att myndigheterna i det arbetet kommer att se till att

besluten fattas på en tillräckligt hög nivå för att garantera en beslutsordning som uppfyller höga krav på kompetens och rättssäkerhet.

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

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

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

Enligt inhämtningslagens huvudregel får uppgifter hämtas in, om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år. Enligt en särskild tidsbegränsad bestämmelse får uppgifter hämtas in också om brottslig verksamhet som innefattar vissa brott med lägre straffminimum än fängelse i två år (3 §). De brott som omfattas av bestämmelsen utgör sådan samhällsfarlig brottslighet som bekämpas av Säkerhetspolisen. En del av vårt uppdrag har varit att analysera Säkerhetspolisens behov av en sådan möjlighet och att lämna förslag på hur detta behov bör tillgodoses och balanseras mot integritetsintresset.

Genom vår kartläggning har det kommit fram att tillämpningen av inhämtningslagen har lett till beaktansvärd nytta i samband med underrättelsearbete avseende brottslig verksamhet som innefattar flera av de brott som i dagsläget omfattas av bestämmelsen. Vi bedömer därför att möjligheten att hämta in uppgifter om brottslig verksamhet som innefattar dessa brott bör finnas kvar och att den i fortsättningen bör gälla permanent. Vidare har det kommit fram att Säkerhetspolisen har ett stort behov av att kunna hämta in uppgifter om brottslig verksamhet som innefattar s.k. statsstyrt företagsspioneri samt grov misshandel och olaga frihetsberövande som begås i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd (s.k. systemhotande brottslighet). Vi föreslår därför att möjligheten att hämta in uppgifter ska omfatta även dessa brott.

Betänkandets lagförslag

Förslag till
lag om ändring i rättegångsbalken

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

Nuvarande lydelse	*Föreslagen lydelse*

27 kap.

22 §[1]

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

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

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

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

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2014:1419.

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

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

Nuvarande lydelse	*Föreslagen lydelse*
6 kap.	
22 §[1]	
Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket ska på begäran lämna	
1. uppgift som avses i 20 § första stycket 1 till en myndighet som i ett särskilt fall behöver en sådan uppgift för delgivning enligt delgivningslagen (2010:1932), om myndigheten finner att det kan antas att den som söks för delgivning håller sig undan eller att det annars finns synnerliga skäl,	
2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet,	2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott *eller brottslig verksamhet* till en åklagarmyndighet, Polismyndigheten, Säkerhetspolisen eller någon annan myndighet som ska ingripa mot brottet *eller den brottsliga verksamheten*,
3. uppgift som avses i 20 § första stycket 1 och 3 samt uppgift om i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits till Polismyndigheten, om myndigheten finner att uppgiften behövs i samband med efterforskning av personer som har försvunnit under sådana omständigheter att det kan befaras att det finns fara för deras liv eller allvarlig risk för deras hälsa,	
4. uppgift som avses i 20 § första stycket 1 till Kronofogdemyndigheten om myndigheten behöver uppgiften i exekutiv verksamhet och myndigheten finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende,	
5. uppgift som avses i 20 § första stycket 1 till Skatteverket, om verket finner att uppgiften är av väsentlig betydelse för handläggningen av ett ärende som avser kontroll av skatt eller avgift eller rätt folkbokföringsort enligt folkbokföringslagen (1991:481),	
6. uppgift som avses i 20 § första stycket 1 till Polismyndigheten, om myndigheten finner att uppgiften behövs i samband med underrättelse, efterforskning eller identifiering vid olyckor eller dödsfall eller för att myndigheten ska kunna fullgöra en uppgift som avses i 12 § polislagen (1984:387),	
7. uppgift som avses i 20 § första stycket 1 till Polismyndigheten eller en åklagarmyndighet, om myndigheten finner att uppgiften behövs i ett särskilt fall för att myndigheten ska kunna fullgöra underrättelseskyldighet	

[1] Senaste lydelse 2014:734.

enligt 33 § lagen (1964:167) med särskilda bestämmelser om unga lagöverträdare, och

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

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

Denna lag träder i kraft den 1 juli 2016.

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

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

Nuvarande lydelse	*Föreslagen lydelse*

11 §[1]

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

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

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

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2012:286.

Bilaga 2

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

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

Nuvarande lydelse	*Föreslagen lydelse*

44 kap.

