Till statsrådet och chefen för Justitiedepartementet

Den 29 april 2014 beslutade statsrådet Beatrice Ask att ge förre ordföranden i Högsta förvaltningsdomstolen Sten Heckscher i uppdrag att biträda Justitiedepartementet med att analysera konsekvenserna för svensk rätt av EU-domstolens ogiltigförklaring av datalagringsdirektivet (direktiv 2006/24/EG).

Professorn i folkrätt vid Uppsala universitet, Iain Cameron, förordnades att som expert biträda utredaren i arbetet. Till sekreterare utsågs kanslirådet Karin Walberg och ämnesrådet Mathias Säfsten.

Sten Heckscher har varit ensam utredningsman och svarar ensam för innehållet i promemorian. Iain Cameron har emellertid deltagit i arbetet i sådan utsträckning att det är befogat att använda vi-form i promemorian.

Med denna promemoria redovisas uppdraget såvitt avser analysen av svensk rätt i ljuset av EU-domstolens dom.

Stockholm i juni 2014

Sten Heckscher

/Karin Walberg
Mathias Säfsten

Innehåll

Förkortningar

BrB	brottsbalken (1962:700)
EES	Europeiska ekonomiska samarbetsområdet
EU	Europeiska unionen
FEU	Fördraget om Europeiska unionen
FEUF	Fördraget om Europeiska unionens funktionssätt
JK	Justitiekanslern
LEK	lagen (2003:389) om elektronisk kommunikation
prop.	proposition
PTS	Post- och telestyrelsen
PuL	personuppgiftslagen (1998:204)
RB	rättegångsbalken (1942:740)
RF	regeringsformen (1974:152)
SIN	Säkerhets- och integritetsskyddsnämnden
SOU	Statens offentliga utredningar

1 Sammanfattning

I promemorian analyseras konsekvenserna för svensk rätt av EU-domstolens dom den 8 april 2014 som ogiltigförklarar 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 (datalagringsdirektivet). Analysen omfattar dels den författningsreglering som antagits i anslutning till genomförandet av direktivet genom ändringar i lagen (2003:389) om elektronisk kommunikation och förordningen (2003:396) om elektronisk kommunikation samt de föreskrifter om datasäkerhet som utfärdats av Post- och telestyrelsen, dels gällande bestämmelser om de brottsbekämpande myndigheternas tillgång till och användning av uppgifter som lagrats hos leverantörer av allmänt tillgängliga kommunikationstjänster eller allmänna kommunikationsnät.

Det svenska regelverket om leverantörernas skyldighet att lagra och lämna ut trafik-, lokalierings- och abonnemangsuppgifter till brottsbekämpande myndigheter analyseras i ljuset av EU-domstolens dom med utgångspunkt i frågan om regelverket uppfyller unionsrättens allmänna princip om krav på proportionalitet vid begränsningar av enskildas grundläggande fri- och rättigheter. I analysen övervägs särskilt hur nationella föreskrifter förhåller sig till rätten till respekt för privatlivet och rätten till skydd av personuppgifter när det gäller lagringens omfattning (vilka uppgifter som lagras och hur länge lagringen sker), förutsättningarna för de brottsbekämpande myndigheterna att få tillgång till uppgifter i olika skeden av det brottsförebyggande och brottsutredande arbetet samt kraven på säkerhet och skydd mot obehörig åtkomst vid lagringen.

Vår samlade bedömning är att det svenska regelverket om lagring och utlämnande av uppgifter ryms inom de ramar som ställs upp av unions- och europarättens allmänna principer och kravet på respekt för grundläggande rättigheter. Mot bakgrund av att unionsrätten och europarätten endast ställer upp vissa minimikrav för skydd av privatlivet som måste uppfyllas i den nationella lagstiftningen gör vi trots det bedömningen att det finns skäl att närmare överväga några regelförändringar för att ytterligare stärka skyddet för den personliga integriteten.

Vi har således redan i detta skede av utredningen funnit att det finns skäl att närmare överväga om lagringsskyldighetens omfattning när det gäller vissa uppgiftskategorier bör begränsas i något avseende. Vi har också kommit fram till att det finns skäl att noga överväga om det den externa kontrollen över inhämtning av abonnemangsuppgifter och inhämtning av uppgifter i underrättelseskedet bör stärkas. Det ter sig enligt vår uppfattning också som befogat att ytterligare överväga om det bör ställas krav på att uppgifterna ska lagras inom EU eller EES.

2 Inledning

2.1 Datalagringsdirektivet ogiltigförklarat

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

Domen har väckt starka reaktioner, framför allt i Sverige. Den har bland annat fått till följd att ett antal svenska leverantörer av elektroniska kommunikationstjänster och kommunikationsnät med hänvisning till unionsrätten har upphört att lagra uppgifter som de åläggs enligt den lagstiftning som genomförde datalagringsdirektivet i Sverige. Därmed har de brottsbekämpande myndigheternas tillgång till sådana uppgifter begränsats.

2.2 Uppdraget

Utredarens uppdrag är att i ett första steg, i ljuset av EU-domstolens dom, grundligt analysera reglerna om lagring av uppgifter enligt 6 kap. 16 a–f §§ lagen (2003:389) om elektronisk kommunikation (LEK) samt övriga bestämmelser om tillgång och behandling av sådana uppgifter och deras förhållande till unionsrätten.

I ett nästa steg ska utredaren föreslå de ändringar han finner lämpliga för att stärka skyddet för den personliga integriteten samt, om resultatet av analysen visar på brister i förhållande till unionsrätten, för att leva upp till unionsrättens krav. Denna del av uppdraget ska redovisas senast den 1 oktober 2014.

I den nu aktuella delen av uppdraget – analysen av de ovan angivna reglernas förenlighet med unionsrätten – har utredaren inhämtat särskild sakkunskap om unionsrätten jämte internationell rätt avseende mänskliga rättigheter från professor Iain Cameron vid Uppsala universitet. Utredaren har även haft kontakter med Åklagarmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Tullverket och Post- och telestyrelsen.

Uppdraget (dnr Ju2014/3010/P) återges i sin helhet i en *bilaga* till promemorian.

2.3 Promemorians disposition

Promemorian består av sju avsnitt. I avsnitt 3 redovisas gällande regler om skydd för den personliga integriteten och om uppgiftsskydd och i avsnitt 4 redogörs för datalagringsdirektivet och dess genomförande i svensk rätt. Därefter följer i avsnitt 5 en redogörelse för de brottsbekämpande myndigheternas användning av uppgifter om elektronisk kommunikation. I avsnitt 6 lämnas en närmare beskrivning av EU-domstolens dom och reaktionerna på denna i Sverige och i övriga EU. I avsnitt 7 återfinns analysen av svensk rätts förenlighet med unionsrätten. Analysen följer i stora drag dispositionen av EU-domstolens dom, där de frågor domstolen särskilt belyst avhandlas i samma ordning som i domen, varefter det görs en samlad bedömning av det svenska regelverkets förenlighet med unionsrätten.

3 Integritetsskydd

3.1 Skyddet för privatlivet

Begreppen privatliv och personlig integritet

Rätten till respekt för den personliga integriteten ingår som en del av rätten till respekt för privatlivet enligt artikel 8 i den europeiska konventionen den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen).

Av artikel 8 i Europakonventionen följer att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Begreppet privatliv tolkas i Europadomstolens praxis vitt. Europadomstolen har återkommande framhållit att det inte är möjligt att definiera begreppet genom en uttömmande beskrivning av olika aspekter som rör den enskildes privata förhållanden (se t.ex. *S. och Marper mot Förenade kungariket* [GC], nr 30562/04 och 30566/04, § 66 och *Gillberg mot Sverige* [GC], nr 41723/06, § 66). Begreppet täcker olika aspekter av en enskild individs såväl fysiska som psykiska integritet. Det omfattar bl.a. uppgifter om den enskildes identitet, inklusive namn och kön, uppgifter om hälsa och sexuell läggning och information som rör den personliga utveckningen och relationer till andra individer. Respekten för privatlivet omfattar inte enbart ett skydd av rent privata relationer utan kan även omfatta relationer och aktiviteter som är relaterade till den enskildes yrkesliv (se t.ex. *Rotaru mot Rumänien* [GC], nr 28341/95, § 43). Till privatlivet hör vidare en rätt till skydd mot angrepp av den enskildes ära och ryktbarhet och mot spridning av information som rör privata förhållanden (se t.ex. *K.U. mot Finland*, nr 2872/02, §§ 42 och 43, och *von Hannover mot Tyskland*, nr 59320/00, § 50). Vidare omfattar rätten till respekt för privatlivet ett skydd mot registrering och utlämnande

av uppgifter ur allmänna register (se t.ex. *Leander mot Sverige*, nr 9248/81, § 48 och *Segerstedt-Wiberg m.fl. mot Sverige*, nr 62332/00, § 72).

Någon allmängiltig definition av begreppet personlig integritet har inte slagits fast i svensk lagstiftning. I förarbetena till bl.a. regeringsformen (RF) och personuppgiftslagen (1998:205) har lagstiftaren dock försökt att beskriva kärnan i vad som avses skyddas av lagstiftningen genom att slå fast att kränkningar av den personliga integriteten utgör intrång i den fredade sfär som den enskilde bör vara tillförsäkrad och där ett oönskat intrång bör kunna avvisas (prop. 2005/06:173 s. 15 och prop. 2009/10:80 s. 175). Denna beskrivning ligger också väl i linje med den definition av begreppet som ges i t.ex. Nationalencyklopedins ordbok: rätten att få sin personliga egenart och inre sfär respekterad och att inte utsättas för personligen störande ingrepp.

Det konstitutionella ramverket för skydd av privatlivet

Grundläggande bestämmelser om rätten till skydd för enskildas privatliv och personliga integritet finns främst i regeringsformen, Europakonventionen och Europeiska unionens stadga om de grundläggande rättigheterna av den 7 december 2000, anpassad den 12 december 2007 i Strasbourg (rättighetsstadgan).

Av målsättningsstadgandet i 1 kap. 2 § RF framgår att den offentliga makten ska utövas med respekt för den enskilda människans frihet och värdighet samt att det allmänna ska värna den enskildes privatliv och familjeliv. Vidare följer av 2 kap. 6 § första stycket RF att var och en, gentemot det allmänna, är skyddad mot undersökning av förtroliga brev och andra förtroliga försändelser samt mot hemlig avlyssning eller upptagning av telefonsamtal och andra förtroliga meddelanden. Enligt andra stycket i samma paragraf är var och en även i övrigt skyddad mot betydande intrång i den personliga integriteten som sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden.

Europakonventionen och konventionens samtliga ändrings- och tilläggsprotokoll utom ändringsprotokoll 15 och tilläggsprotokollen 12 och 16 har ratificerats av Sverige.

Konventionen med de ändringar och tillägg som gjorts genom dessa protokoll gäller som svensk lag (lagen [1994:1219] om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna). Artikel 8 om rätt till respekt för privatlivet m.m. gäller således som svensk lag. Av 2 kap. 19 § RF följer att en lag eller annan föreskrift inte får meddelas i strid med Sveriges åtaganden på grund av konventionen. Detta innebär att en föreskrift som står i strid med konventionen i princip också kommer i konflikt med grundlagen.

Efter de ändringar i unionsrätten som gjorts genom Lissabonfördraget följer av artikel 6.1 i fördraget om Europeiska unionen (FEU) att unionen ska erkänna de rättigheter, friheter och principer som fastställs i rättighetsstadgan. Stadgan ska ha samma rättsliga värde som fördragen. En bestämmelse om respekt för privat- och familjelivet finns i artikel 7 i stadgan. Av artikel 8 i stadgan följer vidare bl.a. att var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

Enligt artikel 51.1 i rättighetsstadgan riktar sig denna till medlemsstaterna endast när dessa tillämpar unionsrätten. Av EU-domstolens praxis framgår att detta innebär att de grundläggande rättigheterna i stadgan måste iakttas inte bara vid tillämpning av genomförandelagstiftning utan så snart nationell lagstiftning omfattas av unionsrättens tillämpningsområde (*Åkerberg Fransson*, C-617/10, punkt 21).

Av artikel 6.3 FEU framgår vidare att de grundläggande rättigheterna, såsom de garanteras i Europakonventionen och följer av medlemsstaternas gemensamma konstitutionella traditioner, ska ingå i unionsrätten som allmänna principer.

Inskränkningar i skyddet får göras

Rätten till skydd av privatlivet och den personliga integriteten är inte absolut. Det är möjligt att genom lag meddela föreskrifter som innebär begräsningar av det integritetsskydd som slås fast i regeringsformen (2 kap. 20 § RF). Sådana begränsningar får dock göras endast för ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får inte gå utöver vad som är nödvändigt med hänsyn till de ändamål som föranlett dem och inte heller

sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildningen (2 kap. 21 § RF). Det innebär bl.a. att lagförslag som medför intrång i privatlivet för enskilda måste vara grundade på noggranna behovsanalyser och intresseavvägningar. Finns det utrymme att vidta särskilda åtgärder för att begränsa intrångets intensitet, måste sådana normalt övervägas och om möjligt också vidtas.

På liknande sätt får inskränkningar göras när det gäller rätten till respekt för privat- och familjelivet, hemmet och korrespondensen enligt artikel 8 i Europakonventionen. Dessa rättigheter får begränsas i den nationella rättsordningen för vissa närmare angivna ändamål, bl.a. med hänsyn till intresset av nationell säkerhet och för att förebygga oordning och brott. En begränsning måste ha stöd i nationell lag och vara nödvändig i ett demokratiskt samhälle. Av Europadomstolens praxis följer att en inskränkning måste kunna motiveras av ett angeläget samhälleligt behov (*pressing social need*) och att den måste stå i rimlig proportion till det syfte som ska tillgodose genom inskränkningen. Konventionsparterna har ett visst mått av utrymme – *margin of appreciation* – att skönsmässigt avgöra om en inskränkning är nödvändig. Europadomstolen förbehåller sig dock rätten att övervaka om staternas avvägningar uppfyller konventionens krav på proportionalitet. Europadomstolens kontroll i detta avseende varierar beroende bl.a. på vilka ändamål som utgör grund för en inskränkning och är typiskt sett något mindre ingående när en stats vitala intressen motiverar en inskränkning eller när det saknas en enhetlig europeisk rättsuppfattning om hur en fråga ska bedömas.[1]

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

[1] Harris, David, O'Boyle, Michael and Warbrick, Colin, Law of the European Convention on Human Rights, Oxford University Press 2 uppl. 2009, s. 13, Danelius, Hans, Mänskliga rättigheter i europeisk praxis, Norstedts Juridik 4 uppl. 2012, s. 351 f.

rättigheter. Enligt EU-domstolens fasta praxis kräver proportionalitetsprincipen att unionsinstitutionernas åtgärder, för att vara godtagbara, för det första måste vara ägnade att uppnå de legitima mål som eftersträvas. För det andra får åtgärderna inte gå utöver vad som är lämpligt och nödvändigt för att uppnå de eftersträvade målen.[2] Utrymmet för unionslagstiftaren att bedöma om proportionalitetsprincipens krav är uppfyllda kan begränsas på grund av omständigheter som t.ex. vilken rättighet som begränsas, hur omfattande och allvarligt ingreppet i rättigheten är, vilket syfte ingreppet har etc.[3] Ju mer långtgående ett ingrepp är, desto mer strikt blir EU-domstolens kontroll av att proportionalitetsprincipens krav efterlevs.

I den mån en rättighet som erkänns i rättighetsstadgan motsvarar en rättighet som också garanteras i Europakonventionen ska rättigheten i stadgan ha samma innebörd och räckvidd som i konventionen (artikel 52.3 rättighetsstadgan).

3.2 Skyddet för personuppgifter

EU:s primärrätt

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

[2] Se t.ex. *Volker und Markus Schecke* och *Eifert*, C-92/09 och C-93/09, punkt 74, *Sky Österreich*, C-283/11, punkt 50, och *Schaible*, C-101/12, punkt 29.
[3] Jfr Europadomstolens resonemang i *S. och Marper mot Förenade kungariket* [GC], anmärkt ovan, § 102.

Rätten till skydd för enskilda personer med avseende på behandlingen av personuppgifter kommer till uttryck även i artikel 16 i fördraget om Europeiska unionens funktionssätt (FEUF) där den rättsliga grunden för lagstiftningsåtgärder inom unionsrättens tillämpningsområde slås fast. I artikel 16.2 FEUF slås fast att oberoende myndigheter ska kontrollera att de bestämmelser som Europaparlamentet och rådet antar följs. En särskild rättslig grund för lagstiftning på området för den gemensamma utrikes- och säkerhetspolitiken finns i artikel 39 FEU. Även där slås fast att oberoende myndigheter ska kontrollera att bestämmelserna följs.

Dataskyddsdirektivet

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

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

undantag i nationell rätt. Begränsningar får göras bl.a. om det är nödvändigt med hänsyn till statens säkerhet, allmän säkerhet eller förebyggande, undersökning, avslöjande av brott eller åtal för brott (artikel 13).

När det gäller kraven på säkerhet vid behandlingen av personuppgifter följer av direktivet att registeransvariga ska genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, särskilt om behandlingen innefattar överföring av uppgifter i ett nätverk, och mot varje annat slag av otillåten behandling. Dessa åtgärder ska åstadkomma en lämplig säkerhetsnivå i förhållande till de risker som är förknippade med behandlingen och arten av de uppgifter som ska skyddas (artikel 17.1). Åtgärderna ska väljas med beaktande av såväl de tekniska möjligheter som finns för att åstadkomma en lämplig säkerhetsnivå som de kostnader som är förenade med att genomföra åtgärderna. Om den registeransvarige anlitar en registerförare – någon som utför behandlingen för den registeransvariges räkning – förutsätts att registerföraren kan ge tillräckliga garantier för att nödvändiga organisatoriska och tekniska säkerhetsåtgärder inrättas och följs (artikel 17.2). Några möjligheter att i nationell rätt göra undantag från dessa krav finns inte.

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

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

Varje medlemsstat ska enligt artikel 28.1 i dataskyddsdirektivet utse en eller flera myndigheter som har till uppgift att inom dess territorium övervaka tillämpningen av de bestämmelser som medlemsstaterna antar till följd av direktivet. Dessa myndigheter ska fullständigt oberoende utöva de uppgifter som åläggs dem.

Dataskyddsdirektivet har genomförts i svensk rätt genom framför allt personuppgiftslagen (1998:204), förkortad PuL. Lagen är i första hand tillämplig på personuppgiftsansvariga (registeransvariga) som är etablerade i Sverige (4 §). Det innebär att lagen tillämpas på sådana fysiska eller juridiska personer som ensamma eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter och som har en effektiv och faktisk verksamhet med en stabil struktur i Sverige (se skäl 19 i ingressen till direktivet). Bestämmelser om säkerhet vid behandlingen finns i 31 § PuL. Bestämmelserna i denna paragraf genomför bestämmelserna i artikel 17.1 och 2 i direktivet.

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

Integritetsskydd vid elektronisk kommunikation

Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation) innehåller regler som syftar till

att harmonisera medlemsstaternas bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, i synnerhet rätten till integritet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation. De syftar även till att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom unionen. Direktivets bestämmelser preciserar och kompletterar direktiv 95/46 och är därutöver avsedda även att skydda berättigade intressen för de abonnenter som är juridiska personer (artikel 1).

Bestämmelser om säkerhet vid behandlingen av uppgifter finns i artikel 4 i direktiv 2002/58. Enligt artikel 4.1 ska leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten i sina tjänster, om nödvändigt tillsammans med leverantören av det allmänna kommunikationsnätet när det gäller nätsäkerhet. Dessa åtgärder ska säkerställa en säkerhetsnivå som är anpassad till den risk som föreligger, med beaktande av dagens tillgängliga teknik och kostnaderna för att genomföra åtgärderna. Om det föreligger särskilda risker för brott mot nätsäkerheten, ska leverantören enligt artikel 4.2 informera abonnenterna om sådana risker och, om risken ligger utanför tillämpningsområdet för de åtgärder som tjänsteleverantören ska vidta, om hur de kan avhjälpas, inbegripet en uppgift om de sannolika kostnader som detta kan medföra.

Enligt artikel 5 ska medlemsstaterna genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. I artikel 6 finns bestämmelser om för vilka begränsade ändamål trafikuppgifter får behandlas och krav på begränsningar i fråga om tillgången till uppgifter för dem som behöver det för att utföra vissa närmare angivna arbetsuppgifter. I artikel 15 finns vidare ett stöd för medlemsstaterna att föreskriva undantag från de skyddsregler som finns i bl.a. artiklarna 5 och 6.

Direktivet om integritet och elektronisk kommunikation har genomförts i svensk rätt främst genom bestämmelser som tagits in i lagen om elektronisk kommunikation. Den lagen är tillämplig på elektroniska kommunikationsnät och kommunikationstjänster med tillhörande installationer och tjänster samt annan radioanvändning

men inte på sådant innehåll som överförs i elektroniska kommunikationsnät med hjälp av elektroniska kommunikationstjänster (1 kap. 4 §). Bestämmelser om säkerhet vid tillhandahållande av allmänt tillgänglig elektroniska kommunikationstjänster finns i 6 kap. 3–4 b §§ LEK. Dessa bestämmelser genomför regleringen i artikel 4 i direktivet. Konfidentialiteten enligt artikel 5 i direktivet säkerställs bl.a. genom bestämmelser om förbud mot avlyssning i 6 kap. 17 § LEK och bestämmelser om tystnadsplikt i 20 § samma kapitel. I 20 § föreskrivs således att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till vissa närmare angivna uppgifter som rör ett meddelande inte obehörigen får föra vidare eller utnyttja det han eller hon har fått del av eller tillgång till. Tystnadsplikten omfattar uppgift om abonnemang, innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande. Ett obehörigt röjande eller utnyttjande av sådana uppgifter i strid med denna bestämmelse är straffsanktionerat som brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken.

