Lagring av trafikuppgifter för brottsbekämpning

Betänkande av Trafikuppgiftsutredningen

Stockholm 2007

STATENS OFFENTLIGA UTREDNINGAR

SOU 2007:76

SOU och Ds kan köpas från Fritzes kundtjänst. För remissutsändningar av SOU och Ds svarar Fritzes Offentliga Publikationer på uppdrag av Regeringskansliets förvaltningsavdelning.

Beställningsadress:
Fritzes kundtjänst
106 47 Stockholm
Orderfax: 08-690 91 91
Ordertel: 08-690 91 90
E-post: order.fritzes@nj.se
Internet: www.fritzes.se

Svara på remiss. Hur och varför. Statsrådsberedningen, 2003.
– En liten broschyr som underlättar arbetet för den som skall svara på remiss. Broschyren är gratis och kan laddas ner eller beställas på http://www.regeringen.se/remiss

Grafisk formgivning: Susan Nilsson, Jupiter Reklam AB

Tryckt av Edita Sverige AB
Stockholm 2007

ISBN 978-91-38-22818-0
ISSN 0375-250X

Till statsrådet och chefen för Justitiedepartementet

Genom beslut den 18 maj 2006 bemyndigade regeringen chefen för Justitiedepartementet att tillkalla en särskild utredare med uppdrag att lämna förslag till hur EG:s direktiv (2006/24/EG) om lagring av trafikuppgifter ska genomföras i svensk rätt.

Särskild utredare har varit generaldirektören vid Ekobrottsmyndigheten Gudrun Antemar.

Sakkunniga i arbetet har varit juristen Per Bergstrand (Post- och telestyrelsen), ämnesrådet Per Lagerud (Justitiedepartementet), datarådet Hans-Olof Lindblom (Datainspektionen) och numera kammarrättspresidenten Margareta Åberg (Kammarrätten i Sundsvall).

Experter i arbetet har varit kriminalinspektören Carina Axelsson Palmer (Rikskriminalpolisen), rättssakkunniga Helene Bergström (Justitiedepartementet) från mars 2007, kanslirådet Carina Bring Sjögren (Justitiedepartementet) till mars 2007, kanslirådet Mattias Broman (Försvarsdepartementet), projektledaren Fredrik von Essen (IT & Telekomföretagen, Svenskt Näringsliv) från juni 2007, advokaten Per Furberg (Sveriges Advokatsamfund), departementssekreteraren Martin Gynnerstedt (Näringsdepartementet) till september 2006, verkställande direktören Ylva Hambraeus Björling (IT-företagen, Svenskt Näringsliv) till juni 2007, ämnessakkunniga Maria Häll (Näringsdepartementet) från augusti 2007, chefsjuristen Lars-Åke Johansson (Säkerhetspolisen), numera vice chefsåklagaren Katarina Ringertz (Ekobrottsmyndigheten), kammaråklagaren Chatrine Rudström (Åklagarmyndigheten) och kanslirådet Hans Öjemark (Näringsdepartementet) till augusti 2007.

Till utredningen har det funnits referensgrupper knutna med företrädare för myndigheter, branscher och näringsliv. Följande personer har ingått i grupperna. Kurt Alavaara (Säkerhetspolisen), Fredrik von Essen (IT & Telekomföretagen) till juni 2007 därefter expert, Patrik Fältström (den tidigare IT-politiska strategigruppen,

Näringsdepartementet), Mikael Grape (Tele 2 AB), Kajsa Hedberg (Svenska Stadsnätsföreningen), Fredrik Helgesson (B2 Bredband Holding AB), Håkan Hjelmestam (TeliaSonera AB), Annkatrin Hübinette (Tullverket), Mikael Ingemarsson (Konkurrensverket) från januari 2007, Adrienne de Jounge (Konkurrensverket) till januari 2007, Kurt Erik Lindqvist (Sveriges Operatörers Forum), Richard Rebhan (TDC Song) och Staffan Wikell (Sveriges Kommuner och Landsting).

Det har också funnits en referensgrupp med representanter för riksdagspartierna. I den gruppen har ingått Bodil Ceballos (mp), Kenneth G Forslund (s), Björn Hamilton (m), Johan Linander (c), Inger Lundgren (v) från juni 2007, Rolf Olsson (v) till maj 2007, Olle Sandahl (kd) och Cecilia Wigström (fp).

Ämnesrådet Per Lagerud och numera rådmannen Annacarin Rathsman har varit utredningens sekreterare.

Utredningen, som tagit namnet Trafikuppgiftsutredningen, överlämnar härmed betänkandet *Lagring av trafikuppgifter för brottsbekämpning* (SOU 2007:76).

Arbetet har bedrivits i nära samråd med de sakkunniga och experterna och är därför skrivet i ”vi-form”.

Hans-Olof Lindblom och Per Furberg har avgivit särskilda yttranden.

Uppdraget är härmed avslutat.

Stockholm i november 2007

Gudrun Antemar

/Per Lagerud
Annacarin Rathsman

Innehåll

Förkortningar

BRU	Beredningen för rättsväsendets utveckling (Ju 2000:13)
Dir.	Kommittédirektiv
Ds	Betänkande i departementsserien
JO	Riksdagens ombudsmän (Justitieombudsmannen) eller Justitieombudsmännens ämbetsberättelse
KPI	Konsumentprisindex
LEK	Lagen (2003:389) om elektronisk kommunikation
Prop.	Proposition
PTS	Post- och telestyrelsen
PTSFS	Post- och telestyrelsens författningssamling
PUL	Personuppgiftslagen (1998:204)
RB	Rättegångsbalken
SCB	Statistiska centralbyrån
SOU	Statens offentliga utredningar
TU	Trafikutskottet