4 §[1]

Rätten enligt 1 kap. 1 § tryckfrihetsförordningen och 1 kap. 1 och 2 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter inskränks av den tystnadsplikt som följer av

1. 2 kap. 14 § första stycket 1 *och* 3 postlagen (2010:1045),	1. 2 kap. 14 § första stycket 1, 3 *och 4* postlagen (2010:1045),

2. 6 kap. 20 § lagen (2003:389) om elektronisk kommunikation, när det är fråga om uppgift om innehållet i ett elektroniskt meddelande eller som annars rör ett särskilt sådant meddelande, och

3. 6 kap. 21 § lagen om elektronisk kommunikation, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, om hemlig avlyssning av elektronisk kommunikation eller hemlig övervakning av elektronisk kommunikation på grund av beslut av domstol, undersökningsledare eller åklagare eller om inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Denna lag träder i kraft den 1 juli 2016.

[1] Senaste lydelse 2012:288.

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

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

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

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

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

Denna lag träder i kraft den 1 juli 2016.

Bilaga 2

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

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

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

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

Nuvarande lydelse	*Föreslagen lydelse*
2 §	
Uppgifter får hämtas in om omständigheterna är sådana att	Uppgifter får hämtas in om omständigheterna är sådana att *åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar*
1. *åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar* brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år, *och*	1. brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år,
2. skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den som åtgärden riktar sig mot eller för något annat motstående intresse.	*2. sabotage enligt 13 kap. 4 § brottsbalken,*
	3. kapning, sjö- eller luftfartssabotage eller flygplats-sabotage enligt 13 kap. 5 a § första eller andra stycket eller 5 b § första stycket brottsbalken, om brottet innefattar sabotage enligt 4 § samma kapitel,
	4. brott mot medborgerlig frihet enligt 18 kap. 5 § brottsbalken,
	5. spioneri, grov obehörig befattning med hemlig uppgift eller grov olovlig underrättelseverksamhet mot Sverige, mot främmande makt eller mot person enligt 19 kap. 5 eller 8 §, 10 § andra stycket, 10 a § andra stycket eller 10 b § andra stycket brottsbalken,
	6. företagsspioneri enligt 3 § *lagen (1990:409) om skydd för*

företagshemligheter, om det finns anledning att anta att den brottsliga verksamheten utövas på uppdrag av eller understödjs av en främmande makt eller av någon som agerar för en främmande makts räkning,

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

8. grov misshandel eller olaga frihetsberövande enligt 3 kap. 6 § eller 4 kap. 2 § första stycket brottsbalken i avsikt att påverka offentliga organ eller den som yrkesmässigt bedriver nyhetsförmedling eller annan journalistik att vidta eller avstå från att vidta en åtgärd eller att hämnas en åtgärd.

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

5 §

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

8 §

Uppteckningar av uppgifter ska granskas snarast möjligt.

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

Uppteckningar ska dock omedelbart förstöras i de delar innehållet avser uppgifter som, på grund av

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

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

---

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

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

Förteckning över remissinstanserna

Remissyttranden över betänkandet Datalagring och integritet (SOU 2015:31) har lämnats av följande instanser. Riksdagens ombudsmän (JO), Göta hovrätt, Stockholms tingsrätt, Malmö tingsrätt, Kammarrätten i Stockholm, Förvaltningsrätten i Umeå, Förvaltningsrätten i Göteborg, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Brottsförebyggande rådet, Datainspektionen, Kustbevakningen, Försvarsmakten, Försvarets radioanstalt, Statens inspektion för försvarsunderrättelseverksamheten, Försvarsunderrättelsedomstolen, Tullverket, Försäkringskassan, Skatteverket, Statskontoret, Post- och telestyrelsen, Lunds universitet (Juridiska fakulteten), Stockholms universitet (Juridiska fakulteten), Göteborgs universitet (Juridiska fakulteten), Kungliga tekniska högskolan (KTH), Blekinge tekniska Högskola, Diskrimineringsombudsmannen (DO), Sveriges advokatsamfund, TULL-KUST, Tidningsutgivarna, Journalistförbundet, Utgivarna, Sveriges psykologförbund, Sveriges läkarförbund, Svenska kyrkan, Sveriges kristna råd, Judiska centralrådet i Sverige, Islamiska förbundet i Sverige, Amnesty international Sverige, Svenska avdelningen av Internationella Juristkommissionen, Civil Rights Defenders, Centrum för rättvisa, Svenska Stadsnätsföreningen, IT&Telekomföretagen, Alltele Privat AB, Bahnhof AB, Com Hem AB, Hi3G Access AB, TDC Sverige AB, Tele2 Sverige AB, Telenor Sverige AB, TeliaSonera Sverige AB, Stiftelsen för internetinfrastruktur, SNUS (Swedish Network Users' Society), Svensk biblioteksförening, Filmproducenternas rättighetsförening, Konstnärliga och Litterära Yrkesutövares Samarbetsnämnd (KLYS), IFPI Sverige, Rättighetsalliansen, Netnod Internet Exchange, Föreningen för Digitala fri- och rättigheter, Institutet för Juridik och Internet (IJI) och Swedish institute of Computer Science (SICS).