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

3.3 Allmänna förutsättningar för att använda straffprocessuella tvångsmedel

En åtgärd från det allmännas sida som innebär ett intrång i en persons rättssfär, som sker utan att den enskilde har lämnat sitt samtycke till åtgärden, karaktäriseras som en påtvingat ingrepp – en tvångsåtgärd. Som framgår av avsnitt 3.1 är enskilda enligt 2 kap. 6 § RF skyddade gentemot det allmänna mot olika former av påtvingade ingrepp i den personliga rättssfären, bl.a. sådana ingrepp som innefattar undersökning av den enskildes kropp, kläder, väskor eller bostad, undersökning av förtroliga försändelser och avlyssning av samtal och andra meddelanden, samt även i övrigt mot betydande integritetsintrång i vissa fall. Ett ingrepp i den skyddade sfären får göras bara om det har stöd i lag. Sådana föreskrifter får

meddelas i den utsträckning ett ingrepp kan motiveras av ett ändamål som är godtagbart i ett demokratiskt samhälle. Ingreppet måste vidare begränsas till vad som är nödvändigt för att tillgodose syftet med åtgärden; det måste vara proportionellt. Föreskrifterna får inte strida mot Sveriges åtaganden på grund av Europakonventionen eller vara oförenliga med EU-rätten.

Genom lagar på skilda områden får förvaltningsmyndigheterna stöd för att vidta åtgärder som innefattar olika slags intrång i den enskildes skyddade rättssfär. Det kan t.ex. handla om en rätt för myndigheterna att i sin verksamhet behandla personuppgifter utan den enskildes samtycke, en rätt att få tillgång till uppgifter om enskilda som finns hos en myndighet eller ett privat rättssubjekt eller en rätt att använda olika former av tvångsmedel vid brottsbekämpning.

Föreskrifter om förutsättningar för att använda olika slag av tvångsmedel i den brottsbekämpande verksamheten finns i 24–28 kap. RB, lagen (1991:572) om särskild utlänningskontroll, lagen (2007:978) om hemlig rumsavlyssning, lagen (2007:979) om åtgärder för att förhindra vissa särskilt allvarliga brott, lagen (2008:854) om åtgärder för att utreda vissa samhällsfarliga brott och lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen). Denna reglering ger i första hand stöd för användning av tvångmedel i en förundersökning om brott, dvs. när det av något skäl finns anledning att anta att ett brott som hör under allmänt åtal har förövats (23 kap. 1 § och 16 § RB). Den omfattar användningen av åtgärder som t.ex. beslag och husrannsakan, anhållande och häktning, hemlig avlyssning och hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning och hemlig rumsavlyssning (s.k. buggning) under närmare angivna förutsättningar. Tvångsmedlen används i dessa fall i brottsutredande syfte eller för att en rättegång i brottmål ska kunna genomföras. Regleringen ger emellertid även stöd för att använda tvångsmedel för att förebygga och avslöja brottslig verksamhet, dvs. i underrättelseverksamhet. Detta gäller enligt 1991 års lag om särskild utlänningskontroll, 2008 års lag om åtgärder för att förhindra vissa särskilt allvarliga brott och 2012 års inhämtningslag.

När lagstiftaren har preciserat i vilka fall en viss myndighet ska ha rätt att få tillgång till en viss typ av uppgifter gäller enligt tolkningsprincipen om lex specialis att de begränsningar som följer av denna reglering inte ska kunna kringgås genom att myndigheten väljer att tillämpa t.ex. de allmänna bestämmelserna om husrannsakan och beslag. Regeringen har mot den bakgrunden uttalat att uppgifter som angår ett särskilt elektroniskt meddelande som finns hos en leverantör inte kan inhämtas med stöd av ett editionsföreläggande eller husrannsakan i förening med beslag i fall där annars andra regler för utfående av sådana uppgifter gäller (prop. 2002/03:74 s. 45 f.).

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

4 Genomförandet av datalagringsdirektivet

4.1 Datalagringsdirektivet

Direktivets syfte och tillämpningsområde

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

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

Lagringsskyldighetens omfattning

Artikel 3 i direktivet ålägger medlemsstaterna att anta åtgärder för att säkerställa lagring av sådana uppgifter som specificeras i artikel 5. Lagringsskyldigheten omfattar uppgifter som genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska

kommunikationstjänster eller allmänna kommunikationsnät vid leverans av kommunikationstjänster, i den utsträckning det sker inom statens territorium. Enligt direktivet får inga uppgifter som avslöjar kommunikationens innehåll lagras.

Medlemsstaterna åläggs enligt artikel 6 att säkerställa att uppgifterna lagras under minst sex månader från det datum kommunikationen ägde rum. Uppgifterna får inte lagras längre än två år.

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

Hanteringen av lagrade uppgifter

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

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

Som ett minimum för datasäkerhet ska medlemsstaterna säkerställa att leverantörerna respekterar vissa i artikel 7 angivna principer när det gäller lagrade uppgifter. De lagrade uppgifterna ska vara av samma kvalitet och vara föremål för samma säkerhet och skydd som uppgifterna i nätverket. Lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda uppgifterna mot oavsiktlig eller olaglig förstöring, oavsiktlig förlust, oavsiktlig ändring eller otillåten eller olaglig lagring av, behandling av, tillgång till eller avslöjande av uppgifterna. Lämpliga tekniska och organisatoriska åtgärder ska vidare vidtas för att säkerställa att tillgång till uppgifterna ges endast särskilt bemyndigad personal. Uppgifterna ska förstöras vid slutet av lagringstiden, utom uppgifter för vilka tillgång medgetts och som har bevarats.

För att övervaka tillämpningen av bestämmelserna om säkerhet för de lagrade uppgifterna ska varje medlemsstat utse en eller flera tillsynsmyndigheter (artikel 9).

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

Medlemsstaterna åläggs vidare att införa sanktioner för att beivra otillåten avsiktlig tillgång till eller överföring av lagrade trafikuppgifter (artikel 13). Europarådskonventionen om IT-brottslighet från 2001 (CETS 185) liksom Europarådskonventionen om skydd för enskilda vid automatisk databehandling av personuppgifter från 1981 (CETS 108) ska också

omfatta uppgifter som lagras i enlighet med direktivet om lagring av trafikuppgifter (skäl 20).

4.2 Det svenska genomförandet av direktivet

Genomförandeprocessen

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

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

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

Närmare om den svenska regleringen

Den centrala bestämmelsen avseende lagringsskyldighetens omfattning finns i 6 kap. 16 a § LEK. Lagringsskyldiga är enligt den bestämmelsen de som bedriver anmälningspliktig verksamhet enligt 2 kap. 1 § samma lag. Därigenom omfattas leverantörer av allmänt

tillgängliga kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning och av allmänt tillgängliga elektroniska kommunikationstjänster. Lagringsskyldigheten omfattar uppgifter som anges som nödvändiga för vissa preciserade syften. Dessa är formulerade som uppgifter som är nödvändiga för att kunna spåra och identifiera en kommunikationskälla, slutmålet för kommunikationen, datum, tid och varaktighet för kommunikationen, typ av kommunikation, kommunikationsutrustning samt lokalisering av mobil kommunikationsutrustning. Lagringsskyldigheten omfattar uppgifter som leverantören genererar eller behandlar i sin verksamhet. Det innebär att leverantören inte har någon skyldighet att "skaffa sig" de aktuella uppgifterna. Lagringsskyldigheten är närmare strukturerad i vissa teknikslag. Dessa är angivna som telefoni, meddelandehantering, internetåtkomst och tillhandahållande av kapacitet för att få internetåtkomst (anslutningsform). I 39–43 §§ förordningen om elektronisk kommunikation anges på en mer tekniskt detaljerad nivå vilka uppgifter som ska lagras inom respektive teknikslag.

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

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

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

De uppgifter som har lagrats enligt 6 kap. 16 a § LEK får, enligt 6 kap. 16 c §, lämnas ut till brottsbekämpande myndigheter endast enligt 22 § första stycket 2 i samma kapitel, 27 kap. 19 § RB eller inhämtningslagen. De lagringsskyldiga leverantörerna ska enligt 6 kap. 16 f § LEK bedriva sin verksamhet så att uppgifterna kan lämnas ut utan dröjsmål och så att det inte röjs att uppgifterna

lämnats ut. Uppgifterna ska också göras tillgängliga på ett sådant sätt att informationen enkelt kan tas om hand av de brottsbekämpande myndigheterna.

De kostnader som uppstår vid utlämnande av lagrade trafikuppgifter ska leverantören få ersättning för av den myndighet som begärt ut uppgifterna (6 kap. 16 e § LEK). Övriga kostnader för lagring, säkerhet och anpassning av tekniska system m.m. ska leverantörerna själva stå för.

I lagen om elektronisk kommunikation fanns då direktivet genomfördes redan bestämmelser om teknisk säkerhet för lagrade uppgifter. Dessa bedömdes dock inte vara tillräckliga, utan en ny bestämmelse om skyldighet att vidta särskilda tekniska och organisatoriska åtgärder för att skydda de lagrade uppgifterna vid behandling infördes (6 kap. 3 a § LEK). I bestämmelsen bemyndigas regeringen eller den myndighet regeringen bestämmer att meddela föreskrifter om sådana skyddsåtgärder. Regeringen har meddelat sådana föreskrifter i 37 § förordningen om elektronisk kommunikation. Där framgår att den som är lagringsskyldig ska vidta åtgärder för att säkerställa att de lagrade uppgifterna är av samma kvalitet och föremål för samma säkerhet och skydd som vid den behandling som skett före lagringen. Vidare framgår att åtgärder ska vidtas för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring samt för att förhindra otillåten lagring, behandling av eller tillgång till och otillåtet avslöjande av uppgifterna. Slutligen får uppgifterna göras tillgängliga endast för personal med särskild behörighet. PTS får efter att ha hört Rikspolisstyrelsen och Datainspektionen meddela närmare föreskrifter om de åtgärder som ska vidtas. PTS har meddelat sådana föreskrifter (PTSFS 2012:4), vilka bl.a. närmare reglerar frågor om behörighet och åtkomst till och fysiskt skydd för de lagrade uppgifterna.

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

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

5 Brottsbekämpande myndigheters användning av uppgifter om elektronisk kommunikation

5.1 Nyttan med uppgifter om elektronisk kommunikation i brottsbekämpande verksamhet

Var och en som vistas i riket har rätt att göra anspråk på att staten vidtar effektiva åtgärder till skydd för deras säkerhet. I detta ligger bl.a. att staten måste anstränga sig för att se till att brott förebyggs och utreds och att gärningsmän ställs till svars för sina brottsliga handlingar. En effektiv brottsbekämpning är en förutsättning för att rättstryggheten för enskilda ska kunna upprätthållas. Som framgår av redovisningen i avsnitt 3 är det samtidigt i en rättsstat viktigt att den offentliga maktutövningen är bunden av förutsebara normer och underkastad vissa begräsningar. Staten måste respektera enskildas berättigande krav på skydd mot godtycke och respekt för de grundläggande fri- och rättigheterna.

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.

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

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

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

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

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

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

5.2 Tillgång till uppgifter om elektronisk kommunikation

Som ovan framgått reglerar datalagringsdirektivet inte närmare frågan om de nationella myndigheternas tillgång till de uppgifter som har lagrats enligt direktivet. Tillgångsfrågan reglerades inte heller i det lagstiftningsärende som genomförde datalagringsdirektivet i Sverige. I stället behandlades frågan om de brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation i ett parallellt lagstiftningsärende (prop. 2011/12:55, bet. 2011/12:JuU8, rskr. 2011/12:212).

Utlämnande av uppgifter om elektronisk kommunikation till brottsbekämpande myndigheter i förundersökningar regleras främst i 27 kap. RB. Förutsättningarna för inhämtning av uppgifter enligt denna reglering redovisas mer ingående i avsnitt 7.3.6. Regler om hemlig övervakning av elektronisk kommunikation under förundersökning finns även i 1991 års lag om särskild utlänningskontroll, när det finns misstankar om planläggning av terroristbrott i vissa fall, och i 2008 års lag om åtgärder för att utreda vissa samhällsfarliga brott. Dessa lagar tillämpas uteslutande i Säkerhetspolisens verksamhet.

Polisens och Tullverkets förutsättningar att inhämta uppgifter om elektronisk kommunikation i sin underrättelseverksamhet regleras främst i inhämtningslagen. Förutsättningarna för inhämtning enligt denna reglering redovisas mera ingående i avsnitt 7.3.7. Därutöver finns i 2007 års lag om åtgärder för att förhindra vissa särskilt allvarliga brott vissa regler som möjliggör hemlig övervakning i realtid av elektronisk kommunikation, om det bedöms vara av synnerlig vikt för att förhindra vissa i lagen angivna brott. Beslut enligt 2007 års lag fattas av domstol.

Det finns vidare i 6 kap. 22 § första stycket 2 LEK en särskild reglering avseende brottsbekämpande myndigheters tillgång till s.k. abonnemangsuppgifter. Med detta begrepp avses främst uppgifter om namn, adress, ip-adress, och abonnentnummer (se närmare avsnitt 7.3.5).

6 EU-domstolens dom

6.1 Domen i sammanfattning

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

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

Domstolen slår fast att direktivet innebär ett långtgående och synnerligen allvarligt ingrepp i rätten till privatliv och skyddet av personuppgifter. Domstolen noterar i samband med det bl.a. att lagringen och den senare användningen kan ge berörda personer en känsla av att deras privatliv står under ständig övervakning (punkt 37). Domstolen konstaterar trots det att skyldigheten för leverantörer av allmänt tillgängliga kommunikationstjänster eller

allmänna kommunikationsnät att lagra uppgifter och de nationella myndigheternas tillgång till dessa uppgifter inte kränker det väsentliga innehållet i de skyddade rättigheterna och att datalagringsdirektivets materiella syfte – tillgängliggörandet av uppgifter för bekämpning av allvarlig brottslighet – motsvarar ett mål av allmänt samhällsintresse som erkänns av unionen (punkterna 39–42). Var och en har enligt stadgan rätt inte bara till frihet utan även till personlig säkerhet. Kravet att en inskränkning av en rättighet faktiskt måste svara mot ett allmänt samhällsintresse är därmed enligt EU-domstolen uppfyllt (punkt 44).

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

De förhållanden som domstolen särskilt uppmärksammar vid sin proportionalitetsbedömning är för det första att det i direktivet inte finns några generella begränsningar i lagringsskyldigheten då det i fråga om de uppgifter som ska lagras inte görs någon åtskillnad eller några undantag som tar sin utgångspunkt i syftet att bekämpa brott (punkterna 57–59). Lagringskravet omfattar nästintill all kommunikation – alla personer, alla kommunikationsmedel och alla trafikuppgifter – mellan enskilda i hela Europa. Domstolen konstaterar för det andra att det i direktivet inte anges några objektiva kriterier för att avgränsa de nationella myndigheternas tillgång till och användning av de lagrade uppgifterna för bekämpning av brott som kan anses vara av

tillräckligt allvarligt slag för att motivera det aktuella ingreppet. Det lämnas i stället till medlemsstaterna att själva bestämma vad som utgör allvarlig brottslighet i detta sammanhang (punkt 60). Inte heller regleras i direktivet vilka formella och materiella villkor som ska gälla och vilka krav som ska ställas på förfarandet för tillgång till uppgifterna. Domstolen noterar särskilt att tillgången till uppgifter inte är underkastad någon förhandskontroll av en domstol eller oberoende myndighet som har till uppgift är att se till att tillgången begränsas till vad som är strikt nödvändigt (punkterna 61 och 62). Domstolen pekar vidare på att direktivet inte innehåller några bestämmelser som innebär att en åtskillnad ska göras i fråga om lagringstiden för olika slags trafikuppgifter utifrån den nytta dessa har för att tillgodose syftet med lagringen och att det inte heller föreskrivs att lagringstiden måste bestämmas utifrån objektiva kriterier för att säkerställa att den inte går utöver vad som är strikt nödvändigt (punkterna 63 och 64). Slutligen uppmärksammar domstolen att det i direktivet saknas specifika regler om skydd av och säkerhet för lagrade personuppgifter som anpassar kraven till såväl mängden och arten av uppgifter som riskerna för otillåten tillgång till dessa. Domstolen menar i detta sammanhang att det inte finns några garantier för att leverantörerna inte tar ekonomiska hänsyn när de bestämmer säkerhetsnivån eller för att uppgifterna förstörs när lagringstiden har gått ut. Domstolen pekar också på att kravet på en oberoende tillsyn inte kan garanteras om uppgifterna lagras utanför EU (punkterna 66–68).

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

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

verkan medlemsstaternas unionsrättsliga skyldighet att lojalt genomföra unionsrättsakten.

6.2 Reaktioner på domen

Reaktioner i Sverige

I nära anslutning till att domen offentliggjordes meddelade flera leverantörer av elektroniska kommunikationstjänster och kommunikationsnät i Sverige att de gjorde bedömningen att den svenska lagstiftning som genomför direktivet står i strid med EU-rätten och att de därför avsåg att upphöra med lagringen av uppgifter enligt 6 kap. 16 a § LEK. Några av dem gick också ut med information om att lagrade uppgifter skulle komma att raderas. Ett par leverantörer begärde i anslutning till domen även besked från PTS om vilken bedömning myndigheten gjorde av domen. En leverantör har även begärt besked från regeringen om lagstiftningen kommer att rivas upp.

PTS informerade på sin hemsida på internet kort tid efter att domen hade meddelats att myndigheten ”i nuläget inte [kommer] att vidta några åtgärder utifrån datalagringsreglerna”. Rikspolisstyrelsen har i två skrivelser till PTS, den 15 april och den 23 maj 2014, påtalat att en utpekad leverantör agerar i strid med bestämmelserna i lagen om elektronisk kommunikation genom att inte lagra och tillhandahålla uppgifter för brottsbekämpande ändamål. PTS har i anledning därav den 30 maj 2014 begärt upplysningar från den aktuella leverantören. Några övriga tillsynsåtgärder har inte vidtagits.

Miljöpartiet har i en motion (2013/14:MP100), som gavs in efter att EU-domstolens dom hade meddelats, begärt att den lagstiftning som genomför datalagringsdirektivet ska upphävas (riksdagens snabbprotokoll 2013/14:105 den 29 april 2014). Till stöd för att motionen skulle hänvisas till utskott för vidare behandling åberopades bestämmelserna i 3 kap. 13 § riksdagsordningen av vilka följer att motioner med anledning av en händelse av större vikt får väckas av minst tio ledamöter om händelsen inte kunnat förutses eller beaktas under den allmänna motionstiden eller någon annan motionstid. Talmannen fann dock att EU-domstolens ogiltigförklarande av datalagringsdirektivet inte

utgjorde någon sådan oförutsedd händelse av större vikt som medger motionsrätt. Motionen lades därför till handlingarna utan vidare åtgärd.

Reaktioner i andra medlemsstater

Vi har trots den knappa tid som stått till buds försökt få en bild av reaktionerna i andra medlemsstater. Justitiedepartementet skickade efter EU-domstolens dom ut en beställning till ambassaderna i övriga medlemsstater med en förfrågan om vilka reaktioner domen har väckt där (dnr Ju2014/3819/EU). De svar som hittills har kommit in visar sammanfattningsvis att domen generellt inte har väckt lika stor uppmärksamhet i andra länder som den har i Sverige. Av den information som vi tagit del av synes den slutsatsen kunna dras att man inte i något annat land har satt i fråga den nationella lagstiftning varigenom det nu upphävda direktivet genomförts. Ett antal stater har aviserat att en analys av rättsläget måste göras. I Norge pågår exempelvis för närvarande ett analysarbete, som enligt uppgift från det norska Justitiedepartementet förväntas kunna presenteras inom kort. I Österrike har författningsdomstolen getts i uppdrag att utreda vilka effekter EU-domstolens beslut har för österrikisk lagstiftning. Resultatet ska presenteras i höst. Det danska Justitieministeriet presenterade den 2 juni 2014 en analys av domens effekter för dansk rätt. Det danska Justitieministeriet drar slutsatsen att de danska reglerna om datalagring inte står i strid med unionsrätten.[4]

I Slovakien fattade landets författningsdomstol den 24 april 2014 ett beslut som innebär att de slovakiska reglerna om lagring av trafikuppgifter inte längre får tillämpas. Det granskningsärende som låg till grund för bedömningen hade dock påbörjats redan 2012 och var således inte en följd av EU-domstolens dom. Det kan i detta sammanhang också anmärkas att författningsdomstolarna i Tyskland, Tjeckien och Rumänien i tidigare avgöranden har underkänt nationella genomförandebestämmelser till datalagringsdirektivet. Dessa domstolar har dock inte ifrågasatt lagringskravet i direktivet som sådant utan snarare kvaliteten på de

[4] http://justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning

nationella bestämmelserna. Av dessa länder är det endast Tyskland som ännu inte ändrat lagstiftningen i linje med författningsdomstolens avgörande.