Sammanfattning

Bakgrund

Bombattentaten i Madrid den 25 mars 2004 initierade det arbete som så småningom ledde till att Europaparlamentet och rådet den 15 mars 2006 antog direktivet (2006/24/EG) om lagring av trafikuppgifter. Direktivet syftar till att säkerställa att uppgifter om kommunikation med fast och mobil telefoni, Internetåtkomst, e-post och Internettelefoni lagras så att de brottsbekämpande myndigheterna kan få tillgång till uppgifterna för utredning, avslöjande och åtal som avser allvarlig brottslighet. Till skillnad mot vad som gäller i dag när varje leverantör själv har att bedöma vilka uppgifter som behöver lagras för den egna verksamheten ska samtliga de trafikuppgifter som anges i direktivet lagras under en viss bestämd tid för brottsbekämpande syften. Enkelt uttryckt rör det sig om uppgifter som svarar på frågorna *vem* kommunicerade med *vem*, *när* skedde det, *var* befann sig de som kommunicerade och *vilken* typ av kommunikation användes. Uppgifterna får dock inte avslöja innehållet i en kommunikation, t.ex. telefonsamtalet, sms-meddelandet, telefaxmeddelandet eller e-postmeddelandet.

Bestämmelser om lagring av trafikuppgifter håller på att genomföras eller har genomförts i alla länder i EU. Det följer av Sveriges medlemskap i unionen att direktivet om lagring av trafikuppgifter ska genomföras även här. Utredningens uppgift är att föreslå en reglering för genomförandet som tillgodoser både behovet av att bekämpa allvarlig brottslighet och skyddet för medborgarnas integritet. En utgångspunkt ska vara att lagringsskyldigheten ska omfatta de trafikuppgifter som myndigheterna kan ha tillgång till i dag och som avser fast och mobil telefoni, Internetåtkomst, e-post och Internettelefoni. Direktivet ålägger medlemsstaterna att genomföra bestämmelserna i nationell rätt senast den 15 september 2007. När det gäller Internetåtkomst, e-post och Internettelefoni finns en

möjlighet att skjuta upp genomförandet av direktivet till och med den 15 mars 2009. Den möjligheten har Sverige utnyttjat.

Utredningen drog tidigt den slutsatsen att det inte var meningsfullt att först föreslå regler om lagring av trafikuppgifter som enbart rörde fast och mobil telefoni för att senare återkomma med förslag rörande övriga delar. I stället behövde förslagen presenteras i ett sammanhang. Utredningen har därför fått förlängd tid till den 1 november 2007 för uppdraget.

Genomförandet i andra länder

Vi har inhämtat uppgifter om genomförandet eller förslag till genomförande av direktivet i Danmark, Finland och Norge, de baltiska staterna, Irland, Spanien, Storbritannien, Tjeckien och Tyskland.

Genomförandeproceduren skiljer sig åt mellan länderna när det gäller huruvida direktivet genomförs i sin helhet vid ett tillfälle eller uppdelat mellan fast och mobil telefoni och Internet och när det gäller tidpunkten för genomförandet. Exempelvis är direktivet redan genomfört i sin helhet i Danmark medan Storbritannien har genomfört lagringsskyldigheten rörande fast och mobil telefoni. De uppgifter vi har fått innebär att Finland, Irland, Spanien och Tjeckien avser att genomföra direktivet i sin helhet vid ett och samma tillfälle medan genomförandet kommer att ske i etapper i Norge, Estland, Lettland, Litauen, Storbritannien och Tyskland.

Utifrån de uppgifter vi har fått om genomförandet i de olika länderna eller deras planer för genomförandet ser vi att de flesta länder kommer att ha en lagringstid på ett år. I Irland kommer tiden att vara tre år för fast och mobil telefoni och sex månader för Internetuppgifter. Sex månaders lagringstid för samtliga kategorier av uppgifter är föreslagen i Tjeckien och Tyskland medan 18 månader är föreslagen i Lettland.

Det finns också skillnader mellan länderna i frågorna om vilka trafikuppgifter som ska lagras, om det ska finnas undantag från lagringsskyldigheten t.ex. för små leverantörer, om leverantörerna ska ha möjlighet att låta annan fullgöra lagringen samt i frågan om vem som ska stå för kostnaderna för att fullgöra lagringsskyldigheten och kostnaderna för utlämnande av uppgifter. I Finland, Litauen och Storbritannien ska det allmänna stå för samtliga kostnader medan leverantörerna ska stå för samliga kostnader i Irland, Lettland

och Spanien. I övriga länder (Danmark, Estland, Tjeckien och Tyskland) ska det ske en fördelning av kostnaderna. Enligt de uppgifter vi har fått har integritetsfrågorna och direktivets inverkan på konkurrensen diskuterats i de enskilda länderna men debatten har inte uppfattats som ett hinder för genomförandet av direktivet utan tagits till vara för att höja kvaliteten i lagstiftningsarbetet i respektive land.

Skyddet för den personliga integriteten

Direktivet om lagring av trafikuppgifter innebär att det blir en regel att vissa trafikuppgifter ska lagras under en viss bestämd tid. Ett genomförande av direktivet medför att mycket stora informationsmängder kommer att lagras. Endast en ytterst begränsad del av uppgifterna kommer att lämnas ut till de brottsbekämpande myndigheterna och användas vid bekämpning av allvarlig brottslighet.

Trafikuppgifter är i många fall uppgifter om enskildas personliga förhållanden och korrespondens. Det är mot bakgrund av uppgifternas integritetskänsliga karaktär som de nuvarande bestämmelserna om de brottsbekämpande myndigheternas tillgång till trafikuppgifter har utformats. Att få ut trafikuppgifter för utredning om brott har ansetts vara särskilt känsligt från integritetssynpunkt och förutsättningarna för utlämnande är noggrant reglerade i rättegångsbalken och lagen om elektronisk kommunikation.