Yttrande har också inkommit från Piratpartiet och Ung pirat.

Följande instanser har inbjudits att yttra sig men avstått. Sveriges psykologförbund, Sveriges läkarförbund, Judiska centralrådet i Sverige, Islamiska förbudet i Sverige, Amnesty international Sverige, Svenska avdelningen av Internationella Juristkommissionen, Civil Rights Defenders, Centrum för rättvisa, Alltele Privat AB, Bahnhof AB, TDC Sverige AB, Telenor Sverige AB, Filmproducenternas rättighetsförening, IFPI Sverige och Netnod Internet Exchange.

Sammanfattning av delbetänkandet Datalagring – brottsbekämpning och integritet (SOU 2017:75)

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 brotts-utredande 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 beteendemönster 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 ip-telefoni 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 kammar-rätten 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 data-lagrade 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, Tull-verket 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 domstols-prövning 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 lokaliserings-uppgifter 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 kommunikations-medel 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, tids-uppgifter 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.

Lagringsskyldighetens 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 underrättelse-verksamhet. 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 förut-sättningarna för de brottsbekämpande myndigheternas tillgång till uppgifter om abonnemang.

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.

Delbetänkandets lagförslag

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.

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.

Bilaga 6

Förteckning över remissinstanserna

Remissyttranden över delbetänkandet Datalagring – brottsbekämpning och integritet (SOU 2017:75) har lämnats av följande instanser. Riksdagens ombudsmän (JO), Svea hovrätt, Hovrätten för Övre Norrland, Stockholms tingsrätt, Södertälje tingsrätt, Malmö tingsrätt, Göteborgs tingsrätt, Kammarrätten i Stockholm, Kammarrätten i Göteborg, Förvaltningsrätten i Stockholm, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Polismyndigheten, Säkerhetspolisen, Säkerhets- och integritetsskyddsnämnden, Kriminalvården, Brottsförebyggande rådet, Kustbevakningen, Datainspektionen, Försvarsmakten, Försvarets radioanstalt, Statens inspektion för försvarsunderrättelseverksamheten, Försäkringskassan, Tullverket, Skatteverket, Göteborgs universitet (Juridiska institutionen), Stockholms universitet (Juridiska fakulteten), Umeå universitet (Juridiska institutionen), Örebro universitet (Institutionen för juridik, psykologi och socialt arbete), Kungliga Tekniska högskolan, Post- och telestyrelsen, Diskrimineringsombudsmannen, Sveriges advokatsamfund, Civil Rights Defenders, Dataskydd.net Sverige, Dataspelsbranschen, ECPAT Sverige, Föreningen för Digitala fri- och rättigheter, IFPI Sverige, IT&Telekomföretagen, Rädda Barnen, Rättighetsalliansen, Stiftelsen för Internetinfrastruktur, Svenska stadsnätsföreningen, Svenska Journalistförbundet (SJF), Bahnhof AB, Com Hem AB, Hi3G Access AB, Netnod Internet Exchange i Sverige AB, RISE SICS AB, Tele2 Sverige AB och Telia Sverige AB.

Yttrande har också inkommit från The Business Carrier Coalition (BCC), Sveriges Biografägareförbund (SBF), Colt Technology Services AB, Musikförläggarna, Sveriges Filmuthyrare förening UPA, Film- och TV-branschens Samarbetskommitté (FTVS), Sveriges Videodistributörers förening (SVF) och u9623@protonmail.com.

Följande instanser har inbjudits att yttra sig men avstått. Amnesty International (Svenska sektionen), Centrum för rättvisa, Institutet för Juridik och Internet, NetClean, Svenska avdelningen av Internationella Juristkommissionen, Sveriges läkarförbund, Sveriges psykologförbund, Alltele Privat AB, IP-Only AB, Net at Once Sweden AB, TDC Sverige AB och Telenor Sverige AB.

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, Pohotovost', 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