Det har inte kommit till utredningens kännedom att någon av de leverantörer som har upphört att lagra uppgifter i Sverige med hänvisning till att lagringen inte är förenlig med unionsrätten och som bedriver verksamhet även i andra medlemsstater har gjort motsvarande bedömning och slutat lagra uppgifter i någon annan medlemsstat.

Reaktioner från EU:s institutioner

EU-kommissionären med ansvar för inrikes frågor Cecilia Malmström har i en kommentar till EU-domstolens dom uttalat att kommissionen kommer att utvärdera domen noggrant. Detta kommer att ske med beaktande av de framsteg som görs med anledning av den revision av direktiv 2002/58 som kan bli aktuell och i ljuset av det pågående arbetet med utformningen av en ny dataskyddsreglering i EU (KOM [2012] 9–11 slutlig). Kommissionen har aviserats att resultatet av denna översyn kan dröja.

Europaparlamentets rättstjänst har i sin rättsliga analys av EU-domstolens avgörande konstaterat bl.a. att domen inte per automatik medför att nationella bestämmelser som genomför direktivet blir ogiltiga trots att ogiltigförklaringen av direktivet får retroaktiv effekt. Rättstjänsten har tvärtom betonat att medlemsstaterna har kvar sin autonoma befogenhet att antingen bevara, ändra eller upphäva de föreskrifter som har antagits för att genomföra direktivet och att det är upp till nationella domstolar att bedöma om de föreskrifter som behålls respekterar de grundläggande rättigheterna.

Rådets sekretariat har den 5 maj 2014 sammanfattat domen och informerat om hur man ser på dess konsekvenser för rådets framtida arbete.[5] Rådet konstaterar att domen kommer att få mycket stor betydelse för unionens fortsatta arbete i fråga om rätten till privatliv och dataskydd och att det åligger kommissionen

[5] Dok. 9009/14, JUR 249, DAPIX 58, TELECOM 106, COPEN 124.

att nu ta initiativ för att se till att såväl redan existerande som kommande rättsakter avseende dataskydd är i linje med domen.

6.3 Tillgången till uppgifter och kostnaderna för dessa har påverkats

Ett antal leverantörer har alltså i Sverige gjort bedömningen att de svenska reglerna som genomför datalagringsdirektivet står i strid med unionsrätten. De hanterar därför trafikuppgifter och andra uppgifter som rör ett särskilt elektroniskt meddelande med utgångspunkt i det rättsläge som rådde i Sverige före maj 2012, dvs. innan ändringarna i 6 kap. LEK genomfördes med anledning av direktivet. Mot den bakgrunden har vissa leverantörer framhållit att de inte längre anser sig ha rätt att spara uppgifter i vidare utsträckning än vad som behövs för bl.a. abonnentfakturering, betalning av samtrafikavgifter och nätövervakning. Några leverantörer har också ansett sig vara rättsligt förpliktade att radera tidigare lagrade uppgifter som inte fortsättningsvis får sparas för dessa ändamål.

Utvecklingen har inneburit att flera leverantörer på marknaden för allmänna elektroniska kommunikationstjänster och allmänna kommunikationsnät i varierande omfattning levererar trafikuppgifter till de brottsbekämpande myndigheterna enligt de regler i lagen om elektronisk kommunikation som gällde innan datalagringsdirektivet genomfördes, om uppgifterna finns tillgängliga hos leverantören i deras faktureringssystem eller andra system som uppgifterna bevaras i med syftet att förhindra och avslöja obehörig användning av kommunikationsnät och kommunikationstjänster. De brottsbekämpande myndigheternas möjligheter att få tillgång till framför allt uppgifter om inkommande samtal eller positionering av mobil telefoniutrustning har därigenom i påtaglig grad kommit att begränsas i förhållande till vad som var fallet före EU-domstolens dom.

Många leverantörer har vidare vägrat att tillämpa de föreskrifter om avgifter som PTS med stöd av 46 § förordningen om elektronisk kommunikation beslutat ska gälla från och med den 1 januari 2014 (PTSFS 2013:5). Leverantörerna har återgått till att tillämpa de grunder för beräkning av kostnaderna för utlämnande

som tidigare gällde enligt sedvänja och avtal (PTS rapport den 1 december 2013, PTS-ER-2013:24). Detta har inneburit att kostnaderna för de brottsbekämpande myndigheternas inhämtning av trafikuppgifter ökat markant i jämförelse med de första månaderna under 2014.

7 Analys

7.1 Analysens utgångspunkter

Vårt uppdrag är att, i ljuset av EU-domstolens dom, i ett första steg grundligt analysera reglerna om lagring av uppgifter enligt 6 kap. 16 a–f §§ LEK samt övriga bestämmelser om tillgång och behandling av sådana uppgifter och bestämmelsernas förhållande till unionsrätten. Med andra ord går uppdraget i denna del ut på att pröva de utpekade svenska reglerna mot unionsrätten, med beaktande av det ytterligare instrument för tolkning av unionsrätten som EU-domstolens dom innebär.

I domen har EU-domstolen ogiltigförklarat datalagringsdirektivet efter en proportionalitetsprövning. I utredningsuppdraget anges att EU-domstolens ställningstagande inte med automatik innebär att nationell reglering som genomför direktivet strider mot unionsrättens krav på proportionalitet. En liknande syn har presenterats av Europaparlamentets rättstjänst. Den synes också delas av övriga medlemsstater som har genomfört datalagringsdirektivet. Vår utgångspunkt är således att enbart det faktum att EU-domstolen har funnit datalagringsdirektivet ogiltigt inte medför att svenska regler också är ogiltiga.[6]

Sedan datalagringsdirektivet upphävts har medlemsstaterna i princip samma behörighet att besluta om nationell lagstiftning rörande lagring, tillgång och behandling av trafikuppgifter som innan direktivet antogs. EU-domstolen har i sin dom konstaterat att skyldigheten att lagra trafikuppgifter för brottsbekämpande ändamål i och för sig motsvarar ett mål av allmänt samhällsintresse som erkänns av unionen. Frågan om lagring av trafikuppgifter

[6] Se även Asp, Petter, The Substantive Criminal Law Competence of the EU, Stockholm: Juridiska fakultetens skriftserie nr 79, Jure 2013, s. 222–224.

reglerades innan datalagringsdirektivet unionsrättsligt i direktiv 2002/58/EG om integritet och elektronisk kommunikation. Utgångspunkten enligt detta direktiv är att trafikuppgifter ska utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra kommunikationen. Vissa undantag från kravet tillåts dock. Bl.a. får uppgifter behållas för fakturering och – efter samtycke – för marknadsföringsändamål. Vidare tillåts medlemsstaterna enligt artikel 15.1 i direktiv 2002/58 att begränsa ovan nämnda krav på utplåning eller avidentifiering av trafikuppgifter och vidta nationella lagstiftningsåtgärder som innebär att trafikuppgifter får bevaras under en begränsad period, om det motiveras av de skäl som närmare anges i artikeln. Dessa skäl är angivna så att åtgärden ska vara 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. Alla åtgärder som vidtas ska vara i enlighet med de allmänna principerna i gemenskapslagstiftningen, inklusive principerna i artikel 6.1 och 6.2 FEU.[7] Sammanfattningsvis finns därmed, när datalagringsdirektivet nu upphävts, inte längre någon unionsrättslig *skyldighet* att lagra trafikuppgifter, men sådana uppgifter *får*, såvitt ankommer på EU-rätten, lagras om kraven i direktiv 2002/58 är uppfyllda och det inte heller i övrigt strider mot unionsrätten.

I utredningsuppdraget anges vidare att bedömningen av om rättighetsstadgans krav är uppfyllda i samband med att nationell lagstiftning antas inom ramen för unionsrättens tillämpningsområde förutsätter en samlad bedömning av den svenska lagstiftningen som helhet. Vidare anges att, eftersom rättighetsstadgans bestämmelser ska ha samma innebörd som Europakonventionens motsvarande bestämmelser, utgångspunkten vid bedömningen av gränserna för medlemsstaternas nationella beslutanderätt på unionsrättens tillämpningsområde måste tas i praxis från såväl EU-domstolen som Europadomstolen för mänskliga rättigheter. De EU- och europarättsliga ramar inom vilka vi rör oss har redovisats ovan.

[7] Efter Lissabonfördragets ikraftträdande kommer dessa principer i allt väsentligt till uttryck i artiklarna 2 och 6.3 FEU.

EU-domstolen prövar i sin dom ett antal omständigheter kopplade till frågan om proportionalitet, varefter direktivets reglering vid en samlad bedömning bedöms oproportionerlig. Inledningsvis slår domstolen fast vissa utgångspunkter för prövningen, vilka på motsvarande sätt bör vara utgångspunkter även i den analys som vi ska göra. Domstolen konstaterar att de uppgifter som ska lagras enligt direktivet sammantaget leder till att ingående slutsatser kan dras avseende de personer lagringen omfattar. Intrånget i den personliga integriteten är därför stort, oavsett det faktum att innehållet i en kommunikation inte lagras.[8] Domstolen konstaterar dock att lagringen av trafikuppgifter är ägnad att uppnå det eftersträvade målet, eftersom det är värdefullt i den brottsbekämpande verksamheten att få tillgång till uppgifter av det aktuella slaget. För att lagringen också ska vara en proportionerlig åtgärd för att bekämpa brott slår domstolen fast att inskränkningen av de grundläggande friheterna måste begränsas till vad som är *strikt nödvändigt*. Av detta följer enligt domstolen att unionslagstiftningen måste föreskriva tydliga och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden och som slår fast minimikrav för att möjliggöra ett effektivt skydd mot riskerna för missbruk och otillåten tillgång och användning av enskildas personuppgifter. Därmed måste samma krav ställas på nationella bestämmelser.

EU-domstolen uppmärksammar vidare i sin proportionalitetsbedömning ett antal specifika frågor. Vår närmare analys kommer att följa domens upplägg. Det bör dock poängteras att EU-domstolen i sin dom gör en samlad bedömning av alla de behandlade frågorna. Domen kan inte tolkas så att domstolen har presenterat en lista som i alla delar måste vara uppfylld för att regleringen inte ska anses oproportionerlig. På samma sätt kommer de aspekter domstolen har prövat mot direktivet i vår analys i tur och ordning att prövas mot svensk rätt, men det är först vid den avslutande sammantagna bedömningen som svensk rätts förenlighet med unionsrätten fullt ut kan avgöras.

[8] Se vidare om denna fråga även Opsahl, Kurt, Why Metadata Matters, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2013/06/why-metadata-matters, och Naarttijärvi, Markus, För din och andras säkerhet, Umeå: Juridiska institutionens skriftserie nr 29, Iustus 2013, s. 270.

I avsnitt 7.2 analyseras inledningsvis lagringsskyldighetens omfattning. Avsnitt 7.3 ägnas åt en analys av villkoren för de brottsbekämpande myndigheternas tillgång till lagrade uppgifter om elektronisk kommunikation. I avsnitt 7.4 görs därefter en analys av frågan om lagringstidens omfattning. Kraven på säkerhet vid lagring analyseras ur olika perspektiv i avsnitt 7.5. Slutligen görs en samlad bedömning i avsnitt 7.6.

7.2 Lagringsskyldighetens omfattning

7.2.1 Direktivet och EU-domstolens dom

Artikel 3 i det ogiltigförklarade direktivet ålägger medlemsstaterna att anta åtgärder för att säkerställa lagring av sådana trafikuppgifter som specificeras i artikel 5. Lagringsskyldigheten omfattar uppgifter som genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät vid leverans av kommunikationstjänster i den utsträckning det sker inom statens territorium. Däremot ställs inte upp något krav på lagring av uppgifter om samtal som inte kopplats fram. Under vissa förutsättningar omfattas misslyckade uppringningsförsök som enligt artikel 2.2f definieras som en kommunikation då ett telefonsamtal kopplats men inget svar erhållits eller när det skett ett ingrepp i driften av kommunikationsnätet.

Uppgifter som avslöjar kommunikationens innehåll får enligt direktivet inte lagras. Av skäl 13 i ingressen framgår att lagringen också bör ske på ett sådant sätt att man undviker att uppgifter lagras mer än en gång.

Artikel 5 är uppdelad utifrån olika ändamål för vilka uppgifterna ska lagras. I anslutning till respektive ändamål anges i detalj de kategorier av trafikuppgifter som ska lagras för respektive kommunikationssätt.

Uppgifter som är nödvändiga för att *spåra och identifiera en kommunikationskälla* (punkten 1a) omfattar, beträffande fast och mobil telefoni, det uppringande telefonnumret och abonnentens eller den registrerade användarens namn och adress. När det gäller internetåtkomst, internetbaserad e-post och internettelefoni omfattas uppgift om tilldelad användar-id (som är en unikt id som

tilldelas den som abonnerar på eller registrerar sig på en internetåtkomsttjänst eller en internetkommunikationstjänst, artikel 2.2d). Användar-id och telefonnummer som tilldelats kommunikationen i det allmänna telenätet liksom namn på och adress till den abonnent eller registrerade användare som ip-adressen, användar-id eller telefonnumret tilldelades vid tidpunkten för kommunikationen omfattas också av lagringsskyldigheten.

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

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

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

För att *identifiera användarnas kommunikationsutrustning* (punkten 1e) ska lagring ske av det uppringande och det uppringda telefonnumret vid fast och mobil telefoni. När det gäller mobiltelefoni ska lagringen därutöver omfatta den uppringande respektive den uppringda partens IMSI (International Mobile Subscriber Identity) och IMEI (International Mobile Equipment Identity) samt, vid förbetalda anonyma tjänster, datum och tid för den första aktiveringen av tjänsten och den lokaliseringsbeteckning (cell-id) från vilken tjänsten aktiverades. Lokaliseringsbeteckningen definieras i direktivet som identiteten hos den cell från vilken ett mobiltelefonsamtal påbörjades eller avslutades (artikel 2.2e). Varje basstation i kommunikationsnätet har nämligen en beteckning som är unik för stationen, ett cell-id. När

det gäller internetåtkomst, internetbaserad e-post och internet-telefoni gäller lagringen uppringande telefonnummer och DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare.

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

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

7.2.2 Den svenska regleringen

Som ovan redovisats regleras lagringsskyldighetens omfattning i svensk rätt i 6 kap. 16 a § LEK samt i 39–43 §§ förordningen om elektronisk kommunikation. Dessa bestämmelser omfattar samtliga de uppgiftskategorier som anges i artikel 5 i datalagringsdirektivet, men de är i viss mån annorlunda strukturerade och definierade. Skälet till detta angavs vid genomförandet främst vara att få till

stånd en tydlig och teknikneutral reglering (prop. 2010/11:46 s. 27). Vid genomförande av direktivet beslutades även att lagringsskyldigheten på två punkter skulle gå utöver den lagringsskyldighet som direktivet krävde. Leverantörerna ålades därmed att lagra även uppgifter om misslyckad uppringning och uppgifter om lokalisering av mobilsamtals slut. I motiven anfördes att dessa uppgifter var av stort värde för de brottsbekämpande myndigheterna och att det, även med beaktande av integritets-, kostnads- och konkurrensaspekter, bedömdes att en sådan lagringsskyldighet var proportionerlig i förhållande till ändamålet att beivra brott (prop. 2010/11:46 s. 31 f.). En prövning gjordes alltså i dessa delar mot artikel 15.1 i direktiv 2002/58. Ett lagringskrav som omfattade även lokaliseringsuppgifter beträffande pågående kommunikation, något som vissa brottsbekämpande myndigheter hade anfört att det fanns ett behov av, ansågs däremot inte proportionerligt och infördes därför inte (prop. 2010/11:46 s. 35).

7.2.3 Analys

Är lagringsskyldighetens omfattning lämplig och proportionerlig?

Som ovan konstaterats gäller, när datalagringsdirektivet nu har förklarats ogiltigt, att nationella lagringsreglers förenlighet med unionsrätten i första hand måste prövas mot artikel 15.1 i direktiv 2002/58. Det följde tidigare av artikel 11 i datalagringsdirektivet att artikel 15.1 i direktiv 2002/58 inte skulle tillämpas på de uppgifter som specifikt måste lagras enligt datalagringsdirektivets bestämmelser. I det lagstiftningsärende som behandlade genomförandet av datalagringsdirektivet gjordes en sådan prövning i förhållande till artikel 15.1 följaktligen endast beträffande de uppgiftskategorier som skulle lagras utan att det fanns ett krav i datalagringsdirektivet. Nu måste emellertid prövas om lagringen av alla de aktuella trafikuppgifterna kan anses vara en lämplig och proportionerlig åtgärd för att skydda allmän säkerhet och/eller för att förebygga, undersöka, avslöja och lagföra brott. Lagringen måste naturligtvis även i övrigt vara förenlig med de allmänna principerna i unionslagstiftningen för att vara tillåten. En åtgärd kan anses lämplig endast om den objektivt sett är ägnad att uppnå

det eftersträvade målet med åtgärden och den kan anses proportionerlig bara om åtgärden avgränsas på sådant sätt att integritetsintrånget inte blir större än vad som är strikt nödvändigt för att uppnå det efterstävade målet.

Först och främst måste alltså bedömas om en lagring av de uppgifter som omfattas av det ovan beskrivna svenska regelverket är en åtgärd som är ägnad att uppnå syftet med lagringen. Som ovan redovisats har i flera sammanhang tidigare konstaterats att uppgifter om elektronisk kommunikation är av stort värde för att kunna upptäcka och utreda brott, inte minst vad gäller grov och organiserad brottslighet. För viss typ av internetrelaterad brottslighet, såsom exempelvis barnpornografibrott, är trafikuppgifter också av avgörande betydelse för att kunna identifiera en misstänkt gärningsman.

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

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

Vid en prövning av om lagringen dessutom kan anses proportionerlig, dvs. att lagringen vid en avvägning mellan motstående intressen inte sträcker sig längre än vad som är strikt nödvändigt för att uppnå det efterstävade målet, kan inledningsvis konstateras att vissa frågetecken kan ställas upp såvitt avser lagringen av de få uppgifter som Polisen har angett som mindre viktiga eller bra att ha i vissa fall. Denna fråga kommer att övervägas närmare i det fortsatta arbetet. Att lagringen av övriga slag av uppgifter, utifrån ett behovsperspektiv, är proportionerlig verkar dock stå klart av de uppgifter vi kunnat få del av.

I proportionalitetsprövningen måste dock beaktas även de aspekter som EU-domstolen särskilt lyfter fram i sin dom. Domstolens resonemang kan i denna del sammanfattningsvis sägas gå ut på att det kan ifrågasättas om en lagring av trafikuppgifter som omfattar samtliga personer och samtliga elektroniska kommunikationsslag är en proportionerlig åtgärd, trots att de uppgifter som lagras i de allra flesta fallen inte har någon som helst koppling till brottslig verksamhet av allvarligt slag eller kan förväntas komma att användas vid utredande och lagföring av brott.

Det råder ingen tvekan om att lagringen av trafikuppgifter hade utgjort ett betydligt mindre allvarligt intrång i de av domstolen utpekade grundläggande rättigheterna om den skulle vara begränsad till att omfatta bara trafikuppgifter som har en konstaterad koppling till brottslig verksamhet. Lagrings-skyldigheten skulle då uppkomma först sedan någon form av misstanke riktats mot en viss person. Någon annan rimlig väg att på förhand begränsa lagringens omfattning till att omfatta endast uppgifter med koppling till brottslig verksamhet är svår att se. Det kan dock omedelbart konstateras att en sådan begränsning inte kan göras utan att en mängd uppgifter som är av stor vikt för brottsbekämpningen försvinner. Inga historiska trafikuppgifter från tiden före ett brott begåtts och inga av de uppgifter som i dag

inhämtas i polisens underrättelseverksamhet för att förebygga, förhindra eller upptäcka allvarlig brottslighet skulle då med säkerhet finnas att tillgå. De skulle i stället finnas tillgängliga endast om och under den tid leverantörerna sparar uppgifterna för egna ändamål, t.ex. fakturering. Metoden förutsätter kort sagt att alla uppgifter lagras, bl.a. eftersom det inte är möjligt att i förväg veta eller misstänka vilka uppgifter som kan vara viktiga. Urvalet av vilka uppgifter som ska användas kan ske först senare vilket innebär att sållningen av uppgifter sker då.

Det EU-domstolen i denna del sätter fingret på kan sägas utgöra själva grundtanken med lagringen av trafikuppgifter enligt datalagringsdirektivet, nämligen att säkerställa att uppgifterna finns tillgängliga för det fall de skulle behövas för att bekämpa allvarliga brott. Man bör ha i åtanke att förhandlingarna som ledde fram till datalagringsdirektivet inleddes efter bombattentaten i Madrid den 11 mars 2004, där det hade kommit fram att det faktum att historiska trafikuppgifter inte lagrades i alla medlemsstater utgjorde ett problem vid utredningen av attentaten. Som vi ser det kan EU-domstolens dom inte tolkas så att denna grundtanke, sedd för sig, har underkänts av domstolen, utan det är den omfattande lagringen *kombinerat med* i första hand bristen på regler som begränsar tillgången till uppgifterna som gör lagringen oproportionerlig. Även den stora mängden lagrade uppgifter kombinerat med, som domstolen konstaterar, bristfälliga skyddsregler leder till slutsatsen att direktivet innebär ett oproportionerligt intrång. Detta följer av att domstolen, som ovan redovisats, gör en *samlad bedömning* vid vilken direktivet ogiltigförklaras.