Enligt vår mening är dock inte frågan om integritetsskyddet vid lagring av trafikuppgifter begränsat till de situationer där trafikuppgifter lämnas ut till de brottsbekämpande myndigheterna. En utgångspunkt för våra resonemang är att en generell lagring av trafikuppgifter i den omfattning som direktivet förutsätter påverkar både enskildas upplevelse av att få sin privata sfär inskränkt och integritetsskyddet för medborgarna i allmänhet. Intrånget i integriteten sker enligt vår mening redan genom att det allmänna säkrar tillgången till trafikuppgifterna genom lagringen.

Utredningen har vid en hearing inhämtat synpunkter på vilka risker som lagringen av trafikuppgifter medför för integritetsskyddet. Vid hearingen framfördes bl.a. följande. Generella åtgärder som innebär att uppgifter om enskilda samlas in är mer problematiska från integritetssynpunkt än specifika åtgärder i enskilda fall. Lagringsskyldigheten innebär att trafikuppgifter som på något sätt

rör praktiskt taget alla medborgare kommer att finnas lagrade. Uppgifterna kan ge kännedom om förhållanden av privat natur som man inte vill att andra ska få insyn i. Det är vetskapen om att dessa uppgifter finns lagrade och kan tas fram och granskas under lagringstiden och risken för att de läcker ut till obehöriga som deltagare vid hearingen ansåg vara det allvarliga bekymret från integritetssynpunkt. Det ansågs att lagstiftningen riskerar att få en psykologisk verkan som innebär att människor blir rädda och misstänksamma och i högre grad upplever att de lever i ett kontrollsamhälle. Det kan påverka tilltron till myndigheterna. Vid hearingen framfördes också att en ökad informationsvolym i allmänhet innebär en ökad risk för att informationen läcker eller sprids till obehöriga. Uppgifter kan komma ut genom bristande säkerhetsrutiner eller genom medvetna åtgärder. Det framfördes också att det finns risk för att de brottsbekämpande myndigheterna kan komma att utnyttja trafikuppgifter i mycket högre utsträckning än tidigare. Mot det anfördes dock att trafikuppgifterna behövs för utredning om allvarlig brottslighet och att de leder till att fler allvarliga brott klaras upp och att fler brottsoffer därmed kan få upprättelse. En annan faktor som berördes vid hearingen är risken för ändamålsglidning, dvs. risken för att när systemet för lagring av trafikuppgifter väl finns och fungerar kommer det att användas för andra syften än det ursprungligen var tänkt för. Deltagarna vid hearingen underströk också vikten av ett säkert, öppet och transparent kontrollsystem så att medborgarna kan bedöma vilka trafikuppgifter som lagras, hur länge de lagras och hur uppgifterna används i brottbekämpningen.

Direktivet innehåller flera artiklar som ska garantera en rimlig proportion mellan intresset av att allvarliga brott utreds och lagförs och integritetsskyddet. I vårt uppdrag ingår att belysa de integritetsaspekter som aktualiseras vid genomförandet av direktivet och lämna förslag om regler för lagring av trafikuppgifter som innebär ett tillräckligt skydd för lagrade uppgifter och som är förenliga med grundlags- och konventionsskyddet för den personliga integriteten.

Trafikuppgifter som ska lagras

Tillgång till trafikuppgifter är av avgörande betydelse för bekämpningen av allvarlig brottslighet. När behovet av trafikuppgifter för brottsbekämpningen ska bedömas måste utgångspunkten vara att

det är medborgarnas behov av att allvarlig brottslighet utreds och lagförs som ska tillgodoses. Det är medborgarna i allmänhet och brottsoffren som för sin trygghet respektive upprättelse har anspråk på en effektiv brottsbekämpning.

Ett genomförande av direktivet innebär att trafikuppgifter lagras som sammantaget ger upplysning om vilka som kommunicerade med varandra, när det skedde, var det skedde och vilken typ av kommunikationslösning som användes. Svaret på alla dessa frågor kommer i de flesta fall inte att finnas hos en enda leverantör utan de brottskämpande myndigheterna kommer att behöva ställa samman uppgifter från flera leverantörer för att få en klar bild.

Den enskilde leverantören ska ha skyldighet att lagra enbart sådana uppgifter som denne någon gång *genererar* eller *behandlar*. Det finns med andra ord ingen skyldighet att skaffa sig alla de uppgifter som lagringsskyldigheten omfattar. Det betyder i princip att om uppgifterna finns hos leverantören någon gång, även om det bara rör sig om en ytterst kort tid, ska de lagras. Lagringsskyldigheten utgör därmed inget hinder mot exempelvis anonyma kontantkort.

Vid telefoni ska uppgift om följande lagras:

- uppringande telefonnummer,
- nummer som slagits och nummer till vilka samtalet styrts,
- uppgifter om abonnent och registrerad användare,
- datum och spårbar tid då kommunikationen påbörjades och avslutades,
- den tjänst som använts, samt
- slutpunkter.

Vid mobil telefoni ska utöver det som anges under telefoni uppgift om följande lagras:

- uppringande parts abonnemangsidentitet och utrustningsidentitet,
- uppringd parts abonnemangsidentitet och utrustningsidentitet,
- lokaliseringsinformation för kommunikationens början och slut, samt
- datum, spårbar tid och lokaliseringsinformation för den första aktiveringen av en förbetald anonym tjänst.

Vid Internettelefoni ska utöver det som anges under telefoni uppgift om följande lagras:

- uppringande parts IP-adresser, samt
- uppringd parts IP-adresser.

Vid meddelandehantering (t.ex. e-post och SMS) ska uppgift om följande lagras:

- avsändarens och mottagarens meddelandeadress,
- uppgifter om abonnent och registrerad användare,
- datum och spårbar tid för på- och avloggning i meddelandetjänsten,
- datum och spårbar tid för avsändande och mottagande av meddelandet, samt
- den tjänst som har använts och spårbar tid för användandet.

Vid Internetåtkomst ska uppgift om följande lagras:

- användarens IP-adresser,
- uppgifter om abonnent och registrerad användare,
- datum och spårbar tid för på- och avloggning i Internettjänsten,
- typen av Internetanslutning som använts, samt
- slutpunkter.