Den svenska lagstiftningen är konstruerad så att lagringen av trafikuppgifter är generell, på det sätt som följer av datalagringsdirektivet, medan de brottsbekämpande myndigheternas tillgång till de lagrade uppgifterna är begränsad genom ett antal regler. I motiven anges att de avgränsningar som krävs med hänsyn till integritetsskyddet till betydande del avgörs av de bestämmelser som reglerar förutsättningarna för tillgång till lagrade trafikuppgifter (prop. 2010/11:46 s. 21). Begränsningarna som har bedömts som nödvändiga för att skydda den personliga integriteten har med andra ord i huvudsak inte skett genom att begränsa vilka uppgifter som lagras utan genom att tillgången till

uppgifterna begränsats genom regler om vilka brottsbekämpande myndigheter som kan få tillgång till uppgifterna och under vilka förutsättningar det kan ske. Det är också vår mening att EU-domstolens dom ska tolkas så att om förutsättningarna för myndigheterna att få tillgång till lagrade uppgifter kan anses tillräckligt stramt reglerade så utgör enbart det faktum att lagringen sker utan koppling till på förhand konstaterad brottslig verksamhet inte i sig att lagringen är oproportionerlig, sedan denna åtgärd väl har konstaterats vara lämplig för att uppnå syftet med lagringen. Som vi ser det är utformningen av de svenska tillgångsreglerna således av avgörande betydelse även för bedömningen av frågan om lagringens omfattning kan anses proportionerlig. Även skyddet för den merpart av alla uppgifter som lagras men aldrig begärs utlämnade måste också konstateras vara tillräckligt högt. Dessa båda frågor behandlas närmare i efterföljande avsnitt.

Särskilt om uppgifter som omfattas av yrkesmässig tystnadsplikt

Domstolen lyfter i sin dom fram att ingen begränsning finns i direktivet som möjliggör att kommunikation med personer som enligt nationell lag omfattas av yrkesmässig tystnadsplikt undantas från lagringskravet. Här kan konstateras att svenska regler om undantag från vittnesplikt för exempelvis advokater och läkare omfattar uppgifter som anförtrotts dessa i sin yrkesutövning. Vidare kan noteras att regeringen nyligen föreslagit att reglerna om avlyssningsförbud vid hemlig avlyssning av elektronisk kommunikation i 27 kap. 22 § RB ska utökas från att avse endast kommunikation med försvarare till att omfatta alla de yrkeskategorier som undantas från vittnesplikt i 36 kap. 5 § andra–sjätte styckena RB (prop. 2013/14:237 s. 131 f.). Att något motsvarande förbud skulle införas även för uppgifter som inhämtas genom hemlig övervakning av elektronisk kommunikation, alltså s.k. metadata som visar att en kommunikation har ägt rum men inte vad den innehöll, har dock aldrig varit aktuellt. Med det synsätt som således kommer till uttryck i svensk lagstiftning – att det är uppgiftens innehåll som avgör om den omfattas av yrkesmässig tystnadsplikt – måste det också anses långsökt med en modell där exempelvis vissa telefonnummer på förhand skulle

undantas från ett lagringskrav som i övrigt gäller generellt. Även om uppgifter som kommer fram i t.ex. en advokats eller läkares kommunikation i vissa situationer omfattas av tystnadsplikt och undantag från vittnesplikt, så gör inte det faktum att kommunikationen har ägt rum det. Även om det i fråga om viss slags kommunikation i något fall skulle kunna finnas ett intresse av att begränsa myndigheternas insyn i att kommunikationen över huvud taget har förekommit, är det enligt vår mening lämpligast att säkerställa en proportionell avvägning mellan brottsbekämpnings- och integritetsintresset i sådana fall genom en balanserad reglering om brottsbekämpande myndigheters tillgång till lagrade uppgifter. Detta hindrar naturligtvis inte att det sker fortsatta överväganden om möjligheterna att även på andra sätt förstärka skyddet såvitt gäller viss kommunikation.

EU-rätten tillåter att medlemsstaterna löser frågor på olika sätt och enligt egna traditioner. Sammanfattningsvis gör vi således bedömningen att det ur ett EU-rättsligt perspektiv inte finns något som tyder på en konflikt mellan reglerna om yrkesmässig tystnadsplikt och ett generellt lagringskrav avseende trafikuppgifter.

7.3 Tillgången till lagrade uppgifter om elektronisk kommunikation

7.3.1 Direktivet och EU-domstolens dom

I artikel 4 i datalagringsdirektivet anges att medlemsstaterna ska vidta åtgärder för att säkerställa att uppgifter som lagras i enlighet med direktivet görs tillgängliga endast för behöriga nationella myndigheter i närmare angivna fall och i enlighet med nationell lagstiftning. De förfaranden som ska följas och de villkor som ska uppfyllas för att få tillgång ska fastställas av varje medlemsstat för sig i enlighet med nödvändighets- och proportionalitetskraven samt i enlighet med EU-rätten och folkrätten, särskilt med beaktande av Europakonventionen. Av artikel 1.1 framgår att syftet med lagringen är att säkerställa att uppgifterna finns tillgängliga för utredning, avslöjande och åtal av allvarliga brott såsom de definieras av varje medlemsstat i deras nationella i lagstiftning. Tillgången är därigenom begränsad till brottsbekämpande

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

EU-domstolen har i sin dom på ett antal punkter kritiserat det faktum att datalagringsdirektivet inte närmare reglerar hur tillgång ska ges till de uppgifter som lagras enligt direktivet, utan i stor utsträckning lämnar fritt för medlemsstaterna att själva reglera den frågan (punkterna 60–62). Domstolen pekar på att det inte finns något objektivt kriterium som begränsar tillgången till uppgifter i förhållande till brottets svårighetsgrad. Inte heller reglerar direktivet närmare hur de nationella myndigheterna ska få tillgång till uppgifterna. Vidare innehåller direktivet inga bestämmelser som begränsar antalet personer som kan få tillgång till uppgifterna till vad som kan anses absolut nödvändigt. Domstolen lyfter också fram att de nationella myndigheternas tillgång till lagrade trafikuppgifter inte har gjorts beroende av en föregående kontroll, antingen av en domstol eller av ett annat organ vars uppgift är att begränsa tillgången till vad som kan anses strikt nödvändigt.

7.3.2 Inhämtning av uppgifter rörande elektronisk kommunikation i svensk rätt – inledande anmärkningar

Bestämmelser om när leverantörer av elektroniska kommunikationstjänster och kommunikationsnät ska lämna ut uppgifter om elektronisk kommunikation och kommunikationsutrustning till de brottsbekämpande myndigheterna finns i lagen om elektronisk kommunikation. Av regleringen i 6 kap. LEK följer att trafikuppgifter som lagras av en leverantör med stöd av den tvingande regleringen i 16 a § i nämnda

kapitel får behandlas – vid sidan av själva lagringen och den efterföljande raderingen – endast för att lämnas ut enligt 6 kap. 22 § första stycket 2 LEK (abonnemangsuppgifter), 27 kap. 19 § RB och enligt inhämtningslagen. Villkoren för denna inhämtning av uppgifter, som alltså är uppdelad på tre olika regelverk, berörs mer ingående nedan.

Det kan nämnas att uppgifter som inte lagrats med stöd av den tvingande regleringen i 6 kap. 16 a § LEK ändå kan finnas tillgängliga hos leverantören exempelvis för att denne behöver uppgifterna för sin fakturering. Sådana uppgifter kan också hämtas in av de brottsbekämpande myndigheterna enligt gällande regelverk.

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

Abonnemangsuppgifter, trafikuppgifter och lokaliseringsuppgifter

Med uppgifter om abonnemang i 6 kap. 20 § LEK avses t.ex. uppgifter om abonnentens nummer, namn, titel och adress – s.k. kataloguppgifter (prop. 1992/93:200 s. 310). Sådana uppgifter finns ofta tillgängliga i elektronisk form i abonnentförteckningar som leverantörerna upprättar. För att uppgifter om en fysisk person ska tas in i en abonnentförteckning som görs allmänt tillgänglig krävs att den enskilde lämnat sitt samtycke till det (6 kap. 16 § LEK). I den utsträckning uppgifter finns tillgängliga i sådana allmänt tillgängliga förteckningar omfattas de, till följd av abonnentens samtycke, i praktiken inte av tystnadsplikten. Bestämmelserna om skyldighet att lämna ut uppgifter om abonnenter får därför

betydelse i första hand i fråga om uppgifter som rör abonnenter som inte har lämnat sitt samtycke till att uppgifterna offentliggörs och när det gäller nummer som tilldelas olika abonnenter med slumpvis variation, framför allt dynamiska ip-adresser.

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

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

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

kommunikationsutrustning som används vid överföringen av ett elektroniskt meddelande.

7.3.3 Förhandskontroll vid inhämtning av uppgifter om elektronisk kommunikation

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

Genom en förhandskontroll av domstol inrymmer systemet ett inslag som skapar starka garantier för att de åtgärder som brottsbekämpande myndigheter vidtar i varje enskilt fall uppfyller lagens stränga begränsningar och skyddsregler. Eftersom prövningen ska göras efter en ansökan av åklagaren tvingas de brottsbekämpande myndigheterna noga motivera behovet av åtgärden för att övertyga domstolen om att övervakningsåtgärden ska medges. Denna typ av kontroll ses i vissa jurisdiktioner som en grundläggande förutsättning för en rättssäker brottmålsprocess.[9]

Som argument för att kräva förhandskontroll när det gäller åtgärder som inte är så resurskrävande för de offentliga organen kan också framhållas att resursargumenten, som annars i praktiken ofta är av stor betydelse för verksamheten (se t.ex. SOU 2012:44

[9] Se t.ex. Katz v. United States, 289 U.S. 247 (1967), som rörde hemlig telefonavlyssning.

s. 648) i sådana fall inte får någon påtaglig återhållande effekt. Vidare kan konstateras att en tillsyn som sker i efterhand normalt måste genomföras utifrån några slags urvalskriterier och knappast kan bli heltäckande.

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

7.3.4 Efterhandskontroll vid inhämtning av uppgifter om elektronisk kommunikation och behandlingen av personuppgifter

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

SIN bedriver sin verksamhet genom inspektioner och andra utredningar som sker på eget initiativ (2 §). Till grund för tillsynsverksamheten ligger bl.a. de anmälningar som de brottsbekämpande myndigheterna gör om interimistiska beslut om tvångsmedelsanvändning som upphört att gälla innan domstolen prövat åtgärderna (6 § lagen om åtgärder för att utreda vissa allvarliga samhällsfarliga brott), om inhämtning enligt inhämtningslagen (6 § inhämtningslagen) och om de fall då underrättelse till enskilda som varit föremål för en övervakningsåtgärd har underlåtits på grund av sekretess (14 b § förundersökningskungörelsen [1947:948] och förordningen [2007:1144] om fullgörande av underrättelseskyldighet enligt lagen [2007:979] om åtgärder för att förhindra vissa särskilt allvarliga brott). Urvalet av tillsynsärenden görs med utgångspunkt i nämndens bedömning av var risken för felaktig rättstillämpning hos de granskade myndigheterna är som störst och tillsynsmetodiken är i huvudsak tematisk (se t.ex. SIN:s årsredovisning för 2013, dnr 7-2014, s. 10). Nämnden får uttala sig om konstaterade förhållanden och sin uppfattning om behov av förändringar i verksamheten och ska verka för att brister i lag eller annan författning avhjälps.

SIN:s tillsyn avseende användningen av hemliga tvångsmedel har på senare tid särskilt inriktats på ärenden i vilka åklagare beslutat att underlåta underrättelse till enskild, frågor om förstöring av upptagningar och uppteckningar efter hemlig tvångsmedelsanvändning, dokumentationsfrågor samt beslut om inhämtning enligt inhämtningslagen. Under 2013 omfattande tillsynen även anmälningar till nämnden om interimistiska beslut enligt lagen om åtgärder för att utreda vissa samhällsfarliga brott samt tillämpningen av 20 § förundersökningskungörelsen när det gäller protokollföringen av uppgifter som rör användningen av hemliga tvångsmedel. Tillsynen har enligt nämndens redovisningar visat att de brottsbekämpande myndigheterna överlag har bedrivit sin verksamhet i enlighet med lag och andra författningar. Brister har dock uppmärksammats, bl.a. att åklagarnas rättstillämpning av de regler som styr underrättelseskyldigheten till enskild inte förefaller vara enhetlig, att förstöringen av upptagningar och uppteckningar från hemliga tvångsmedel i vissa fall har dröjt för länge och att dokumentationen över vidtagna åtgärder brustit.

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

Antalet kontrollärenden på begäran av enskilda har varierat över åren. Under åren 2011 och 2012 inkom omkring 50 framställningar per år. År 2013 ökade antalet till 411. Av SIN:s årsredovisning för 2013 (dnr 7-2014) framgår att nämnden bedömer att den stora ökningen av antalet kontrollärenden huvudsakligen kan förklaras av de avslöjanden som gjordes i november 2013 om Polismyndigheten i Skånes behandling av personuppgifter i det s.k. kringresanderegistret. Kontrollärendena har i flertalet fall avslutats med att den enskilde har underrättats om att kontrollen inte har påvisat någon hantering i strid med lag eller annan författning. År 2013 överlämnades dock tre ärenden till JK för prövning av om det förekommit felaktigheter som kan medföra skadeståndsansvar för staten gentemot den enskilde. År 2012 överlämnades ett sådant ärende och år 2011 fyra sådana ärenden till JK för prövning. Av dessa åtta ärenden är endast ett ärende ännu inte avslutat. Ett ärende har skrivits av utan åtgärd. I tre fall har JK beviljat ersättning för kränkning av artikel 8 i Europakonventionen på den grunden att personuppgifter inte gallrats ur Säkerhetspolisens register i föreskriven ordning (i likhet med vad som i några fall förekommit i *Segerstedt-Wiberg m.fl. mot Sverige)*. I tre fall har kränkning av artikel 8 konstaterats på grund av att upptagningar från hemlig teleavlyssning bevarats under längre tid än vad som

medgetts i lag, dvs. utan stöd i lag. I dessa fall har JK bedömt att konstaterandet av en rättighetskränkning ansetts vara tillräcklig gottgörelse för den ideella skada kränkningen inneburit. År 2012 överlämnades också ett ärende till åklagaren.

När det gäller andra brottsbekämpande myndigheter än Polisen och Säkerhetspolisen är det endast Datainspektionen som har ansvar att utöva tillsyn över behandlingen av personuppgifter i myndigheternas verksamhet. Datainspektionens tillsynsansvar omfattar all behandling av personuppgifter som är helt eller delvis automatiserad eller som ingår i manuella register.

De brottsbekämpande myndigheternas inhämtning av uppgifter enligt 6 kap. 22 § första stycket 2 LEK är normalt ett led i en automatiserad behandling av personuppgifter. Sådan behandling står således under Datainspektionens kontroll. Inspektionens tillsyn begränsar sig dock till om reglerna om behandlingen av personuppgifter har efterlevts i verksamheten. Sådana bestämmelser finns i – vid sidan av personuppgiftslagen – t.ex. kustbevakningsdatalagen (2012:145), polisdatalagen, lagen om polisens allmänna spaningsregister, lagen (2005:787) om behandlingen av uppgifter i Tullverkets brottsbekämpande verksamhet och lagen (1999:90) om behandlingen av personuppgifter vid Skatteverkets medverkan i brottsutredningar och anknytande förordningar samt förordningen (2006:937) om behandling av personuppgifter inom åklagarväsendet.

7.3.5 Tillgången till abonnemangsuppgifter

Den svenska regleringen

En leverantör som har fått del av eller har tillgång till uppgifter om abonnemang, innehållet i ett elektroniskt meddelande och andra uppgifter som angår ett särskilt elektroniskt meddelande har – med vissa undantag i förhållande till innehavaren av ett abonnemang och den som tagit del i utväxlingen av meddelandet – tystnadsplikt för dessa uppgifter (6 kap. 20 § LEK). Uppgifter som angår ett särskilt elektroniskt meddelande anses enligt praxis vara uppgifter om vilka som har deltagit i utväxlingen av ett elektroniskt meddelande, uppgifter om när och under hur lång tid utväxlingen ägde rum och uppgifter om positionen hos den utrustning som använts vid

kommunikationen. Tystnadsplikten omfattar i förekommande fall även t.ex. information om att uppgifter i hemlighet har inhämtats av de brottsbekämpande myndigheterna (6 kap. 21 § LEK).

En åklagarmyndighet, polismyndighet eller annan myndighet som ska ingripa mot brott (Tullverket, Kustbevakningen och Skatteverket) har utan hinder av tystnadsplikten rätt att få tillgång till abonnemangsuppgifter, om uppgiften gäller misstanke om brott som myndigheten ska ingripa mot (6 kap. 22 § första stycket 2 LEK). Regleringen innebär att de brottsbekämpande myndigheterna i princip har rätt att inhämta abonnemangsuppgifter för att beivra alla typer av brott utom sådana brott som åtalas enbart av målsäganden. En begränsning av tillgången följer dock av ändamåls-, behovs- och proportionalitetens krav (jfr de krav som följer av artikel 8 i Europakonventionen och 2 kap. 21 § RF som gäller för att begränsa grundläggande fri- och rättigheter och de allmänna principer som gäller för användning av tvångsmedel som redovisas i avsnitt 3.3).

Fram till den 1 juli 2012 gällde att tystnadsplikten för abonnemangsuppgifter genombröts bara om fängelse var föreskrivet för brottet och det enligt myndighetens bedömning kunde föranleda annan påföljd än böter. På grund av denna begränsning kunde abonnemangsuppgifter i realiteten inte hämtas in för många brott av normalgraden med böter i straffskalan. I förarbetena till 2012 års ändring i lagen om elektronisk kommunikation konstaterade regeringen bl.a. att det hade skett en betydande teknisk utveckling och förändring av i vilken omfattning enskilda använder bl.a. datorer och mobiltelefoner (prop. 2011/12:55 s. 102). Trakasserier via internet av olika slag, nätmobbning och förtal, liksom vuxnas kontakter med barn i sexuella syften (grooming) hade blivit ett allt större problem. När sådant beteende misstänktes utgöra brott hade de brottsutredande myndigheterna ofta begränsade möjligheter att utreda brotten, bl.a. eftersom möjligheterna att identifiera den som stått bakom kommunikationen många gånger varit små på grund av begränsningarna i rätten att få tillgång till abonnemangsuppgifter. Detsamma gällde i fråga om de reella möjligheterna för Polisen att ingripa mot internetrelaterade immaterialrättsbrott. Vid bedömningen av det intrång som ett enskilt utlämnande av uppgifter om en abonnent innebär beaktade regeringen särskilt att

privatpersoner vanligen använder dynamiska ip-adresser. Möjligheterna till kartläggning av en abonnents kontakter via internet vid andra tillfällen bedömdes därmed bli begränsade vid ett enstaka utlämnande. Vidare menade regeringen att de brottsbekämpande myndigheternas intresse av tillgång till uppgifter om abonnemang hade förändrats på grund av utvecklingen av den internetrelaterade brottsligheten. Regeringen ansåg att intresset av att lämna ut abonnemangsuppgifter för att bekämpa brott vägde tyngre än det motstående intresset av att skydda enskildas integritet och föreslog därför att kravet på fängelse i straffskalan och det särskilda kravet i fråga om brottets straffvärde skulle tas bort (prop. 2011/12:55 s. 103). Riksdagen ställde sig bakom denna bedömning (bet. 2011/12:JuU8, rskr. 2011/12:212).

Analys

Abonnemangsuppgifter är integritetskänsliga

En uppgift om vilket abonnentnummer som har använts för att skicka eller ta emot ett visst meddelande utgör alltså en trafikuppgift då uppgifterna behövs för att överföra meddelandet. En uppgift om vem som innehar detta nummer är samtidigt en abonnemangsuppgift.[10] Dessa uppgifter finns normalt tillgängliga i leverantörernas kund- och faktureringssystem under den tid som de behövs för att fakturera för utnyttjade tjänster, erbjuda andra mervärdestjänster eller övervaka nätsäkerheten.

En uppgift om vem som innehar eller nyttjar ett visst nummer för kommunikation är inte information som i sig är särskilt integritetskänslig. Sett isolerade i förhållandet till annan information om hur numret har använts kan sådana uppgifter nämligen inte användas för att kartlägga och analysera en individs privatliv.[11] Uppgifterna kan emellertid användas *tillsammans* med andra uppgifter om trafik som förekommer i de allmänna

[10] Jfr dock Naarttijärvi, Markus, För din och andras säkerhet, anmärkt ovan, s. 284, och där gjorda hänvisningar.
[11] Detta innebär givetvis inte att uppgifterna inte kan vara skyddsvärda, t.ex. om det finns risk för att innehavaren utsätts för hot och förföljelse om kontaktuppgifterna röjs (jfr 21 kap. 3 § offentlighets- och sekretesslagen [2009:400]).

kommunikationsnäten och därigenom indirekt utnyttjas för att kartlägga integritetskänsliga uppgifter om den enskildes privatliv. Ibland kan uppgifter om vilka personer eller organisationer en individ har haft kontakt med i sig vara mycket integritetskänsliga. Det gäller t.ex. om uppgifterna kan avslöja att kontakter har förekommit med stödorganisationer för psykiatriska hälsoproblem eller med medicinska institutioner av olika slag. Även om trafikanalys av metadata i vissa fall kommer att kunna avslöja integritetskänsliga uppgifter om en enskilds personliga förhållanden, kommer uppgifterna inte att kunna avslöja själva innehållet i kommunikationen. En enstaka uppgift om vem som är abonnent kommer inte heller att kunna användas för att kartlägga sociala kontakter. För det krävs tillgång till ytterligare metadata. Det kan även noteras att uppgiften om vem som innehar ett visst internetabonnemang inte med säkerhet säger något om identiteten på användaren av en ip-adress. En viss adress kan nyttjas av flera personer som har tillgång till ett lokalt nätverk. Om nätverket inte är skyddat, kan det nyttjas även av för abonnenten okända personer. Möjligheterna att kartlägga enskildas privatliv med utgångspunkt i enstaka kontaktuppgifter blir därför i många fall begränsade.