Vid verksamheter som tillhandahåller kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst ska uppgift om följande lagras:

- uppgifter om abonnent,
- vilken typ av kapacitet för överföring som har använts och spårbar tid för användandet, samt
- slutpunkter.

De uppgifter som ska lagras vid telefoni, mobil telefoni och Internettelefoni ska även lagras vid misslyckad uppringning, alltså fall där någon t.ex. inte har svarat på uppringningen.

Den lagringsskyldighet vi föreslår för uppgifter vid mobil telefoni om lokalisering vid kommunikationens slut och lagringsskyldigheten för uppgifter vid misslyckad uppringning som inte lagras eller loggas av leverantören går utöver direktivet om lagring av trafikuppgifter. Vi bedömer att skälen för att lagra även dessa uppgifter är så starka att de uppväger det integritetsintrång som lagringen medför och att lagringsskyldigheten därför kan motiveras utifrån

direktivet (2002/58/EG) om integritet och elektronisk kommunikation.

De trafikuppgifter som lagringsskyldigheten omfattar är ingen uttömmande uppräkning av de uppgifter som de brottsbekämpande myndigheterna kan få ut vid hemlig teleövervakning eller enligt lagen om elektronisk kommunikation. Skulle andra uppgifter finnas hos leverantören ska de lämnas ut till de brottsbekämpande myndigheterna när det finns förutsättningar för det enligt rättegångsbalken eller lagen om elektronisk kommunikation.

Lagringsskyldighetens fullgörande

Var ska trafikuppgifter lagras och av vem?

Vi föreslår att lagringen av trafikuppgifter ska ske hos leverantörerna. Enligt lagen om elektronisk kommunikation måste leverantörer av allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning och leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster anmäla sin verksamhet till Post- och telestyrelsen innan verksamheten inleds. Direktivet om lagring av trafikuppgifter innehåller precis samma uttryck för vilka leverantörer som ska vara skyldiga att lagra trafikuppgifterna. Vi föreslår att skyldigheten att lagra trafikuppgifter ska gälla för de leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation. Vi föreslår att tillsynsmyndigheten efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen ska få medge undantag i enskilda fall. Vid den bedömningen får det ske en avvägning mellan nyttan för brottsbekämpningen av att leverantören lagrar trafikuppgifterna och kostnaden för leverantören för att fullgöra lagringsskyldigheten. Sekretess enligt 5 kap. 1 § sekretesslagen bör gälla för tillsynsmyndighetens prövning av frågor om undantag från lagringsskyldigheten.

Lagringstiden

Direktivet om lagring av trafikuppgifter anger att trafikuppgifterna ska lagras under en period om minst sex månader och högst två år från det datum då kommunikationen ägde rum. Regeringens direktiv till utredningen innebär att lagringstiden ska vara minst ett år.

Vi föreslår att alla trafikuppgifter ska lagras under lika lång tid. Vi föreslår en lagringstid på ett år. Vår bedömning är att en lagringstid på två år väl skulle kunna motiveras sett utifrån medborgarnas och brottsoffrens intresse av att allvarliga brott utreds och lagförs. Samtidigt talar både intresset av skydd för den personliga integriteten, kostnads-, säkerhets- och konkurrensaspekter med olika styrka för en så kort lagringstid som möjligt. Vi har gjort en avvägning mellan dessa olika intressen och funnit att en lagringstid på ett år innebär en förbättring för brottsbekämpningen i förhållande till vad som gäller i dag. Den lagringstiden tillgodoser en stor del av de behov som finns av trafikuppgifter för brottsbekämpningen samtidigt som skyddet för integriteten kan upprätthållas och risken för konkreta integritetsintrång inte blir oacceptabel. Ett års lagringstid innebär också att vi valt att bestämma lika lång lagringstid som flertalet av övriga länder i EU.

Vid lagringstidens slut ska uppgifterna utplånas, om inte de brottsbekämpande myndigheterna vid den tiden har begärt tillgång till uppgifterna men ännu inte fått ut dem, eller leverantören av andra skäl, t.ex. abonnentfakturering, har rätt att behandla uppgifterna även fortsättningsvis.

Leverantörernas medverkan inom viss tid m.m.

Utöver skyldigheten att lagra trafikuppgifterna ska leverantören ha skyldighet att anpassa sin verksamhet så att uppgifterna enkelt kan tas om hand av de brottsbekämpande myndigheterna vid ett utlämnande. Uppgifterna ska utan dröjsmål lämnas ut till den brottbekämpande myndighet som har fått domstols tillstånd till hemlig teleövervakning eller begär att få ut uppgifterna enligt lagen om elektronisk kommunikation.

Ändamålen med behandlingen av trafikuppgifter

Lagrade trafikuppgifter behandlas när de lämnas ut till de brottsbekämpande myndigheterna. I den allmänna debatten har det framförts farhågor för att de lagrade trafikuppgifterna ska användas av leverantörerna för andra syften än att lämnas ut till de brottsbekämpande myndigheterna vid allvarlig brottslighet.

Mot bakgrund av de stora skillnader som finns mellan leverantörerna både i fråga om verksamhet och volym bedömer vi att leverantörerna ska ha möjlighet att anlita annan för att fullgöra lagringen. Det är således tillåtet att behandla uppgifterna om annan fullgör lagringen.

Vid sidan om dessa situationer föreslår vi att det inte ska vara tillåtet för leverantörerna att behandla trafikuppgifter som har lagrats för brottsbekämpningsändamål. Enligt våra förslag blir det alltså tillåtet att behandla de trafikuppgifter som har lagrats för brottsbekämpande syften endast i tre situationer; för att lämna ut dem efter beslut om hemlig teleövervakning, för att lämna ut dem enligt lagen om elektronisk kommunikation och för att annan ska fullgöra lagringen.

Kvalitet och säkerhet

Särskilt mot bakgrund av integritetsskyddet ställer direktivet om lagring av trafikuppgifter i olika avseenden krav på uppgifternas kvalitet och på säkerheten vid lagringen. Det ska med andra ord finnas ett tillräckligt skydd mot att uppgifterna används, sprids eller läcker ut genom medvetna eller oaktsamma handlingar och mot att de förvanskas eller förstörs. Vi föreslår en särskild regel som innebär skyldighet för leverantörerna att vidta särskilda tekniska och organisatoriska åtgärder för ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter. De mer specifika kraven får tillsynsmyndigheten efter samråd med Rikspolisstyrelsen och Datainspektionen besluta om. De kraven kan t.ex. innebära att trafikuppgifterna ska vara enkelt sökbara och vara logiskt skilda från övrig verksamhet hos leverantörerna samt att leverantörerna ska säkerställa att endast behörig personal har tillgång till trafikuppgifterna.

De trafikuppgifter som samtidigt är personuppgifter ska inte få föras över till ett land som inte har en adekvat nivå för skyddet av uppgifterna.

Det straff- och skadeståndsrättsliga skyddet

Vi bedömer att lagringen av trafikuppgifter inte ger anledning att förändra några straff- eller skadeståndsrättsliga bestämmelser. De bestämmelser som finns i dag är uppbyggda till skydd för de integ-

ritetskänsliga uppgifter som redan nu sparas och lagras i olika sammanhang. Mot bakgrund av den mängd trafikuppgifter som kommer att lagras hos leverantörerna kan ett dataintrång få vittgående följder. Det kan därför diskuteras om straffskalan i bestämmelsen om dataintrång är tillräcklig för att en adekvat påföljd ska kunna dömas ut. Det kan övervägas om det behövs en bestämmelse om grovt dataintrång med en mer sträng straffskala. Ett sådant övervägande bör dock enligt vår mening ske i ett vidare sammanhang.

De bestämmelser som gäller i dag innebär i korthet följande.

Om någon hos leverantören eller en utomstående behandlar uppgifterna för andra ändamål än de tillåtna eller om någon ändrar i uppgifter, förstör eller utplånar uppgifter eller för in uppgifter som inte ska finnas i lagret, blir det förfarandet att bedöma enligt bestämmelsen om dataintrång i brottsbalken.

Såväl myndighetsanställda som anställda hos leverantören och uppdragstagare har tystnadsplikt och får inte obehörigen röja trafikuppgifter. Tystnadsplikten har en straffrättslig sanktion i brottsbalkens bestämmelse om brott mot tystnadsplikten.

Integriteten skyddas också av straffbestämmelser i personuppgiftslagen som bl.a. innebär att personuppgifter inte får föras över till ett land som inte har en adekvat skyddsnivå i lagstiftningen för behandlingen.

Att olovligen bereda sig tillgång till trafikuppgifter kan under vissa förutsättningar även bli att betrakta som företagsspionerі.

Vid sidan av detta kan företagsbot och förverkande bli aktuellt t.ex. om leverantören inte har vidtagit särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter.

En enskild person som skadas på grund av brott kan få ersättning för person-, sak- och ren förmögenhetsskada. Vid dataintrång, brott mot tystnadsplikten och brott mot personuppgiftslagen kan också ersättning för kränkning bli aktuell. När trafikuppgifter som är personuppgifter har hanterats oaktsamt eller felaktigt utan att det har varit fråga om brott kan en enskild som skadas få ersättning enligt skadeståndsregeln i personuppgiftslagen för kränkning och person-, sak- och ren förmögenhetsskada om den personuppgiftsansvarige (leverantören) inte visar att felet inte berodde på honom. Skadeståndsersättning kan också bli aktuellt enligt skadeståndslagen och lagen om företagshemligheter.

Tillsyn

Post- och telestyrelsen har tillsyn över verksamhet som bedrivs enligt lagen om elektronisk kommunikation och således tillsyn över leverantörernas verksamhet. Vi föreslår att lagringsskyldigheten ska regleras i den lagen och att Post- och telestyrelsen ska ha tillsynen över leverantörernas lagring av trafikuppgifter.

De befogenheter som Post- och telestyrelsen har i dag i sin tillsynsverksamhet är enligt vår bedömning ändamålsenliga och tillräckliga även för lagringen av trafikuppgifter. Det innebär att Post- och telestyrelsen bl.a. ska kunna begära in upplysningar och handlingar från leverantörerna, besluta om tillträde till områden och lokaler, lämna förelägganden och förbud förenade med vite samt ytterst besluta att verksamheter ska upphöra.

Myndigheternas tillgång till trafikuppgifter

De brottsbekämpande myndigheterna har i dag möjlighet att få ut trafikuppgifter från leverantörerna genom framför allt två regelverk; rättegångsbalken och lagen om elektronisk kommunikation.

Direktivet om lagring av trafikuppgifter innebär inte att myndigheterna ska få fri tillgång till trafikuppgifter utan enbart att uppgifterna ska finnas ”säkrade” för de brottsbekämpande syftena. Med andra ord ska det i fortsättningen inte vara en slump om myndigheterna kan få ut trafikuppgifterna efter beslut enligt rättegångsbalken eller lagen om elektronisk kommunikation.

Förutsättningarna för att få ut trafikuppgifter enligt bestämmelserna om *hemlig teleövervakning* i rättegångsbalken är följande.

1. Det ska finnas en skäligen misstänkt person.
2. Misstanken ska röra

   a) brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader (även anstiftan och medhjälp),

   b) dataintrång, barnpornografibrott som inte är ringa, narkotikabrott eller narkotikasmuggling, eller

   c) försök, förberedelse eller stämpling till brott under a) och b).
3. Åtgärden ska vara av synnerlig vikt för utredningen.
4. Åtgärden får avse uppgifter om telemeddelanden som befordras eller har befordrats till eller från teleadresser med viss anknytning till den misstänkte.
5. Åtgärden ska beslutas av domstol.