Tillgången till abonnemangsuppgifter motiveras av ett viktigt samhällsintresse

Både lagringen och utlämnandet av uppgifter om identiteten på en användare av elektroniska kommunikationstjänster eller kommunikationsnät innefattar ett intrång i användarens privatliv och rätten till självbestämmande över information som rör honom eller henne. Ju längre uppgifterna lagras och ju större spridning uppgifterna får, desto större blir intrånget. Det potentiella intrånget ökar dessutom genom den s.k. ändamålsglidning som uppkommer vid vidareanvändningen av uppgifterna; ju större skillnad det är mellan det ursprungliga insamlingsändamålet och det senare vidareanvändningsändamålet, desto större blir det potentiella integritetsintrånget.

Utlämnandet av uppgifter om en telefoni- eller internetanvändares identitet för brottsbekämpande ändamål svarar mot ett samhällsintresse som kan rättfärdiga ett intrång i

privatlivet. Av EU-domstolens fasta praxis följer att intrånget måste begränsas till vad som är strikt nödvändigt (se t.ex. *Satakunnan Markkinapörssi och Satamedia*, C-73/07, punkt 56, *Volker und Markus Schecke* och *Eifert*, C-92/09 och C-93/09, punkterna 77 och 86, *IPI*, C-473/12, punkt 39). Ju allvarligare ett misstänkt brott är, desto större integritetsintrång måste den enskilde typiskt sett tåla. Men ett intrång kan inte utan vidare avvisas på den grunden att ett misstänkt brott har ett förhållandevis lågt straffvärde. Om uppgifterna är nödvändiga för att det överhuvudtaget ska finnas förutsättningar för myndigheterna att utreda misstankar om brott, torde intrånget normalt vara en proportionell inskränkning av rätten till respekt för privatlivet. Detta gäller t.ex. i fråga om förutsättningarna för utredning av många internetrelaterade brott.

Vi noterar i detta sammanhang att staten till följd av Europakonventionen inte bara har en folkrättsligt grundad skyldighet att avstå från att göra intrång i enskildas privatliv. Det folkrättsliga åtagandet innebär också att staten har en skyldighet att vidta åtgärder för att skydda enskilda mot allvarliga intrång i privatlivet från andra enskilda. Detta åtagande inbegriper en skyldighet att införa och vidmakthålla en straffrättslig lagstiftning till skydd för enskildas personliga frid och säkerhet. Det måste i sådana fall också finnas förutsättningar att effektivt kunna utreda och lagföra brott (se t.ex. Europadomstolens domar i målen *K.U. mot Finland,* anmärkt ovan, § 46, och *Söderman mot Sverige* [GC], nr 5786/08, §§ 78–85).

Utlämnandet är ett proportionellt integritetsintrång

EU-domstolen pekar i datalagringsdomen på ett behov av tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av den rättighetsbegränsande åtgärden och att det ska finnas garantier för ett effektivt skydd mot missbruk och mot otillåten användning av personuppgifter. Trots EU-domstolens generella uttalanden om att myndigheternas tillgång ska begränsas till brott som är av tillräckligt allvarlig natur för att motivera den omfattande datalagringen, framstår det som klart att medlemsstaterna har ett visst utrymme att – inom ramen för

proportionalitetsprincipens krav – reglera vad som ska gälla för att lämna ut olika uppgifter. De artiklar i rättighetsstadgan som har en motsvarighet i Europakonventionen, bl.a. artikel 7 om skyddet för privatlivet, ska nämligen enligt artikel 52.3 i rättighetsstadgan ha samma innebörd och räckvidd som i Europakonventionen. Europadomstolen har i sin praxis gett konventionsparterna ett visst eget tolkningsutrymme vid tillämpningen av konventionen. På samma sätt måste medlemsstaterna också rimligen ha ett visst utrymme att själva bedöma vilka slags kontrollsystem som är nödvändiga i den egna staten för att säkerställa att regleringen följs. Kontrollsystemen måste kunna skifta beroende på hur omfattande integritetsintrånget är med beaktande av bl.a. uppgifternas karaktär, möjligheterna till kartläggning av privatlivet och riskerna för otillåten användning.

Enligt vår uppfattning kan EU-domstolens uttalanden om datalagringsdirektivets brist på reglering av förutsättningarna för myndigheternas tillgång till lagrade uppgifter inte tolkas så att varje form av utlämnande av någon lagrad uppgift som sker för att bekämpa mindre allvarlig brottslighet än sådan brottslighet som ursprungligen motiverat lagringsskyldigheten kommer i konflikt med unionsrätten. En nationell lagstiftning som tillåter att s.k. kataloguppgifter – uppgifter om vem som har en viss adress eller ett visst telefonnummer – kontrolleras och lämnas ut till brottsbekämpande myndigheter för att bekämpa även annan brottslighet än sådan som objektivt sett kan betecknas som allvarlig kan enligt vår bedömning inte i sig stå i strid med den unionsrättsliga proportionalitetsprincipen. Det är i detta sammanhang väsentligt att konstatera att ändamålsglidningen i förhållande till det huvudsakliga ändamålet att bekämpa allvarlig brottslighet är begränsad, eftersom de lagrade uppgifterna inte får lämnas ut för annat än brottsbekämpande ändamål. Vidare bör beaktas att enbart kataloguppgifter av nämnda slag inte är särskilt integritetskänsliga och att en enstaka uppgift om t.ex. en dynamisk ip-adress inte möjliggör någon mer omfattande kartläggning av den enskildes personliga förhållanden.

Är kontrollen i efterhand en tillräcklig skyddsåtgärd?

Enligt vår bedömning kan det av EU-domstolens dom inte utläsas att rättighetsstadgan och unionsrättens allmänna principer innebär att det är nödvändigt att inrätta en ordning med förhandsprövning av *varje* slag av åtkomst till uppgifter som rör förmedlade elektroniska meddelanden. Tvärtom framstår det som rimligt att skilda kontrollmekanismer bör kunna inrättas beroende bl.a. på vilket integritetsintrång som uppkommer till följd av utlämnandet och användningen av uppgifterna (se t.ex. Europadomstolens dom i *P.G. och J.H. mot Förenade kungariket*, nr 44787/98, § 46). Enstaka uppgifter om vem som har tilldelats ett visst telefonnummer eller en viss tillfällig ip-adress är inte, tagna för sig, särskilt integritetskänsliga. Sådana uppgifter ger inte de brottsbekämpande myndigheterna några vittgående möjligheter att kartlägga en individs privatliv. Det ter sig mot den bakgrunden som tillräckligt med en oberoende kontroll och tillsyn i efterhand för att utlämnandet ska vara förenligt med regleringen om skydd för privatlivet och den personliga integriteten i Europakonventionen, rättighetsstadgan och unionsrättens allmänna principer. Frågan är då om den externa kontrollen över tillämpningen av dessa regler är tillräckligt effektiv för att uppfylla unionsrättens och europarättens krav.

Vi kan i detta sammanhang konstatera att tillsynen över Polisens och övriga brottsbekämpande myndigheters tillämpning av lagar och andra författningar i den brottsbekämpande verksamheten delas mellan flera myndigheter. Datainspektionen och SIN har delvis överlappande tillsynsansvar när det gäller Polisens och Säkerhetspolisens behandling av personuppgifter. Frågan om hur tillsynen ska inrättas i framtiden när det gäller dessa myndigheter är för närvarande under utredning och hänger delvis samman med den pågående omorganisationen av Polisen, se Polisorganisationskommitténs (Ju2010:09) betänkande Tillsyn över polisen (SOU 2013:42) och kommitténs tilläggsdirektiv från februari 2014 (dir. 2014:17). Övriga brottsbekämpande myndigheters behandling av personuppgifter står under tillsyn enbart av Datainspektionen. Datainspektionens och SIN:s tillsyn inriktas i första hand på att myndigheterna följer de föreskrifter som gäller för behandlingen av personuppgifter. För SIN:s del

gäller att tillsynen omfattar även användningen av hemliga tvångsmedel och vidareanvändningen av de uppgifter som inhämtas med sådana metoder. Uppdraget att utöva tillsyn över leverantörernas efterlevnad av lagen om elektronisk kommunikation vilar på PTS. Därtill kommer att tillsyn över att statliga förvaltningsmyndigheter följer lagar och andra författningar samt i övrigt fullgör sina skyldigheter utövas även av Riksdagens ombudsmän och JK. Den tillsyn som dessa båda myndigheter utövar sker dock på mer diskretionär grund än vad som gäller för övriga nyss nämnda myndigheter.

Eftersom det är EU-domstolen som i sista hand avgör hur unionsrätten ska tolkas är inte det inte möjligt att vara helt säker på att den nuvarande utformningen av tillsynsansvaret och de brottsbekämpande myndigheternas rutiner för dokumentation och loggning av inhämtning av abonnemangsuppgifter fullt ut tillgodoser kraven på effektiv kontroll av utlämnandet och användningen av sådana uppgifter. Den svenska regleringen torde dock rymmas inom ramen för vad som är godtagbart. Emellertid anger unionsrätten och europarätten bara en miniminivå för skyddet av de grundläggande fri- och rättigheterna, och det är dessutom vår utgångspunkt att den svenska regleringen inte bör balansera på gränser för vad som är tillåtet enligt unionsrätten och Europakonventionen. Vi avser därför att överväga denna fråga närmare i det fortsatta arbetet.

7.3.6 Tillgången till uppgifter om elektronisk kommunikation enligt rättegångsbalken

Den svenska regleringen

Hemlig övervakning av elektronisk kommunikation innebär enligt 27 kap. 19 § RB att uppgifter i hemlighet hämtas in om meddelanden som i ett elektroniskt kommunikationsnät överförts till eller från ett telefonnummer eller en annan adress (t.ex. en ip-adress), vilka elektroniska kommunikationsutrustningar som har funnits inom ett visst geografiskt område eller i vilket geografiskt område en viss elektronisk kommunikationsutrustning finns eller har funnits. Hemlig övervakning av elektronisk kommunikation får

användas också för att hindra meddelanden som överförs i elektroniska kommunikationsnät från att nå fram.

Hemlig övervakning av elektronisk kommunikation får enligt 27 kap. 19 § tredje stycket RB användas vid förundersökning som avser brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader, vid förundersökning som avser dataintrång (4 kap. 9 c § BrB), barnpornografibrott som inte är ringa (16 kap. 10 § BrB), narkotikabrott av normalgraden (1 § narkotikastrafflagen [1968:64]) och narkotikasmuggling av normalgraden (6 § första stycket lagen [2000:1225] om straff för smuggling) samt vid förundersökning som avser försök, förberedelse eller stämpling till sådana brott i den mån sådana förstadier till brott är straffbelagda.

En förutsättning för att hemlig övervakning av elektronisk kommunikation ska få användas vid förundersökning om nämnda brott är att det finns någon som är skäligen misstänkt för brottet och att åtgärden är av synnerlig vikt för utredningen (27 kap. 20 § första stycket RB). Om det inte finns någon som är skäligen misstänkt för brottet får hemlig övervakning av elektronisk kommunikation användas även för att utreda vem som kan misstänkas för brottet. Det krävs då att förundersökningen avser ett brott som kan föranleda hemlig avlyssning av elektronisk kommunikation, dvs. att det är fråga om ett brott för vilket inte är föreskrivet lindrigare straff än fängelse i två år eller att förundersökningen avser försök, förberedelse eller stämpling till ett sådant brott om gärningen är straffbelagd eller att – om utredningen avser ett annat brott – brottet med hänsyn till omständigheterna kan antas ha ett straffvärde som överstiger fängelse i två år. Åtgärden måste även i dessa fall vara av synnerlig vikt för utredningen.

Övervakningsåtgärden får avse ett telefonnummer eller en annan adress eller en viss elektronisk kommunikationsutrustning som innehas eller har innehafts eller annars kan antas ha använts eller komma att användas av den misstänkte under den tid ett tillstånd till övervakning avser (27 kap. 20 § första stycket 1 RB).

Hemlig övervakning av elektronisk kommunikation får enligt huvudregeln användas först efter en förhandsprövning och beslut av domstol. Tingsrätten prövar frågan efter ansökan av åklagaren (27 kap. 21 § RB). Om det kan befaras att ett inhämtande av

domstolens tillstånd skulle medföra en sådan fördröjning eller annan olägenhet som är av väsentlig betydelse för utredningen, får tillstånd medges interimistiskt av åklagaren i avvaktan på domstolens prövning. Ett sådant beslut ska omedelbart anmälas till domstolen, som ska pröva om det finns skäl för åtgärden. Om domstolen vid sin prövning bedömer att det inte finns skäl för åtgärden, får sådana uppgifter som redan har hunnit inhämtas enligt det interimistiska beslutet inte användas i en förundersökning till nackdel för den som har omfattats av övervakningen (27 kap. 21 a § RB).[12]

När hemlig övervakning av elektronisk kommunikation används för att utreda vem som kan misstänkas för ett brott får övervakningen bara innebära inhämtning av uppgifter i förfluten tid (27 kap. 20 § andra stycket 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 är begränsade på så sätt att brott som kan antas föranleda enbart en bötespåföljd normalt inte får utredas (27 kap. 23 a § RB). Uppgifterna får dock användas för att förhindra ett förestående brott.

Vissa bestämmelser om underrättelse till den som har utsatts för en hemlig tvångsåtgärd finns i 27 kap. 31–33 §§ RB, 15 § lagen om hemlig rumsavlyssning och 16 § lagen om åtgärder för att förhindra vissa särskilt allvarliga brott. Av dessa bestämmelser följer att den som är eller har varit misstänkt för brott och utsatts för en hemlig tvångsåtgärd, eller den som utan att vara misstänkt för brott innehar eller har innehaft en adress eller utrustning som omfattas av ett beslut om en hemlig tvångsåtgärd, som regel ska underrättas om åtgärden och dess omfattning i efterhand. Detta gäller även i förhållande till den som har utsatts för en hemlig tvångsåtgärd som använts i syfte att förhindra ett nära förestående brott, om brottet faller inom Polisens verksamhetsområde. Om sekretess fortfarande

[12] I ett beslut att tillåta en övervakningsåtgärd ska det anges under vilken tid åtgärden får användas. Tiden ska bestämmas så att den inte blir längre än nödvändigt och får, för tiden från beslutet, inte avse längre tid än en månad. Den adress och den kommunikationsutrustning som avses med åtgärden och det geografiska område som omfattas av tillståndet ska anges i beslutet (27 kap. 21 § andra och tredje styckena RB). Beslutet ska upphävas så snart det inte längre finns skäl för åtgärden (27 kap. 23 § RB).

ett år efter åtgärden gäller på någon av närmare angivna grunder, bl.a. om uppgifterna omfattas utrikes- eller försvarssekretess eller om ett röjande skulle medföra skada för brottsförebyggande eller brottsutredande verksamhet, får en sådan underrättelse dock underlåtas.[13] Åklagaren ska då underrätta SIN om detta (14 b § förundersökningskungörelsen och förordningen om fullgörande av underrättelseskyldighet enligt lagen om åtgärder för att förhindra vissa särskilt allvarliga brott).

När det gäller förundersökning som avser vissa brott som faller inom Säkerhetspolisens ansvarsområde finns i lagen om åtgärder för att utreda vissa samhällsfarliga brott särskilda bestämmelser om användning av bl.a. hemlig övervakning av elektronisk kommunikation. I de fall denna lag är tillämplig gäller inte de begränsningar som annars följer av bl.a. 27 kap. 19 § tredje stycket RB (straffminimireglerna) för att tillstånd till en övervakningsåtgärd ska få beviljas av domstolen.

En underrättelse till enskild ska inte lämnas när åtgärder används vid brott som faller inom Säkerhetspolisens ansvarsområde (bl.a. terroristbrott och brott mot rikets säkerhet).

Analys

Samhällsintresset av att utreda uppräknade brott är starkt

Det stora flertalet av de brottstyper som omfattas av regleringen om hemlig övervakning av elektronisk kommunikation har ett straffminimum på minst sex månaders fängelse. Inom denna kategori faller exempelvis grov misshandel, grovt vållande till annans död, olaga frihetsberövande, grovt utnyttjande av barn för sexuell posering, grov stöld, rån, grovt vapenbrott, grovt bedrägeri, grov utpressning, grovt penninghäleri och grovt barnpornografibrott. Till dessa brott kommer den kategori av brott som är allvarliga nog för att även kunna motivera användning av hemlig avlyssning. Brott som har ett straffminimum på minst två års fängelse omfattar bl.a. mord, dråp, människorov,

[13] Enligt Riksåklagarens riktlinjer för underrättelser om hemliga tvångsmedel RÅR 2007:3 ska frågan om sekretess fortfarande gäller fortlöpande bevakas och prövas före utgången av varje kalenderkvartal.

människohandel, våldtäkt, grovt koppleri, grovt rån, mordbrand, allmänfarlig ödeläggelse, grovt sabotage, kapning, grov penningförfalskning, grovt spioneri, grovt narkotikabrott, grov narkotikasmuggling och terroristbrott. Enligt vår uppfattning råder det inte någon tvekan om att alla dessa brott är att betrakta som allvarliga och att samhällsintresset av att förebygga och utreda brotten är starkt.

Därutöver får hemlig övervakning av elektronisk kommunikation generellt användas som straffprocessuellt verktyg i förundersökning om narkotikabrott och narkotikasmuggling av normalgraden och för att utreda dataintrång och barnpornografibrott av normalgraden.

För narkotikabrott och narkotikasmuggling döms till fängelse högst tre år. Vid hantering av betydande mängder narkotika i överlåtelsesyfte döms inte sällan till straff i den övre delen av straffskalan. Samhällsintresset av att förebygga och utreda narkotikabrott är betydande, inte minst för att denna brottstyp är vanligt förekommande inom ramen för organiserad brottslighet. Brotten är i dessa fall att betrakta som allvarliga i objektiv mening.

För barnpornografibrott som inte är att anse som ringa döms till fängelse högst två år. För dataintrång döms till böter eller fängelse högst två år. Straffskalorna för dessa brottstyper stödjer slutsatsen att brotten inte är att betrakta som lika allvarliga som de övriga brottstyper som berättigar till användning av hemlig övervakning av elektronisk kommunikation. Vi kan dock konstatera att tillgången till trafikuppgifter många gånger kan vara helt avgörande för att det över huvud taget ska vara möjligt att utreda och lagföra dessa brott, något som naturligtvis påverkar proportionalitetsbedömningen. Mot bakgrund av samhällets starka intresse av att skydda barn mot sexuell exploatering kan – vid en avvägning mellan brottsbekämpningsintresset och den enskildes motstående integritetsintresse – en ordning som innebär att barnpornografibrott inte kommer att kunna utredas knappast godtas. Vid motsvarande avvägning när det gäller dataintrång – en gärning som innebär att någon olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift – konstateras att brottet i vissa fall kan leda till omfattande integritetsintrång för enskilda och även andra omfattande

skadeverkningar, bl.a. vid olika former av affärsspionage eller intrång i samhällsviktiga elektroniska uppgiftssamlingar. Även om brotten inte regelmässigt leder till en längre frihetsberövande påföljd, är samhällsintresset av att utreda brotten betydande.

Utöver i de fall som nämnts ovan får hemlig övervakning av elektronisk kommunikation användas för att utreda – samt i vissa fall också för att förhindra – vissa särskilt angivna brott som inte har ett straffminimum på fängelse i minst sex månader. Det handlar om sådana brott som bekämpas av Säkerhetspolisen, exempelvis sabotage och spionerі. Dessa brott betraktas som särskilt allvarliga eftersom de riktar sig mot samhällsstrukturen och mot rikets säkerhet. Det finns därför ett starkt samhällsintresse av att brotten effektivt kan utredas och förhindras.

Utlämnande bara när det är strikt nödvändigt

EU-domstolen pekar i datalagringsdomen på ett behov av tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av den rättighetsbegränsande åtgärden och att det ska finnas garantier för ett effektivt skydd mot missbruk och mot otillåten användning av personuppgifter. Domstolen efterlyser bl.a. ett objektivt kriterium för att avgränsa de nationella myndigheternas tillgång till och användning av de lagrade uppgifterna för bekämpning av brott som kan anses vara tillräckligt allvarliga för att motivera det aktuella ingreppet.