Förutsättningarna för att få ut trafikuppgifter enligt *lagen om elektronisk kommunikation* är följande (i jämförelse med rättegångsbalken).

1. Det behöver inte finnas en skäligen misstänkt person.
2. Det ska vara fråga om brott för vilket inte är föreskrivet lindrigare straff än två års fängelse (även anstiftan och medhjälp).
3. Åtgärden behöver inte vara av synnerlig vikt för utredningen.
4. Åtgärden är inte begränsad till vissa teleadresser men uppgiften ska angå ett särskilt elektroniskt meddelande.
5. Åtgärden beslutas av den brottsbekämpande myndigheten.

När de brottsbekämpande myndigheterna behöver uppgifter om abonnemang, t.ex. namn, adress, telefonnummer och IP-nummer, krävs inte samma svårhetsgrad rörande brottet. I sådana fall är det enligt lagen om elektronisk kommunikation tillräckligt att det för brottet är föreskrivet fängelse och att det i det enskilda fallet kan bli fråga om annan påföljd än böter.

Lagringsskyldigheten medför att trafikuppgifter är säkrade och tillgängliga för att kunna lämnas ut till de brottsbekämpande myndigheterna. Vi bedömer inte att det förhållandet att uppgifterna kommer att vara tillgängliga på ett mer förutsebart sätt innebär att de bestämmelser som reglerar när uppgifterna får lämnas ut behöver ändras. De förutsättningar som dessa bestämmelser anger för utlämnande innebär att trafikuppgifter kan lämnas ut för brott som är minst lika allvarliga som de brott som anges när utlämnande enligt en europeisk arresteringsorder kan ske. Vi har därför kommit fram till att bestämmelserna om lagring av trafikuppgifter inte ger anledning att förändra förutsättningarna för att de brottsbekämpande myndigheterna ska få tillgång till trafikuppgifterna. Frånsett rena ”kataloguppgifter” är det enbart de mer allvarliga typerna av brott som ger den möjligheten och dessutom är det i många fall enbart den svåraste graden av brotten. Det kan nämnas att de tillstånd till hemlig teleövervakning som meddelades under år 2006 främst avsåg mord, dråp, grov misshandel, människorov, människohandel, olaga hot (grovt brott), grovt koppleri, grov stöld, grovt rån, grovt bedrägeri, utpressning (grovt brott), häleri (grovt brott), grovt bokföringsbrott, grov mordbrand, övergrepp i rättssak (grovt brott), grovt narkotikabrott, grovt skattebrott, grovt vapenbrott, grova smugglingsbrott och grovt dopningsbrott. Vi föreslår inte heller att förutsättningarna för att lämna ut ”kataloguppgifter” ändras eftersom det enligt vår bedömning skulle leda till allvarliga försämringar för brottsbekämpningen.

Balansen mellan brottsbekämpning och integritetsskydd

Direktivet innehåller inte bara en uppräkning av vilka trafikuppgifter som ska lagras utan också flera artiklar som ska garantera en rimlig proportion mellan brottsbekämpningens intressen och integritetsskyddet.

För att kraven i regeringsformen och Europakonventionen ska vara uppfyllda krävs att det finns en balans mellan brottsbekämpningens intressen av att trafikuppgifter lagras och integritetsskyddet. Nyttan av lagringen ska alltså stå i rimlig proportion till den integritetsskada som lagringen kan orsaka.

Direktivet om lagring av trafikuppgifter har tagits fram inom EU mot bakgrund av de fördelar från brottsbekämpningssynpunkt som har kunnat konstateras i flera medlemsländer. Även i Sverige har behovet av tillgång till trafikuppgifter i brottbekämpningen övervägts tidigare.

Behovet av trafikuppgifter bör diskuteras utifrån den precisering av behovet som de brottsbekämpande myndigheterna gör. Den självklara utgångspunkten måste vara att det är medborgarna i allmänhet och brottsoffren som för sin trygghet och upprättelse har behov av en effektiv bekämpning av särskilt den allvarliga brottsligheten.

Vi har kommit fram till att tillgången till trafikuppgifter är av avgörande betydelse för brottsbekämpningen och ofta helt nödvändig för att utredningarna över huvud taget ska kunna föras framåt.

Samtidigt medför lagring av trafikuppgifter ett påtagligt intrång i integritetsskyddet. Integritetsintrånget sker redan genom att det allmänna säkrar tillgången till uppgifterna genom att de lagras. Den främsta risken för integritetsförluster finns i att trafikuppgifterna på ett felaktigt sätt, genom uppsåtliga handlanden eller av oaktsamhet, sprids från leverantörerna till obehöriga och i att leverantörerna använder trafikuppgifterna för andra ändamål än de tillåtna.

Flera av våra förslag går ut på att minska riskerna för att enskilda drabbas av integritetsintrång och orsakas skador till följd av detta. Lagringen ska ske hos leverantörerna och inte i något centrallager. Uppgifter om en persons kommunikation kommer alltså i det stora flertalet fall inte att finnas på ett ställe. Lagringstiden ska vara begränsad till ett år och uppgifterna ska utplånas omedelbart därefter. Det ska vara förbjudet för leverantörerna att behandla uppgifterna för annat än de brottsbekämpande syftena och om annan

fullgör lagringen. Leverantörerna ska vidta särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter. De straff- och skadeståndsrättsliga bestämmelserna skyddar mot missbruk. Tillsynsmyndigheten ska kontrollera så att leverantörernas verksamhet följer gällande regelverk. En del i integritetsskyddet är också att de regler vi föreslår, tillsammans med tillsynsmyndighetens föreskrifter, är så tydliga och väl avgränsade som möjligt. Till det kommer att bestämmelserna om hemlig teleövervakning och utlämnande enligt lagen om elektronisk kommunikation tar hänsyn till integritetsskyddet i de förutsättningar som krävs för att de brottsbekämpande myndigheterna ska få tillgång till uppgifter.

Vi bedömer att våra förslag innebär inte bara en rimlig utan en god balans mellan brottsbekämpningens intressen av att trafikuppgifter lagras och integritetsskyddet.

Fördelning av kostnaderna

Lagringsskyldigheten innebär kostnader för att identifiera, spara, lagra och lämna ut trafikuppgifter. Kostnaderna avser nya tekniska investeringar, anpassning av befintliga system, underhåll av system och administration.

För att få en grund för våra bedömningar av kostnaderna har vi låtit de leverantörer som är representerade i utredningen och en oberoende expert inom området för elektronisk kommunikation göra en analys av de kostnader som våra förslag innebär. Mot bakgrund av de beräkningar som har gjorts av experten bedömer vi att kostnaderna för att identifiera och spara uppgifter kan beräknas till omkring 100 miljoner kronor. Den sammanlagda kostnaden för att lagra trafikuppgifterna uppskattar vi också till omkring 100 miljoner kronor om varje leverantör lagrar i egna system. Den kostnaden bygger på att varje leverantör lagrar uppgifterna i den växel eller server där uppgiften uppkommer, och inte centraliserar lagringen inom verksamheten. Om alla leverantörer i stället skulle ha ett gemensamt system för lagring och utlämnande beräknas den totala kostnaden till 77 miljoner kronor. Kostnaden för att lämna ut trafikuppgifterna uppskattar vi till ca 20 miljoner kronor årligen.

Vi föreslår att leverantörerna ska stå för kostnaderna för anpassning av systemen, lagring och säkerhet och att det allmänna ska ersätta leverantörerna när uppgifter lämnas ut i enskilda ärenden.

Med en sådan fördelning uppnår man fördelen att leverantörerna genom sin kunskap och kompetens om egna system och behov kan hålla kostnaderna nere. Samtidigt får de brottsbekämpande myndigheterna betala för just det som har en direkt koppling till uppgiften att utreda och lagföra allvarlig brottslighet.

Det av resurs- och tidsskäl överlägset bästa sättet att reglera ersättningsnivån är enligt vår bedömning att tillsynsmyndigheten fastställer schabloner och bestämmer vad som ska gälla i de situationer där det finns anledning att avvika från schablonerna. Utgångspunkten vid bestämmandet av schablonerna bör vara att leverantörerna ska få ersättning för sina kostnader för att lämna ut uppgifter. Tillsynsmyndigheten ska samråda med de brottsbekämpande myndigheterna och leverantörerna när schablonbeloppen bestäms.

Konkurrens

Lagringsskyldigheten innebär en viss inverkan på konkurrensen. Om de ökade kostnaderna blir för höga för de små leverantörerna, kan det leda till att de blir tvungna att träda ut från marknaden, vilket i så fall kan leda till en minskad konkurrens. Möjligheten att ge undantag från skyldigheten att lagra trafikuppgifter och att anlita annan för att fullgöra lagringen kan mildra effekterna för de små leverantörerna och därmed ge minskad negativ effekt på deras investeringsvilja och möjligheter att stanna kvar på marknaden.

Statistik

Senast den 15 september 2010 ska kommissionen lämna en utvärdering till Europaparlamentet av tillämpningen av direktivet om lagring av trafikuppgifter. Därför anges det i direktivet att medlemsstaterna ska överlämna statistik till kommissionen varje år. Även från nationella perspektiv finns det skäl att föra statistik. Det kan ge bättre underlag för bedömningen av behovet av trafikuppgifter i brottsbekämpningen och ett underlag för bedömningen av systemets effektivitet. Statistiken skulle också bilda ett gott underlag för de brottsbekämpande myndigheternas egen tillsynsverksamhet. Också andra kontrollorgans möjligheter att utföra sina uppgifter förbättras med ett gott statistikunderlag. Den kanske viktigaste

aspekten är dock att statistiken skulle kunna bidra till en ökad parlamentarisk kontroll av användningen av trafikuppgifter i brottsbekämpningen.

Statistik ska föras över

1. antalet verkställda beslut om hemlig teleövervakning respektive utlämnanden enligt lagen om elektronisk kommunikation,
2. vilka typer av brott som ärendena har avsett,
3. hur lång tid som har förlöpt från det att respektive trafikuppgift lagrades till dess att den brottsbekämpande myndigheten begärde tillgång till uppgiften och
4. antalet ärenden där myndigheternas begäran om att få tillgång till trafikuppgifter inte har kunnat tillgodoses av leverantörerna samt vilka typer av brott ärendena har avsett.

Av sekretesskäl ska statistiken inte innefatta de ärenden som handläggs av Säkerhetspolisen och som rör rikets säkerhet.

De brottsbekämpande myndigheterna ska ansvara för statistiken. Uppgifterna bör sammanställas av Rikspolisstyrelsen och rapporteras till regeringen som ett underlag för regeringens redovisning till kommissionen.

Konsekvenser och genomförande

Vi bedömer att de kostnader som våra förslag medför för rättsväsendets myndigheter uppvägs av de effektivitetsvinster som är förenade med lagringen av trafikuppgifter. Vi bedömer därför att våra förslag inte medför behov av att tillföra rättsväsendet ytterligare resurser.

Förslagen innebär att Post- och telestyrelsen får nya uppgifter inom ramen för sin tillsynsverksamhet och att den verksamheten behöver tillföras resurser motsvarande 2,75 miljoner kronor om året under åren 2008–2010 och därefter en miljon kronor årligen. Det blir en fråga för Post- och telestyrelsen att bedöma om den kostnaden kan bäras inom ramen för de avgifter som myndigheten tar ut i dag.

Förslagen i betänkandet ska träda i kraft den 1 januari 2009. Några övergångsbestämmelser ska inte finnas.