Som framgår ovan (avsnitt 7.3.1) har rådet uttalat att medlemsstaterna, vid bedömningen av om de nationella brott som möjliggör ett utlämnande är tillräckligt allvarliga, ska ta vederbörlig hänsyn till de brott som förtecknas i artikel 2 i rambeslutet om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna. Den svenska regleringen utgår i huvudsak från att brottens allvarlighetsgrad kan bestämmas utifrån brottens straffminimum. Därigenom klargörs genom regleringen i 27 kap. RB på ett tydligt sätt att i huvudsak endast sådana brott som i den svenska lagstiftningen klassificeras som allvarliga kan motivera användningen av hemlig övervakning av elektronisk kommunikation. När det gäller de brottstyper som i Sverige anses motivera en övervakningsåtgärd trots att ett längre

frihetsberövande straff inte kan antas följa på brottet, kan konstateras att samhällsintresset av att brotten utreds och åtal väcks i dessa fall är betydande. Den svenska regleringen ansluter i praktiken tämligen nära till de i rambeslutet förtecknade listbrotten.

Det måste vidare beaktas att den svenska regleringen inte bara innehåller specifika begränsningar i fråga om vilka brott som kan motivera en övervakningsåtgärd utifrån brottens allvarlighetsgrad. Som framgår ovan följer av de allmänna principer som gäller för all användning av straffprocessuella tvångsmedel bl.a. att ett tvångsmedel får användas bara när det finns ett påtagligt behov av det i det enskilda fallet och en mindre ingripande åtgärd inte är tillräcklig. Tvångsmedlet måste även i fråga om sin art, styrka, räckvidd och varaktighet stå i rimlig proportion till vad som står att vinna med åtgärden. Vidare är myndigheternas befogenheter att använda ett tvångsmedel bundna till de ändamål för vilket tvångsmedlet har beslutats. Av regleringen i 27 kap. RB följer därutöver att en hemlig övervakningsåtgärd ska kunna bedömas vara av synnerlig vikt för utredningen för att den ska få användas. Åtgärden måste också normalt rikta sig mot någon som är misstänkt för brott. Om det inte finns någon som är skäligen misstänkt för brottet, är utrymmet att använda åtgärden begränsat till mycket allvarliga brott, nämligen brott som föranleder fängelse minst två år.

Enligt vår uppfattning innehåller den gällande svenska regleringen sådana tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av hemlig övervakning av elektronisk kommunikation som EU-domstolen efterlyser i datalagringsdomen. Vår bedömning är således att den svenska regleringen och de allmänna rättsprinciper som gäller vid tillämpningen av tvångsmedelslagstiftningen uppfyller unionsrättens krav på strikt nödvändighet.

Förhandsprövning av utlämnandet

EU-domstolen pekar i datalagringsdomen på att direktivet inte reglerar de formella och materiella villkor som ska gälla och vilka krav som ska ställas på förfarandet för tillgång till trafik- och

lokaliseringsuppgifterna. Domstolen framhåller att direktivet inte kräver att tillgången till uppgifter ska vara underkastad någon förhandskontroll av en oberoende myndighet som har till uppgift att se till att tillgången begränsas till vad som är strikt nödvändigt.

Vi kan konstatera att den svenska regleringen av de brottsbekämpande myndigheternas tillgång till trafik- och lokaliseringsuppgifter under pågående förundersökning bygger på att en allmän domstol i det enskilda fallet ska pröva om förutsättningarna för utlämnande av uppgifterna är uppfyllda innan uppgifterna lämnas ut. Undantag från denna regel gäller bara i vissa brådskande fall. I dessa fall fattar i stället en åklagare, som är fristående från Polisen, ett interimistiskt beslut om tillstånd till inhämtning vilket omedelbart måste underställas domstolen för prövning. Uppgifter som inhämtats med stöd av ett interimistiskt tillstånd får inte användas om domstolen vid sin kontroll bedömer att det inte funnits skäl för åtgärden. Vi anser att denna ordning säkerställer att det finns en mycket effektiv kontroll över inhämtningen av trafik- och lokaliseringsuppgifter på förundersökningsstadiet.

För att säkerställa att enskildas rätt till skydd av privatlivet inte kränks sker även en efterhandskontroll av att gällande regelverk följs. Den förhandskontroll som görs av domstol och den tillsyn som bedrivs i efterhand av SIN genom inspektioner och genom kontroller på begäran av enskild uppfyller enligt vår bedömning europarättens och unionsrättens krav på tillförlitlig kontroll av att tillgången begränsas till dem som är behöriga mottagare och att integritetsintrånget inte går utöver vad som är nödvändigt med hänsyn till ändamålet.

Sammantaget gör vi alltså bedömningen att lagringen av uppgifter som sker för utlämnande av trafik- och lokaliseringsuppgifter i enlighet med bestämmelserna i 27 kap. RB uppfyller de krav som följer av den unionsrättsliga proportionalitetsprincipen.

7.3.7 Tillgång till uppgifter enligt inhämtningslagen

Den svenska regleringen

Lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (inhämtningslagen) reglerar förutsättningarna för polismyndigheterna och Tullverket att hämta in uppgifter om elektronisk kommunikation i underrättelseverksamhet. Ett uttalat syfte med lagens införande år 2012, då delvis motsvarande regler i lagen om elektronisk kommunikation upphävdes, var att stärka rättssäkerheten och integritetsskyddet (prop. 2011/12:55 s. 65 f.).

De uppgifter som får hämtas in enligt lagen är dels historiska trafikuppgifter, dels lokaliseringsuppgifter (1 §). Den senare kategorin avser såväl historiska lokaliseringsuppgifter som uppgifter om lokaliseringen i realtid. Uppgifter får hämtas in om omständigheterna är sådana att åtgärden är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott vilka har ett straffminimum på fängelse i minst två år och om åtgärden är proportionerlig (2 §). Inhämtning av uppgifter är också möjlig vid brottslig verksamhet som innefattar vissa särskilt angivna samhällsfarliga brott inom Säkerhetspolisens ansvarsområde vilka har ett lägre straffminimum än två år (3 §). Bestämmelsen är tidsbegränsad och ska enligt nuvarande reglering upphöra att gälla vid utgången av 2014, se lagen (2013:935) om ändring i lagen (2012:279) om ändring i lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet. Regeringen har dock föreslagit att bestämmelsens tillämpning ska förlängas till utgången av år 2016 (prop. 2013/14:237 s. 115).

Beslut om inhämtning enligt lagen fattas av myndigheten själv och är inte föremål för någon utomstående prövning (4 §). Det är myndighetschefen eller annan person som har fått uppgiften delegerad till sig som fattar beslutet. Den som enligt delegation har fått rätt att hämta in uppgifter får inte fatta beslut om inhämtning i sådan operativ verksamhet som han eller hon deltar i. Beslutet ska vara preciserat och tiden för beslutet får inte överstiga en månad (5 §).

SIN ska underrättas om ett beslut om inhämtning enligt lagen (6 §). Nämnden ska också utöva tillsyn över polismyndigheternas och Tullverkets användning av lagen. Nämnden är vidare skyldig att på begäran av en enskild person kontrollera om han eller hon har varit föremål för inhämtning enligt lagen (se avsnitt 7.3.4).

S.k. överskottsinformation som kommit fram om annan brottslighet får användas endast för att förhindra brott (7 §). Om uppgifter som kommit fram vid inhämtning ska användas i en förundersökning, krävs ett tillstånd till hemlig övervakning av elektronisk kommunikation (8 §). Ett sådant tillstånd ges av domstol (se avsnitt 7.3.6).

SIN har i sin granskning av underrättelser om beslut om inhämtning av uppgifter enligt inhämtningslagen år 2013 (dnr 14-2013) angett att nämnden mottagit 563 underrättelser avseende 722 beslut (Säkerhetspolisen undantaget). Nämnden har sammanfattningsvis angett att myndigheterna i de allra flesta fall handlägger ärenden enligt inhämtningslagen på ett tillfredsställande sätt men att inhämtningen också har uppvisat vissa brister. Det har exempelvis förekommit flera fall av för sena underrättelser till nämnden. De brister som hade påpekats under föregående års granskning, där inhämtning i vissa fall hade skett för brottslighet som inte omfattas av lagen eller där brottsrubriceringen inte tydligt hade angivits, hade med något enstaka undantag åtgärdats.

Analys

Inhämtning begränsad till allvarliga brott

Som ovan framgått är de brottsbekämpande myndigheternas tillgång enligt inhämtningslagen i princip begränsad till att avse uppgifter som är av särskild vikt för att förebygga, förhindra eller upptäcka brottslig verksamhet som innefattar brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år. Av SIN:s redovisning av tillsynsverksamheten under år 2012 framgår att de vanligast förekommande brottsrubriceringarna vid inhämtning enligt lagen varit grovt narkotikabrott och grov narkotikasmuggling (dnr 96-2013). Av uppgifter som vi inhämtat från Polisen för år 2013 framgår att den absoluta merparten av inhämtningarna även då avsett grovt narkotikabrott. I övrigt har

inhämtningar skett för underrättelser om grova rån, mord, grov allmänfarlig ödeläggelse, grov penningförfalskning, människohandel samt några enstaka beslut avseende andra brott såsom grov mordbrand, grov kapning och grovt spridande av gift eller smitta.

Det finns i svensk rätt ingen generell definition av vad som utgör ett allvarligt brott. Brott med en strafftröskel om två år tillhör dock tveklöst den kategorin. Vilken typ av brott som omfattas har, utöver vad som framgår av uppgifterna från Polisen ovan, närmare redovisats i avsnitt 7.3.6. Som en jämförelse kan också lyftas fram att någon som misstänkts för ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år *ska* häktas om det inte är uppenbart att det saknas skäl för det (s.k. obligatorisk häktning).

Uppgifter får i vissa situationer inhämtas även avseende brott som inte har ett straffminimum på två års fängelse. Det handlar om vissa särskilt angivna samhällsfarliga brott, exempelvis sabotage och spioneri som utreds av Säkerhetspolisen och som omfattas också såväl av lagen om åtgärder för att förhindra vissa särskilt allvarliga brott som av lagen om åtgärder för att utreda vissa samhällsfarliga brott. Som ovan redovisats är bestämmelsen tidsbegränsad och regeringen har aviserat en kartläggning och analys av dess tillämpning (prop. 2013/14:237 s. 116). Inhämtningen med stöd av denna bestämmelse avser brott som, även om de inte har ett straffminimum på två års fängelse, måste betraktas som allvarliga med tanke på att de riktar sig mot samhällsstrukturen och mot rikets säkerhet. Att det finns ett starkt samhällsintresse av att förebygga, förhindra eller upptäcka de angivna brotten kan knappast ifrågasättas. I det sammanhanget kan också nämnas att Europadomstolen i exempelvis fallet *Leander mot Sverige* vid en avvägning mellan skyddet för rikets säkerhet och sökandens rätt till skydd enligt artikel 8 konstaterat att statens utrymme att själv avgöra nödvändigheten i inskränkningen var stort.

Inhämtning utan föregående domstolskontroll

EU-domstolen har som en brist med datalagringsdirektivet framhållit att det i direktivet inte finns något krav på att de

nationella myndigheternas tillgång till uppgifter som lagrats med stöd av direktivet prövas av en domstol eller annat oberoende organ som har till uppgift att begränsa tillgången till vad som är strikt nödvändigt.

Inhämtningslagen innehåller som ovan redovisats regler som definierar förutsättningarna för en begäran och vilka uppgifter inhämtningsbeslutet ska innehålla. Lagen innehåller också en proportionalitetsregel. Prövningen av om ett beslut uppfyller kraven enligt lagen ska dock inte göras av domstol eller något annat oberoende organ utan av den brottsutredande myndigheten själv. En oberoende granskning sker i efterhand av SIN samt, om uppgifterna ska användas i en förundersökning, av domstol. Frågan är om ett sådant system för tillgång till de uppgifter som lagrats med stöd av tvingande regler kan anses godtagbart mot bakgrund av de påpekanden EU-domstolen har gjort. För ett närmare resonemang kring frågan om värdet av för- respektive efterhandskonstroll hänvisas till avsnitt 7.3.3 och 7.3.4.

Frågan om vem som ska ha rätt att fatta beslut om inhämtning var föremål för diskussion då lagen infördes. Regeringen anförde då att det är olika intressen som gör sig gällande i underrättelseverksamhet jämfört med under en förundersökning, där integritetsaspekten i underrättelseskedet ansågs präglas mer av ett medborgarperspektiv än av ett partsintresse (prop. 2011/12:55 s. 88 f.). Bland annat på denna grund föreslogs inte att beslut enligt inhämtningslagen skulle fattas av domstol. Det anfördes även att det kan ifrågasättas om en domstol skulle kunna tillgodose behovet av snabba beslut utanför kontorstid. Det ansågs också främmande med en ordning där åklagare involveras redan på underrättelsestadiet. Inte heller särskilda beslutsnämnder för prövning av frågan om inhämtning av uppgifter i underrättelseverksamhet ansågs vara en lämplig lösning, främst med tanke på praktiska svårigheter att på kort varsel sammankalla en sådan nämnd. I stället ansågs den lämpligaste lösningen vara att beslut om inhämtning enligt lagen skulle fattas av respektive myndighetschef, med en begränsad möjlighet till delegering (se prop. 2011/12:55 s. 123). En oberoende granskning ansågs i stället bäst göras i efterhand, genom att SIN underrättas om alla beslut fattade enligt lagen och genom nämndens kontinuerliga tillsyn.

Ett frågetecken kring de svenska reglerna i ljuset av EU-domstolens dom är naturligtvis att uppgifter hämtas in av myndigheten själv utan föregående prövning av en oberoende instans. Som framgått ovan var frågor om rättssäkerhet och integritetsskydd föremål för ingående överväganden när inhämtningslagen infördes, och det system som då beslutades ansågs uppfylla såväl dessa krav som kraven på ett praktiskt fungerande system. Lagen har varit i kraft i snart två år, och den statistik som hittills har presenterats av SIN och de brottsbekämpande myndigheterna visar att inhämtning sker i ett relativt begränsat antal ärenden och vid arbete med mycket grova brott. En jämförelse kan göras med antalet beslut om hemlig övervakning av elektronisk kommunikation, vilka under år 2013 uppgick till 3 935 stycken. Innan lagen trädde i kraft år 2012 låg antalet inhämtningar enligt rättegångsbalkens regler på ca 1 000 fall per år, medan antalet inhämtningar enligt lagen om elektronisk kommunikation uppgick till ca 9 500 fall per år (se prop. 2010/11:46 s. 70). Dessa statistiska uppgifter är inte helt jämförbara eftersom inhämtningarna enligt lagen om elektronisk kommunikation i tiden före den 1 maj 2012 avsåg både inhämtning av uppgifter om abonnemang och inhämtning av historiska trafik- och lokaliseringsuppgifter. En möjlig slutsats av detta är ändå att, även om ingen oberoende instans i förväg prövar inhämtandebesluten, så har systemet med en efterföljande tillsyn av SIN en disciplinerande effekt på myndigheternas verksamhet. Till detta kommer att det krävs ett domstolsbeslut för att uppgifter inhämtade enligt lagen ska få användas mot den enskilde i en efterföljande förundersökning. Dessa aspekter tyder enligt vår mening på att den svenska regleringen vid en helhetsbedömning uppfyller kravet på att tillgången till lagrade uppgifter är begränsad till vad som kan anses strikt nödvändigt. Vi lägger i den bedömningen också stor vikt vid att uppgifter, som ovan konstaterats, enligt inhämtningslagen kan hämtas in bara för mycket allvarlig brottslighet för vilken samhällsintresset av att brotten upptäcks är betydande.

Det kan dock finnas skäl att på nytt överväga vilken lösning för kontroll över den inhämtning som sker enligt lagen som bör gälla. Sådana överväganden är också, oberoende av domen, redan på väg. Regeringen har aviserat att den har för avsikt att låta kartlägga och

analysera inhämtningslagens tillämpning. Vidare ska undersökas om de rättssäkerhets- och integritetsstärkande åtgärder som vidtogs när lagen infördes har varit tillräckliga eller om det finns behov av andra sådana åtgärder, t.ex. införande av domstolskontroll (prop. 2013/14:237 s. 116). De frågor som har lyfts här kommer således att utredas vidare.

7.4 Lagringstiden

7.4.1 Direktivet och EU-domstolens dom

Artikel 6 i datalagringsdirektivet anger att de uppgifter som ska lagras enligt artikel 5 ska lagras under en period om minst sex månader och högst två år från det datum då kommunikationen ägde rum. Domstolen konstaterar i sin dom att lagringskravet i artikel 6 har ställts upp utan någon differentiering mellan olika kategorier av data, baserat på hur användbara uppgifterna kan tänkas vara. Inte heller anges i direktivet, med hänsyn till att medlemsstaterna har tillåtits ett tidspann på sex månader upp till två år, några objektiva kriterier som tillgodoser att lagringstiden begränsas till vad som kan anses strikt nödvändigt (punkterna 63 och 64). Nämnas kan också att Generaladvokaten i sitt yttrande i målet hade kommit till slutsatsen att en lagringstid som överstiger ett år inte kan anses proportionerlig.

7.4.2 Den svenska regleringen

När datalagringsdirektivet genomfördes i Sverige valdes en lagringstid om sex månader räknat från den dag då kommunikationen avslutades (6 kap. 16 d § LEK). Det angavs att det inte går att generellt påstå att vissa trafikuppgifter som ska lagras är mer eller mindre viktiga än andra för utredning av brott (prop. 2010/11:46 s. 37). Samma lagringstid kom därför att gälla för alla uppgifter som lagras enligt 6 kap. 16 a §.

Trafikuppgiftsutredningen hade föreslagit en generell lagringstid om ett år. Regeringen konstaterade att det sett utifrån ett brottsbekämpningsperspektiv väl kunde motiveras en lagringstid på upp till två år och att en kortare lagringstid än den utredningen

hade föreslagit skulle innebära ökad tidspress för de brottsbekämpande myndigheterna. Såväl skyddet för den personliga integriteten som kostnads-, säkerhets- och konkurrensaspekter angavs dock tala för en kortare lagringstid. Främst med hänsyn till den personliga integriteten föreslogs den kortaste lagringstid direktivet medgav, dvs. sex månader (prop. 2010/11:46 s. 38 f.).

7.4.3 Analys

Är en lagringstid om sex månader proportionerlig?

Som ovan redovisats valdes i Sverige den kortaste lagringstid direktivet tillåter för samtliga uppgiftskategorier. Av kommissionens utvärderingsrapport avseende datalagringsdirektivet från 2011[14] framgår att endast ett par andra medlemsstater vid sina respektive genomföranden valt en så kort lagringstid. Majoriteten av medlemsstaterna har i stället valt en lagringstid på mellan ett och två år.

När direktivet nu har ogiltigförklarats finns naturligtvis inte längre några EU-rättsliga krav som hindrar att en ännu kortare lagringstid än sex månader väljs. Det kan dock konstateras att för att de lagrade uppgifterna ska tjäna sitt syfte, nämligen att kunna användas för att upptäcka, utreda och lagföra allvarliga brott, måste de också finnas tillgängliga under en så pass lång tid att de brottsbekämpande myndigheterna har en reell möjlighet att hinna begära ut dem innan de raderas.

I den nyss nämnda utvärderingsrapporten från kommissionen anges viss statistik avseende åldern på de trafikuppgifter brottsbekämpande myndigheter begärt ut. Statistiken avser år 2008 och baseras på uppgifter från endast nio medlemsstater, varför dess värde i och för sig kan ifrågasättas. Men av denna går att utläsa att ca 90 procent av de uppgifter behöriga myndigheter fått tillgång till varit sex månader eller yngre. Det anges vidare att internetrelaterade uppgifter har en tendens att begäras ut i ett senare skede än uppgifter som hänför sig till telefoni samt att

[14] Rapport från kommissionen till rådet och Europaparlamentet, Utvärderingsrapport om direktiv 2006/24/EG, KOM (2011) 225 slutlig.

utredningar om särskilt grova brott tenderar att bygga på äldre uppgifter.

Vid genomförandet av direktivet i Sverige angavs exempel från Åklagarmyndigheten och Säkerhetspolisen på fall då trafikuppgifter som varit över ett år gamla varit av avgörande betydelse vid utredning och lagföring av allvarlig brottslighet (prop. 2010/11:46 s. 38).

Av uppgifter som utredningen inhämtat från Polisen framgår att uppgifter som inhämtas i underrättelseverksamheten i de flesta fall är yngre än en månad men att det även finns ärenden där historik upp till sex månader varit av stor vikt i analysarbetet. I utredningsverksamheten är den största andel uppgifter som begärs in yngre än tre månader. Uppskattningsvis 20–25 procent anges vara äldre än tre månader och cirka 10 procent av den totala mängden är äldre än fem månader. Samtidigt anges att det finns ett stort behov av att ta del av uppgifter som är äldre än tre månader, ibland även äldre än sex månader. Detta uppges särskilt gälla tidskrävande förundersökningar avseende grova våldsbrott av spaningskaraktär, dvs. förundersökningar där det initialt inte finns någon som är misstänkt. Det gäller även bekämpning av grova seriebrott såsom våldtäkter och mordförsök där det många gånger finns behov av äldre trafikdata för att kunna knyta en person till tidigare anmälda brott.

Mot bakgrund av vad som redovisats drar vi slutsatsen att en kortare lagringstid än sex månader skulle leda till att syftet med lagringen riskerade att inte kunna uppfyllas. Även om merparten av de uppgifter som hämtas in är yngre än tre månader, så finns vid utredning av de grövsta brotten ett uttalat behov av tillgång till äldre uppgifter än så. Ur ett proportionalitetsperspektiv är det naturligtvis inte acceptabelt med en lagring som tillgodoser behovet av uppgifter för att utreda mindre allvarlig brottslighet, samtidigt som uppgifter inte finns tillgängliga för att utreda grövre brott. Om en lagring för brottsbekämpande ändamål över huvud taget ska ske, måste tiden för lagringen vara sådan att det blir möjligt för de brottsbekämpande myndigheterna att använda de lagrade uppgifterna. Det ter sig i det ljuset inte rimligt att föreskriva en kortare tid än det upphävda direktivets minimitid.

Sammanfattningsvis måste därför en lagringstid om sex månader anses uppfylla det krav som EU-domstolen ställer upp och som

innebär att tiden ska begränsas till vad som kan anses strikt nödvändigt. Inga andra uttalanden i EU-domstolens dom pekar heller på att domstolen anser att en lagringstid om sex månader skulle vara att anse som oproportionerlig.

7.5 Säkerheten för de lagrade uppgifterna

7.5.1 Skyddsregler och utplåning av uppgifter

Direktivet och EU-domstolens dom

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

EU-domstolen har på flera punkter funnit direktivets skyddsregler otillräckliga (punkterna 66 och 67). Domstolen konstaterar att artikel 7 inte ställer upp säkerhetskrav som är anpassade till (i) den stora mängd data som ska lagras enligt direktivet, (ii) uppgifternas känsliga natur eller (iii) risken för att uppgifterna kommer i orätta händer, på ett sätt som kan sägas garantera att uppgifterna hålls konfidentiella. Inte heller har medlemsstaterna förpliktats att själva reglera en sådan ordning. Domstolen finner vidare att artikel 7, läst tillsammans med artikel 4.1 i direktiv 2002/58 samt artikel 17.1 i direktiv 95/46, inte ställer

krav på att en särskilt hög säkerhetsnivå upprätthålls hos leverantörerna vad gäller tekniska och organisatoriska åtgärder. Detta eftersom leverantörerna tillåts att ta ekonomiska hänsyn när de beslutar om lämplig säkerhetsnivå. Dessutom finner domstolen att direktivet inte ställer något absolut krav på att uppgifterna utplånas vid slutet av lagringstiden.

Den svenska regleringen

Vid genomförandet av direktivet i Sverige konstaterades att det i lagen om elektronisk kommunikation redan fanns regler om såväl driftsäkerhet (5 kap. 6 a §) som integritetsskydd (6 kap. 3 §). Sist nämnda bestämmelse, som genomför artikel 4.1 i direktiv 2002/58, reglerar att leverantörerna ska vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för åtgärderna, är anpassad till risken för integritetsintrång (se även avsnitt 3.2). Detta grundskydd ansågs dock inte tillräckligt för uppgifter som skulle lagras enligt datalagringsdirektivet (prop. 2010/11:46 s. 54). Det angavs, mot bakgrund av det nya syfte för vilket uppgifter skulle lagras samt den mängd uppgifter det rörde sig om, att kravet på säkerheten borde höjas samt att säkerhetsnivån borde preciseras. Resultatet blev att det infördes en ny bestämmelse i 6 kap. 3 a § LEK av vilken det framgår att den som är lagringsskyldig enligt 6 kap. 16 a § samma lag ska vidta de särskilda tekniska och organisatoriska åtgärder som behövs för att skydda de lagrade uppgifterna vid behandling. I förarbetena anges att det därav följer att bestämmelsen, till skillnad från vad som gäller enligt 6 kap. 3 § LEK, inte lämnar något utrymme att bestämma säkerhetsnivån genom en avvägning mellan teknik, kostnader och risken för integritetsintrång (prop. 2010/11:46 s. 75).

I 6 kap. 3 a § andra stycket LEK bemyndigas regeringen eller den myndighet regeringen bestämmer att komplettera lagbestämmelsen med ytterligare föreskrifter om säkerheten. Detta har för regeringens del skett i 37 § förordningen om elektronisk kommunikation. Bestämmelsen har, som ovan framgått (avsnitt 4.2), godkänts av riksdagen. Av bestämmelsen framgår att den som

är lagringsskyldig ska vidta åtgärder för att säkerställa att de lagrade uppgifterna är av samma kvalitet och föremål för samma säkerhet och skydd som vid den behandling som skett före lagringen. Vidare framgår att åtgärder ska vidtas för att skydda uppgifterna mot oavsiktlig eller otillåten förstöring och oavsiktlig förlust eller ändring samt för att förhindra otillåten lagring, behandling av eller tillgång till och otillåtet avslöjande av uppgifterna. Slutligen får uppgifterna göras tillgängliga endast för personal med särskild behörighet. PTS får efter att ha hört Rikspolisstyrelsen och Datainspektionen meddela närmare föreskrifter om de åtgärder som ska vidtas.

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

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

Analys

Är skyddet för lagrade uppgifter tillräckligt?

Som framgått ovan finns i det svenska regelverket ett antal regler om skydd för de uppgifter som lagras för brottsbekämpande ändamål som går väsentligt längre och är mer detaljerade än vad direktivet som ett minimum kräver. Frågan är om dessa regler, i ljuset av vad EU-domstolen anför, är tillräckliga.

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

Domstolen anser vidare att det säkerhetsskydd som regleras i direktivets artikel 7 på ett antal punkter är otillräckligt för att säkerställa att uppgifterna hålls skyddade. Här kan konstateras att 37 § förordningen om elektronisk kommunikation har utformats i mycket nära anslutning till artikel 7. Det skulle mot den bakgrunden, med hänsyn till EU-domstolens uttalanden, kunna ifrågasättas om enbart regleringen i 6 kap. 3 a § LEK och 37 § i förordningen ställer upp ett tillräckligt preciserat skydd för de lagrade uppgifterna. Här måste emellertid även de krav som följer av de föreskrifter som har meddelats av PTS beaktas. Dessa föreskrifter är detaljerade och reglerar såväl frågor om behörighet och åtkomst som om fysiskt skydd för den utrustning som används för att lagra uppgifterna. De reglerar även i detalj frågor om loggning, som gör det möjligt att i efterhand se vem som haft tillgång till lagrade uppgifter, samt om säkerhetskopiering. Enligt vår uppfattning kan detta sammantaget inte leda till någon annan slutsats än att det skydd som i Sverige regleras genom lag, förordning och myndighetsföreskrifter är betydligt mer omfattande och mer detaljerat än vad som följer av direktivets krav. Skyddsnivån är också betydligt högre och skyddsreglerna mer preciserade än vad som gäller de uppgifter leverantörerna har tillstånd att lagra med stöd av direktiv 2002/58. Utifrån de kriterier domstolen lyfter fram är det vår uppfattning att de svenska regler

som ska säkerställa skyddet för de lagrade uppgifterna är tillräckligt strikta och precisa. Inget som stöder en annan slutsats har heller kommit fram vid våra kontakter med PTS.

Särskilt om utplåning av uppgifter vid lagringstidens slut

En särskild säkerhetsfråga som EU-domstolen lyfter fram är frågan om utplåning av uppgifter vid lagringstidens slut. Av artikel 7(d) i datalagringsdirektivet följer att de lagrade uppgifterna ska förstöras vid slutet av lagringstiden, utom de uppgifter för vilka tillgång har medgetts och som har bevarats. Av bestämmelsens ordalydelse framstår det som om regleringen öppnar för att leverantörerna utan begränsning i tid får spara de uppgifter som väl har lämnats ut till de brottsbekämpande myndigheterna. En sådan avvikelse från huvudregeln i direktiv 2002/58 om utplåning eller avidentifiering så snart ändamålet med lagringen är uppfyllt går dock betydligt längre än vad som rimligen kan vara motiverat av syftet med datalagringsdirektivet. Som framgår ovan infördes vid det svenska genomförandet av direktivet en bestämmelse i 6 kap. 16 d § LEK som ställer krav på leverantörerna att utplåna uppgifterna vid lagringstidens utgång eller, om en begäran om utlämnande inkommit men inte hunnit behandlas, så fort uppgifterna har lämnats ut. En sådan reglering är en rimlig tolkning av artikel 7 (d) i datalagringsdirektivet. Kravet på radering innebär då ett strängare krav på leverantörerna att utplåna uppgifter än vad som följer av direktiv 2002/58.

När det sedan gäller det fortsatta bevarandet hos de brottsbekämpande myndigheterna av uppgifter som har lämnats ut finns det av naturliga skäl ingen bestämd frist föreskriven för hur länge uppgifterna får bevaras. Därmed inte sagt att det helt saknas reglering om detta bevarande.

Frågan om utplåning av uppgifter som inhämtats genom hemlig övervakning av elektronisk kommunikation regleras i första hand i 27 kap. 24 § rättegångsbalken. Av bestämmelsens andra stycke följer att uppgifter som är av betydelse från brottsutredningssynpunkt ska bevaras till dess förundersökningen lagts ner eller avlutats eller, om åtal har väckts, till dess målet slutligt har avgjorts. I de delar uppgifterna är av betydelse för att

förhindra förestående brott ska de bevaras så länge de behövs och därefter förstöras. Av bestämmelsens fjärde stycke följer att brottsutredande myndigheter, trots vad som sägs i andra stycket, får behandla uppgifter i enlighet med vad som är särskilt föreskrivet i lag. Med denna skrivning avses att, om det i exempelvis polisdatalagen finns särskilda regler om hur uppgifter får behandlas, så kan detta gälla även nu aktuella uppgifter. Bestämmelser om utplåning av uppgifter som inhämtats på underrättelsestadiet finns i 9 § inhämtandelagen. Regleringen motsvarar den som finns i rättegångsbalken. För utplåning av abonnemangsuppgifter som inhämtats av brottsbekämpande myndigheter med stöd av 6 kap. 22 § andra stycket 2 LEK finns inga särskilda regler, utan reglerna om gallring i exempelvis polisdatalagen gäller.

Frågan om vid vilken tidpunkt material som inhämtats med stöd av ett hemligt tvångsmedel ska förstöras har varit föremål för utredning och diskussion vid ett antal tillfällen (se t.ex. prop. 2004/05:143 s. 44 och prop. 2013/14:237 s. 159). I den senare propositionen redovisas att åklagarens skyldighet att kontinuerligt sortera ut material som saknar relevans kan kollidera med den misstänktes rätt att få ut materialet. Det följer nämligen av Europadomstolens praxis att förstörandet av material från hemliga tvångsmedel innan en rättegång är avslutad i vissa fall kan kränka den misstänktes rätt till en rättvis rättegång (se Europadomstolens domar i målen *Natunen mot Finland*, nr 21022/04, och *Janatuinen mot Finland*, nr 28552/05, vilka båda avsåg material som inhämtats vid hemlig avlyssning).

Mot den givna bakgrunden och särskilt med beaktande av Europadomstolens uttalanden, är det uteslutet att EU-domstolen med sin skrivning har avsett att det även borde finnas regler om utplåning av lagrade trafikuppgifter vid lagringstidens slut hos de brottsbekämpande myndigheterna. Ett krav på utplåning av uppgifterna vid en viss bestämd tidpunkt, utan att hänsyn tas till var i processen ett ärende befinner sig, skulle kunna kränka den misstänktes rätt till en rättvis rättegång enligt artikel 47 i rättighetsstadgan och artikel 6 i Europakonventionen.

Sammanfattningsvis är vi av uppfattningen att regleringen i 6 kap. 16 d § LEK om utplåning av uppgifter vid lagringstidens slut

hos leverantören uppfyller de krav på ett oåterkalleligt förstörande av uppgifterna som EU-domstolen efterlyser.

7.5.2 Krav på lagring i EU

Den svenska regleringen

Datalagringsdirektivet innehåller inte några bestämmelser om var trafikuppgifter får lagras. Något krav på att uppgifterna ska lagras inom unionen ställs alltså inte upp. Inte heller direktiv 2002/58 innehåller några regler om var lagringen av uppgifter ska ske. I den utsträckning trafikuppgifterna är personuppgifter kan den allmänna dataskyddsregleringen dock påverka i vilken mån det är möjligt att överföra trafikuppgifter till andra länder.

Vid genomförandet av datalagringsdirektivet konstaterade regeringen att det på området för elektronisk kommunikation finns tjänsteleverantörer som är verksamma samtidigt i flera länder och att direktivet inte ger utrymme för att begränsa leverantörernas möjlighet att lagra trafikuppgifter som har genererats i Sverige i något annat EU-land (prop. 2010/11:46 s. 58 f.). Bedömningen av vilket utrymme som finns att begränsa möjligheterna att föra över uppgifter till andra länder av hänsyn till enskildas personliga integritet måste i stället göras utifrån den generella regleringen i dataskyddsdirektivet och de bestämmelser som gäller för den inre marknaden på området för elektronisk kommunikation i direktiv 2002/58.

Enligt 6 kap. 16 a § LEK är den som bedriver sådan verksamhet som är anmälningspliktig enligt 2 kap. 1 § LEK lagringsskyldig i Sverige när det gäller vissa slags uppgifter. En leverantör som är etablerad och bedriver verksamhet i något annat EU-land är inte anmälningspliktig i Sverige och följaktligen inte heller skyldig att lagra trafikuppgifter enligt den svenska lagstiftningen. Om en sådan leverantör ändå av någon anledning väljer att i Sverige lagra trafikuppgifter som genereras och behandlas i det företagets verksamhet, blir bestämmelserna i personuppgiftslagen inte tillämpliga på den lagring av personuppgifter som sker i landet eftersom den lagens tillämpningsområde inte omfattar personuppgiftsansvariga som är etablerade i någon annan stat som ingår i EU. För lagringen gäller i stället de bestämmelser, bl.a.

kraven i fråga om datasäkerhet, som genomför dataskyddsdirektivet och direktiv 2002/58 i etableringslandet. På motsvarande sätt är en leverantör som bedriver anmälningspliktig verksamhet i Sverige skyldig att tillämpa de krav som gäller för lagringen av trafikuppgifterna enligt svenska författningar, även om uppgifterna förs över till något annat land och lagras där (prop. 2010/11:46 s. 59).

Regleringen om överföring till tredjeland

Den EU-rättsliga regleringen

Av artikel 1 i direktiv 95/46 framgår att medlemsstaterna inte får begränsa det fria flödet av personuppgifter mellan medlemsstaterna med hänvisning till skäl som rör den enskildes personliga integritet. En reglering som hindrar en leverantör i Sverige från att lagra uppgifter i en annan medlemsstat i EU skulle uppenbarligen kunna påverka leverantörens konkurrenskraft i förhållande till andra leverantörer på den inre marknaden och skulle även komma i konflikt med ett av de uttryckliga syftena med dataskyddsdirektivet.

När det gäller utrymmet att begränsa möjligheterna till överföring av uppgifter till tredjeland kan vidare konstateras att det av regleringen i dataskyddsdirektivet framgår att sådan överföring i princip ska vara tillåten om den avser ett land som erbjuder en adekvat skyddsnivå för uppgifterna. Om kommissionen med stöd av artikel 25.6 i dataskyddsdirektivet har beslutat att ett tredjeland, genom sin interna lagstiftning eller på grund av sina internationella åtaganden, har en adekvat skyddsnivå, ska medlemsstaterna vidta åtgärder för att följa beslutet. I Sverige har kommissionens beslut om adekvat skyddsnivå genomförts genom föreskrifter i en bilaga till personuppgiftsförordningen. Av dessa framgår bl.a. att länder som Andorra, Argentina, Israel, Nya Zealand, Schweiz och Uruguay erbjuder en adekvat skyddsnivå för överförda personuppgifter. Av regleringen följer även att överföring till privata företag i USA som åtagit sig att följa de s.k. Safe Harbour Privacy Principles är tillåten enligt kommissionens beslut. Överföringar är också tillåtna till Kanada, om mottagaren omfattas av landets lagstiftning om skydd av personuppgifter. Tillämpningen

av dessa beslut har dock ifrågasatts av bl.a. Europaparlamentet som i kölvattnet av avslöjandena om den amerikanska försvarsunderrättelsemyndigheten NSA:s (National Security Agency) övervakning av elektronisk kommunikation har antagit en resolution som uppmanar kommissionen att omedelbart upphäva Safe Harbour-beslutet och överväga detsamma när det gäller besluten rörande Kanada och Nya Zealand.[15]

Det är inte självklart att medlemsstaterna har stöd i unionsrätten för att genom nationella föreskrifter eller administrativa beslut i enskilda fall åsidosätta kommissionens beslut om adekvat skyddsnivå och därigenom förhindra överföring till ett tredjeland som omfattas av ett adekvansbeslut. Om medlemsstaterna antas ha befogenhet att generellt förbjuda vissa överföringar av personuppgifter till länder som ansetts erbjuda en adekvat skyddsnivå, skulle de mekanismer som inrättats för att tillgodose marknadens intresse av harmoniserade villkor lätt kunna kringgås.

I den aktuella situationen handlar det dock inte om att överväga nationella föreskrifter som innebär ett generellt åsidosättande av kommissionens beslut om adekvat skyddsnivå i tredjeland. Vad det handlar om är i stället att ta ställning till om det finns utrymme för att i nationell rätt, när det gäller en viss typ av noggrant avgränsad lagring av personuppgifter, inskränka möjligheterna till överföring med hänsyn till att säkerhetskraven måste ställas så högt att en lagring i tredjelandet inte kan godtas trots att landet generellt ansetts erbjuda en adekvat skyddsnivå.

Risk för ändamålsglidning

Det finns inte några generella hinder mot att en leverantör anlitar ett s.k. personuppgiftsbiträde (en registerförare enligt dataskyddsdirektivets terminologi) som får i uppdrag att lagra uppgifterna för leverantörens räkning. Biträdet kan finnas i Sverige eller i något annat land. Ett arrangemang av sådant slag förutsätter dock att biträdet kan garantera att de för verksamheten gällande säkerhetskraven upprätthålls. Om överföringen är tänkt att ske till

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

ett land utanför EU och EES, krävs vidare att mottagarlandet har en adekvat skyddsnivå för personuppgifterna eller att tillräckliga garantier för enskildas grundläggande rättigheter kan säkerställas på annat sätt.

En leverantör som är lagringsskyldig i Sverige och som väljer att förlägga lagringen av trafikuppgifter utomlands undgår givetvis inte på den grunden skyldigheten att lämna ut uppgifter enligt föreskrifter i rättegångsbalken och annan lag. I den utsträckning en leverantör väljer att i egen regi lagra uppgifterna på en server som finns på en annan stats territorium – dvs. inom en annan stats jurisdiktionsområde – kan det dock hända att företaget därutöver blir tvungen att lämna ut trafikuppgifter till utländska myndigheter som begär tillgång till dessa med stöd av lagstiftningen i lagringslandet. Om leverantören i stället har anlitat ett personuppgiftsbiträde för lagring av uppgifterna i en annan stat, kan det inte heller uteslutas att biträdet åläggs en skyldighet enligt den statens lagstiftning att lämna ut uppgifter till myndigheterna i biträdets hemstat. Ett biträde kan nämligen inte värja sig mot förpliktelser som följer av lag genom att hänvisa till att uppgifter får hanteras endast på instruktion av den registeransvarige.

Det förhållandet att ändamålen för behandling är strängt begränsade enligt 6 kap. 16 c § LEK kan inte antas få till följd att en leverantör måste kunna garantera att tillgången till uppgifter begränsas på det sätt som framgår av denna reglering för att kravet på konfidentialitet ska vara uppfyllt. Ett annat synsätt skulle nämligen förutsätta att man accepterar att den nationella lagstiftaren kan begränsa det fria flödet av personuppgifter även inom EU genom att i författning slå fast preciserade ändamål för utlämnande. Detta skulle dock strida mot ett av de grundläggande syftena med dataskyddsdirektivet som kommer till uttryck i artikel 1 i direktivet. Utöver den begränsning som följer av att samtliga medlemsländer i EU har rättsregler för dataskydd som bygger på EU-direktiv kan, som Trafikuppgiftsutredningen konstaterade (SOU 2007:76 s. 197), några garantier därför inte ställas för att uppgifter som lagras i ett annat EU-land inte där används för andra ändamål än de som den svenska lagstiftningen medger.

Det sagda innebär alltså att det inte kan uteslutas att uppgifter som lagras med stöd av svensk lagstiftning enbart för ändamål som rör bekämpning av vissa närmare avgränsade typer av brott skulle

kunna komma till användning i annan verksamhet eller för bekämpning av andra typer av brott om uppgifterna förs över för lagring i en annan stat. I vilken mån lagrade uppgifter kan komma att spridas för användning i vidare utsträckning än vad som medges enligt svensk lag blir i dessa fall helt beroende av lagstiftningen i lagringslandet.

Ett rimligt antagande är att riskerna för s.k. ändamålsglidning generellt sett torde öka om lagringen sker i ett tredjeland än om det sker inom EU eller EES. Riskerna torde vidare vara högre i länder som inte har en adekvat skyddsnivå till följd av sin nationella lagstiftning och administrativa praxis än i tredjeländer som anses ha en sådan skyddsnivå. En berättigad fråga är därför om det inte finns skäl att genom generella föreskrifter utesluta möjligheten för leverantörerna att överföra trafik- och lokalieringsuppgifter till tredjeland för lagring där.

Analys

EU-domstolen menar att avsaknaden av regler i datalagringsdirektivet som begränsar utrymmet för överföring av trafikuppgifter utanför EU innebär att den i artikel 8.3 i rättighetsstadgan uttryckligen föreskrivna oberoende myndighetskontrollen av att skydds- och säkerhetskraven följs inte fullt ut kan garanteras (punkt 68). En sådan kontroll är enligt EU-domstolen en grundläggande beståndsdel i skyddet för enskilda individer i samband med behandlingen av personuppgifter.[16] Domstolen har också i tidigare avgöranden betonat tillsynsmyndigheternas avgörande betydelse för skyddet av enskilda personer med avseende på behandlingen av personuppgifter genom sin oberoende tillsyn över att dataskyddsregleringen följs.[17]

Mot bakgrund av de uttalanden som EU-domstolen gör i datalagringsdomen om intresset av effektiv tillsyn är det mycket som talar för att det bör införas ett krav på att trafikuppgifter som genereras eller behandlas vid användningen av allmänna kommunikationsnät och elektroniska kommunikationstjänster som

[16] Se även *Europeiska kommissionen mot Republiken Österrike*, C-614/10, punkt 37.
[17] Se *Europeiska kommissionen mot Förbundsrepubliken Tyskland*, C‑518/07, punkt 23

är anmälningspliktiga i Sverige och omfattas av lagringsskyldigheten enligt 6 kap. 16 a § LEK ska ske inom EU eller EES. Detta skulle t.ex. kunna göras genom ett särskilt förbud mot överföring av sådana trafikuppgifter till ett tredjeland för lagring där. En reglering som innebär att leverantörerna förbjuds att överföra trafikuppgifter för lagring i ett tredjeland skulle visserligen komma i konflikt med den generella regleringen på detta område, främst kommissionens beslut om adekvat skyddsnivå. Vi bedömer dock att medlemsstaterna kan rättfärdiga ett överföringsförbud med hänvisning till att den aktuella lagringen till sin art, omfattning och varaktighet innefattar ett så långtgående ingrepp i enskildas personliga integritet att kraven på säkerhet vid lagringen förutsätter att uppgifterna inte förs över till ett tredjeland.

Såvitt vi erfarit lagrar de svenska leverantörerna inte trafik- och lokaliseringsuppgifter utanför EU eller EES. En förbudsbestämmelse skulle därför knappast få några direkta konsekvenser för leverantörernas verksamhet. Men avsaknaden av ett förbud mot lagring av uppgifter i tredjeland kan enligt vår uppfattning inte heller anses innebära att regleringen i svensk lag i sig strider mot bestämmelserna om grundläggande rättigheter i EU.

7.6 Samlad bedömning

EU-domstolen har i sin dom redogjort för i huvudsak fyra punkter där datalagringsdirektivets reglering har funnits vara bristfällig eller på annat sätt kunnat kritiseras. Den första punkten avser lagringsskyldighetens generella omfattning, den andra avsaknaden av regler som begränsar tillgången till de lagrade uppgifterna, den tredje avser lagringstiden och den fjärde punkten avser säkerheten för uppgifterna. Som påtalats vid ett flertal tillfällen är det vid en *samlad bedömning* av de utpekade omständigheterna som EU-domstolen kommer fram till att direktivet innebär ett oproportionerligt ingrepp i de rättigheter som anges i artiklarna 7 och 8 i rättighetsstadgan. Domen kan med andra ord inte tolkas så att domstolen har redovisat en lista på åtgärder som i alla delar måste vara vidtagna för att regleringen inte ska anses oproportionerlig. På samma sätt som i domen avser vi att mot

bakgrund av den analys som presenterats ovan göra en samlad bedömning av det svenska regelverkets förenlighet med unionsrätten.

Det har i analysen konstaterats att de trafik-, lokaliserings- och abonnemangsuppgifter som lagras enligt reglerna i 6 kap. 16 a–f §§ LEK samtliga är integritetskänsliga. Graden av integritetsintrång kan dock variera beroende på typen av uppgifter. Det har vidare konstaterats att nyttan av uppgifterna för att kunna förhindra, förebygga, upptäcka, utreda och lagföra brott är stor. Vissa typer av brott skulle i praktiken vara omöjliga att bekämpa utan tillgång till de aktuella uppgifterna. Det är således dessa båda angelägna intressen – skyddet för den personliga integriteten och intresset av att bekämpa brott – som måste balanseras för att åtgärden att lagra uppgifter ska kunna anses proportionerlig.

Vad inledningsvis gäller lagringsskylighetens omfattning har av de uppgifter vi inhämtat framgått att behovet såvitt gäller ett fåtal av de uppgiftskategorier som lagras kan ifrågasättas. Det finns anledning att titta närmare på detta i det fortsatta arbetet. Den absoluta merparten av de uppgiftskategorier som lagras är emellertid viktiga, i vissa fall till och med helt avgörande, för att bekämpa brott.

Skyldigheten att lagra uppgifter enligt de svenska reglerna är generell, dvs. lagringen sker utan att det på förhand har konstaterats att uppgifterna kan vara intressanta för att bekämpa brott. Vi har funnit att en begränsning av lagringsskyldighetens omfattning svårligen kan göras utan mycket negativa effekter för brottsbekämpningen. Vi har vidare funnit att enbart det faktum att lagringsskyldigheten är generell inte gör att den kan anses oproportionerlig, utan frågan om lagringen kan anses proportionerlig avgörs av om *tillgången* till uppgifterna är tillräckligt strikt reglerad och om uppgifterna kan anses tillräckligt skyddade.

Till skillnad från datalagringsdirektivet innehåller svensk rätt en omfattande reglering av när och hur de brottsbekämpande myndigheterna kan få tillgång till uppgifter som lagras enligt 6 kap. 16 a–f §§ LEK. Tillgångsregleringen är spridd på tre olika regelverk; regler om inhämtning av abonnemangsuppgifter finns i 6 kap. 22 § första stycket 2 LEK, regler om inhämtning av trafik- och lokaliseringsuppgifter under pågående förundersökning i

27 kap. 19 § RB och regler om inhämtning av trafik- och lokaliseringsuppgifter i underrättelseverksamhet i inhämtningslagen.

Vad inledningsvis gäller reglerna om inhämtning i rättegångsbalken har vi funnit att dessa utan tvekan uppfyller unionsrättens krav på en begränsning till vad som kan anses strikt nödvändigt.

Vad vidare gäller inhämtningen av abonnemangsuppgifter har vi funnit att det kan finnas utrymme för vissa rättssäkerhetsstärkande åtgärder såvitt avser tillsynen över inhämtningen. Den nuvarande regleringen torde dock enligt vår bedömning rymmas inom ramen för vad som är godtagbart enligt unionsrätten.

Vad slutligen avser den tillgång till uppgifter som regleras i inhämtningslagen har vi konstaterat att det finns utrymme för tvekan inför ställningstagandet till att denna reglering fullt ut uppfyller unionsrättens krav. Uppgifter inhämtas utan någon föregående kontroll av vare sig domstol eller någon annan oberoende instans. Vid en samlad bedömning har vi emellertid funnit att den svenska regleringen, trots denna brist, på en tillräckligt hög nivå för att det ska anses proportionerligt tillser att de uppgifter som omfattas av lagringsskyldigheten lämnas ut bara när det kan anses nödvändigt. I denna bedömning har vi särskilt beaktat att inhämtning enligt lagen sker bara för mycket allvarliga brott, att beslut om inhämtning fattas av myndighetschef med snäva delegationsmöjligheter, att en tillsyn sker i efterhand av SIN samt – inte minst – att uppgifterna måste passera en domstolskontroll för att kunna användas mot den enskilde i en förundersökning. Vi har samtidigt konstaterat att unionsrätten och europarätten endast anger en miniminivå för integritetsskydd och att Sverige bör sträva efter att uppfylla sådana krav med marginal. Det finns därför goda skäl för den kartläggning och analys av lagen som regeringen redan har aviserat för att underöka om integritetsskyddet bör förbättras.

Vidare har vi, såvitt avser lagringstiden, funnit att en lagringstid om sex månader måste anses uppfylla kravet på en begränsning till vad som är strikt nödvändigt.

Slutligen har vi funnit att det skydd för lagrade uppgifter som garanteras genom det svenska regelverket är tillräckligt högt. Vi har konstaterat att det svenska regelverket visserligen inte ställer upp

något uttryckligt krav på att uppgifterna måste lagras inom EU/EES och att denna fråga kan behöva utredas vidare, men att de i Sverige anmälningspliktiga leverantörerna såvitt vi kunnat erfara inte lagrar uppgifter utanför detta område i dag. Vi har också dragit slutsatsen att avsaknaden av förbud mot lagring i tredjeland inte medför att svensk rätt på denna grund inte uppfyller unionsrättens krav.

Sammanfattning

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

Dessa åtgärder skulle verka för att ytterligare stärka rättssäkerheten och integritetsskyddet i den svenska regleringen Det är emellertid vår samlade bedömning att det svenska regelverket avseende lagring enligt 6 kap. 16 a–f §§ LEK samt övriga bestämmelser om tillgång och behandling av sådana uppgifter, även utan sådana åtgärder och med beaktande av EU-domstolens uttalanden, inte strider mot unionsrätten eller europarätten.

Uppdraget

Uppdrag med anledning av EU-domstolens dom om datalagringsdirektivet

Bakgrund

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 (datalagringsdirektivet) syftar till att harmonisera medlemsstaternas regler om skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra trafik- och lokaliseringsuppgifter samt uppgifter som behövs för att identifiera en abonnent eller användare för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal av allvarliga brott.

Datalagringsdirektivet skulle ha genomförts i medlemsstaterna i huvudsakliga delar senast den 15 september 2007. Sverige hade vid denna tidpunkt emellertid inte genomfört direktivet i nationell lagstiftning. EU-kommissionen väckte överträdelsetalan mot Sverige. EU-domstolen ålade Sverige att betala böter för det försenade genomförandet.

Datalagringsdirektivet genomfördes slutligen i svensk rätt genom lagstiftning som trädde i kraft den 1 maj 2012. Bestämmelserna om lagring finns i lagen (2003:389) om elektronisk kommunikation

(prop. 2010/11:46, bet. 2011/12:JuU28, rskr. 2011/12:166). Bestämmelser om utlämnande av trafikuppgifter till brottsbekämpande myndigheter finns i bl.a. rättegångsbalken och lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (underrättelselagen; prop. 2011/12:55, bet. 2011/12:JuU8, rskr. 2011/12:213). Vid utarbetandet av dessa bestämmelser lade regeringen stor vikt vid skyddet för den personliga integriteten.

EU-domstolens dom

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

I domen slår EU-domstolen fast att direktivet innebär ett omfattande och särskilt allvarligt intrång i rätten till privatliv och skyddet av personuppgifter. Domstolen konstaterar dock att en skyldighet att lagra uppgifter är en ändamålsenlig åtgärd för att uppnå syftet att bekämpa allvarlig brottslighet och upprätthålla allmän säkerhet, vilket skulle kunna motivera ett intrång i rättigheterna. Eftersom direktivet i vissa avseenden inte fastställer tydliga och preciserade regler för omfattningen av intrånget i de aktuella rättigheterna begränsas emellertid inte direktivet till vad som är absolut nödvändigt för att uppnå syftet. Domstolen har därför vid en samlad bedömning funnit att EU:s lagstiftande församlingar överskridit sina befogenheter då direktivet antogs eftersom det inte lever upp till proportionalitetsprincipen med avseende på artiklarna 7, 8 och 52.1 i EU:s stadga om de grundläggande rättigheterna (EU-stadgan).

I nära anslutning till domen meddelade flera operatörer av allmänna elektroniska kommunikationsnät att de gjorde bedömningen att den svenska lagstiftning som genomfört direktivet står i strid med EU-rätten och att de därför inte avsåg att fortsättningsvis lagra uppgifter enligt 6 kap. lagen (2003:389) om elektronisk

kommunikation (Ju2014/2665/BIRS). Några operatörer ansåg även att lagrade uppgifter skulle raderas. Operatörerna önskade samtidigt besked från Post- och telestyrelsen (PTS) om vilken bedömning myndigheten gjorde av domen. PTS har på sin webbplats angett att ”PTS kommer i nuläget inte att vidta några åtgärder utifrån datalagringsreglerna” vilket kan tolkas som att PTS inte längre ser någon möjlighet att utöva sitt tillsynsansvar enligt 7 kap. lagen om elektronisk kommunikation i fråga om de bestämmelser som genomför datalagringsdirektivet. Med detta som utgångspunkt har flera operatörer kommit till slutsatsen att det inte finns något rättsligt stöd för att lagra trafikuppgifter.

Förutsättningarna för en myndighet att inte tillämpa en bestämmelse i svensk lag är att bestämmelsen i den lagen strider mot svensk grundlag eller mot unionsrätten. Om bestämmelsen strider mot grundlag ska myndigheten avstå från att tillämpa den i enlighet med de förutsättningar som anges i 12 kap. 10 § regeringsformen (lagprövning). Om en bestämmelse i lag i stället strider mot unionsrätten följer av unionsrättens överordnade ställning i förhållande till nationell rätt att nationella myndigheten har en på unionsrätten grundad skyldighet att inte tillämpa bestämmelsen. Om innebörden av unionsrätten inte är alldeles klar ligger det i EU-domstolens hand att slutligt avgöra vad som följer av denna och vilka begränsningar bl.a. EU-stadgan innebär. Det är bara en nationell domstol som har rätt att begära ett tolkningsbesked genom ett förhandsavgörande av EU-domstolen.

Kommissionen har i anslutning till kommissionär Malmströms pressmeddelande med anledning av domen, uttalat att nationell rätt behöver ändras endast i den utsträckning den är oförenlig med unionsrätten, dvs. domen innebär inte med automatik att den nationella lagstiftning som genomför direktivet i de olika medlemsstaterna därmed också är ogiltig. Kommissionen har även uttalat att den kommer att noggrant analysera domen och dess konsekvenser. Kommissionen kommer vidare att beakta domstolens utslag samt förhandlingarna om ett nytt ramverk för dataskydd i sitt fortsatta arbete med revideringen av direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation

(direktiv om integritet och elektronisk kommunikation). Europaparlamentets rättstjänst har, vid LIBE-kommitténs sammanträde den 10 april 2014, förklarat att nationell lagstiftning som genomför direktivet inte automatiskt blir ogiltig i och med domen.

Konsekvenser för de brottsbekämpande myndigheternas verksamhet

I utredningen Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38), som är ett delbetänkande av Beredningen för rättsväsendets utveckling (BRU), beskrivs behovet av tillgång till trafikuppgifter på följande sätt: ”Vid utredningar av grövre brott används trafikuppgifter på något sätt i nästan samtliga fall. Tillgången till uppgifterna är av fundamental betydelse för brottsutredningsverksamheten och har ofta en direkt koppling till att förundersökningar över huvud taget kan föras framåt.” Den slutsatsen delas av utredningen Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76).

Enligt Rikspolisstyrelsen bidrar trafikuppgifter ofta väsentligt till att kunna ringa in misstänkta, kartlägga planläggning av brott etc., men även till att avfärda någon från misstankar. Det handlar alltså om att kunna lösa sådana grova brott som mord, våldtäkt, grovt narkotikabrott, grov misshandel, människohandel, olaga hot (grovt brott), mordbrand, grov stöld, m.m. För internetrelaterad brottslighet, exempelvis barnpornografibrott, grooming och näthat, är utgångsläget ofta att trafikuppgifter är det enda sätt som polisen kan komma en misstänkt på spåren. Trafikuppgifter kan också enligt styrelsen vara livsavgörande vid räddningsinsatser och nödsituationer, t.ex. för att hitta en försvunnen person.

Utgångspunkter

Var och en är gentemot det allmänna enligt grundlag skyddad mot bl.a. avlyssning och intrång i förtroliga meddelanden och även i övrigt mot vissa andra betydande intrång i den personliga integriteten (2 kap. 6 § regeringsformen). Begränsningar i skyddet

får endast göras genom lag. De måste motiveras av ett ändamål som är godtagbart i ett demokratiskt samhälle och får inte gå längre än vad som är nödvändigt för att uppnå syftet med begränsningen (2 kap. 20 och 21 §§ regeringsformen). Av artikel 8 i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen), som gäller som lag i Sverige, följer vidare att var och en har rätt till respekt för sitt privat- och familjeliv och sin korrespondens. Begränsningar i denna rättighet får göras bl.a. för att förebygga oordning och brott. En begränsning får dock göras bara om den är nödvändig i ett demokratiskt samhälle. Det innebär att den måste motiveras av ett angeläget allmänt intresse och inte får gå utöver vad som behövs för att uppnå sitt syfte. Av regeringsformen följer att en föreskrift i lag eller annan författning inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.

Rätten till respekt för privatlivet slås även fast i artikel 7 i EU-stadgan. Enligt artikel 8 i EU-stadgan har var och en vidare rätt till skydd för sina personuppgifter. Skyddet innefattar bl.a. ett krav på att behandlingen av personuppgifter måste ha stöd i en legitim och lagenlig grund och att en oberoende myndighet ska utöva tillsyn över att reglerna om behandling av personuppgifter följs. Av artikel 6.1 fördraget om Europeiska unionen följer att EU-stadgan har samma rättsliga värde som fördragen.

Enligt artikel 51.1 i EU-stadgan riktar sig denna till medlemsstaterna endast när dessa tillämpar unionsrätten. EU-domstolen har dock slagit fast att detta innebär att de grundläggande rättigheterna måste iakttas inte bara vid tillämpningen av genomförandelagstiftning utan så snart nationell lagstiftning omfattas av unionsrättens tillämpningsområde (EU-domstolens dom den 26 februari 2013 i mål C-617/10 Åkerberg Fransson). Enligt artikel 52.3 i EU-stadgan ska de rättigheter i stadgan som motsvarar sådana som garanteras av Europakonventionen ha samma innebörd och räckvidd som i konventionen.

EU-domstolen har underkänt datalagringsdirektivet på grund av att det strider mot kravet på proportionalitet enligt artikel 52.1 i EU-stadgan. Ställningstagandet görs efter en samlad bedömning av regleringen i direktivet. Domstolen har inte uttalat sig om huruvida de nationella bestämmelserna som genomför direktivet är förenliga med unionsrätten. Domstolens ställningstagande innebär inte med automatik att nationell reglering som genomför direktivet inte uppfyller unionsrättens krav på proportionalitet.

När datalagringsdirektivet genomfördes i Sverige infördes skyldigheten att lagra de aktuella uppgifterna i 6 kap. lagen (2003:389) om elektronisk kommunikation. Regeringen lade vid framtagandet av lagen stor vikt vid balansen mellan intresset av en effektiv brottsbekämpning och intresset av skyddet för den personliga integriteten. Bland annat resulterade denna avvägning i att lagen kom att reglera en lagringstid som ligger på den miniminivå direktivet krävde, dvs. sex månader. Lagringsskyldigheten kompletterades också med regler om tillsyn och om skydd för de lagrade uppgifterna och med ett krav på att lagrade uppgifter ska raderas vid lagringstidens slut, vilka samtliga går längre än vad som anges i direktivet. Vidare infördes bestämmelser som syftade till att ytterligare stärka skyddet för de lagrade uppgifterna. PTS bemyndigades därutöver att meddela föreskrifter om skyddsåtgärder i detta avseende. Lagändringarna antogs av riksdagen med kvalificerad majoritet och trädde i kraft den 1 maj 2012. I regeringens proposition gjordes bedömningen att reglerna sammantaget var förenliga med såväl svensk grundlag som Europakonventionen.

Den 1 juli 2012 trädde också förändringar i regelverket kring tillgången till trafikuppgifter i kraft som syftade till att stärka rättssäkerheten och integritetsskyddet, bl.a. är det tydligt angivet under vilka förutsättningar uppgifter får lämnas ut och hur sådana beslut ska fattas.

Sedan datalagringsdirektivet upphävts har medlemsstaterna i princip samma behörighet att besluta om nationell lagstiftning rörande lagring av trafikdata som innan direktivet antogs. Bedömningen av om EU-stadgans krav är uppfyllda i samband med

att nationell lagstiftning antas inom ramen för unionsrättens tillämpningsområde förutsätter att en samlad bedömning görs av den svenska lagstiftningen som helhet. Efter-som EU-stadgans bestämmelser ska ha samma innebörd som Europakonventionens motsvarande bestämmelser måste utgångspunkten vid bedömningen av gränserna för medlemsstaterans nationella beslutande-rätt på unionsrättens tillämpningsområde tas i praxis från såväl EU-domstolen som Europadomstolen för mänskliga rättigheter.

Uppdraget

En utredare ska, i ljuset av EU-domstolens dom, grundligt analysera reglerna om lagring av uppgifter enligt 6 kap. 16 a–f §§ lagen om elektronisk kommunikation, samt övriga bestämmelser om tillgång och behandling av sådana uppgifter, och deras förhållande till unionsrätten.

Utredaren ska föreslå de ändringar som han finner lämpliga för att stärka skyddet för den personliga integriteteten samt, om resultatet av analysen visar på brister i förhållande till unionsrätten, för att leva upp till unionsrättens krav. Utredaren ska lämna de fullständiga författningsförslag som krävs för sådana ändringar. I utformningen av sådana regler ska utredaren även beakta de brottsbekämpande myndigheternas behov av aktuella uppgifter.

Utredaren ska i analysen enligt första stycket inhämta särskild sakkunskap om unionsrätten jämte internationell rätt avseende mänskliga rättigheter från professor Iain Cameron. Utredaren ska vid genomförandet av uppdraget samråda med Åklagarmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Tullverket och PTS.

Redovisning av uppdraget

Analysen ska redovisas senast den 12 juni 2014. Uppdraget i övrigt ska redovisas senast den 1 oktober 2014.