Författningsförslag

1 Förslag till lag om ändring i sekretesslagen (1980:100)

Härigenom föreskrivs att 5 kap. 1 § sekretesslagen (1980:100) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
5 kap. Sekretess med hänsyn främst till intresset att förebygga eller beivra brott	
1 §	
Sekretess gäller för uppgift som hänför sig till	
1. förundersökning i brottmål,	
2. angelägenhet, som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,	
3. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde,	
4. åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott, *eller*	4. åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott,
5. Finansinspektionens verksamhet som rör övervakning enligt lagen (2005:377) om straff för marknadsmissbruk vid handel med finansiella instrument,	5. Finansinspektionens verksamhet som rör övervakning enligt lagen (2005:377) om straff för marknadsmissbruk vid handel med finansiella instrument, *eller*

6. Post- och telestyrelsens verksamhet för prövning av frågor om undantag enligt 6 kap. 6 c § andra stycket lagen (2003:389) om elektronisk kommunikation,

om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

För uppgift som hänför sig till sådan underrättelseverksamhet som avses i 3 § polisdatalagen (1998:622) eller som i annat fall hänför sig till Säkerhetspolisens verksamhet för att förebygga eller avslöja brott mot rikets säkerhet eller förebygga terroristbrott enligt 2 § lagen (2003:148) om straff för terroristbrott gäller sekretess, om det inte står klart att uppgiften kan röjas utan att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas. Detsamma gäller uppgift som hänför sig till sådan underrättelseverksamhet som avses i 2 § lagen (1999:90) om behandling av personuppgifter vid Skatteverkets medverkan i brottsutredningar samt sådan verksamhet som avses i 7 § 1 lagen (2005:787) om behandling av uppgifter i Tullverkets brottsbekämpande verksamhet.

Sekretess enligt första och andra styckena gäller i annan verksamhet hos myndighet för att biträda åklagarmyndighet, polismyndighet, Skatteverket, Tullverket eller Kustbevakningen med att förebygga, uppdaga, utreda eller beivra brott samt hos tillsynsmyndigheten i konkurs och hos Kronofogdemyndigheten för uppgift som angår misstanke om brott.

Utan hinder av sekretessen enligt andra stycket kan enskild få uppgift om huruvida han eller hon förekommer i Säkerhetspolisens register med anledning av den verksamhet som bedrevs med stöd av

1. personalkontrollkungörelsen (1969:446) och de tilläggsföreskrifter som utfärdats med stöd av den,

2. förordningen den 3 december 1981 med vissa bestämmelser om verksamheten vid Rikspolisstyrelsens säkerhetsavdelning, eller

3. motsvarande äldre bestämmelser.

Sekretess gäller inte för uppgift som hänför sig till sådan verksamhet hos Säkerhetspolisen som avses i andra stycket om uppgiften har införts i en allmän handling före år 1949. I fråga om annan uppgift i allmän handling som hänför sig till sådan verksamhet som avses i andra stycket gäller sekretessen i högst sjuttio år. I fråga om

uppgift i allmän handling i övrigt gäller sekretessen i högst fyrtio år.

Denna lag träder i kraft den 1 januari 2009.

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

Härigenom föreskrivs i fråga om lagen (2003:389) om elektronisk kommunikation

dels att 6 kap. 3 och 5 §§ ska ha följande lydelse,

dels att rubriken närmast före 6 kap. 5 § ska ha följande lydelse,

dels att det i lagen ska införas fem nya paragrafer, 6 kap. 6 a - 6 d och 19 a §§, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap. Integritetsskydd	
3 §	
Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst *skall* vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Den som tillhandahåller ett allmänt kommunikationsnät *skall* vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna *skall* vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsintrång.	Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst *ska* vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Den som tillhandahåller ett allmänt kommunikationsnät *ska* vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna *ska* vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsintrång. *Lagringsskyldiga enligt 6 a § ska dessutom vidta särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter.*

Behandling av trafikuppgifter	**Behandling av trafikuppgifter *m.m.***
	5 §
Trafikuppgifter som avser användare som är fysiska personer eller avser abonnenter och som lagras eller behandlas på annat sätt av den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 §, *skall* utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande, om de inte *får* sparas för sådan behandling som anges i 6 eller 13 §.	Trafikuppgifter som avser användare som är fysiska personer eller avser abonnenter och som lagras eller behandlas på annat sätt av den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 §, *ska* utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande, om de inte sparas för sådan behandling som anges i 6, *6 a* eller 13 §.
	6 a §
	Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § och som genererar eller behandlar uppgifter som avses i 20 § första stycket 1 och 3 ska lagra uppgifterna för brottsbekämpande syften.
	Lagrade uppgifter får behandlas endast
	1. för att lämnas ut enligt 22 § första stycket 2 och 3 eller 27 kap. 19 § rättegångsbalken, eller
	2. enligt 30 § första stycket personuppgiftslagen (1998:204).
	6 b §
	Lagring enligt 6 a § ska pågå under ett år från det datum kommunikationen ägde rum. Vid lagringstidens slut ska uppgifterna utplånas, om de inte har begärts utlämnade men ännu inte lämnats ut eller den lagringsskyldige

annars har rätt att fortsätta behandla dem.

6 c §

Regeringen meddelar föreskrifter om lagringsskyldighet enligt 6 a §.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om säkerhet enligt 3 § andra stycket och får i enskilda fall medge undantag från lagringsskyldigheten enligt 6 a §.

6 d §

Lagringsskyldiga enligt 6 a § har rätt till ersättning när lagrade trafikuppgifter lämnas ut enligt 22 § första stycket 2 och 3 eller 27 kap. 19 § rättegångsbalken. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om ersättningen.

19 a §

Lagringsskyldiga enligt 6 a § ska bedriva verksamheten så att uppgifterna enkelt kan tas om hand och lämnas ut utan dröjsmål.

Denna lag träder i kraft den 1 januari 2009.

3 Förslag till förordning (0000:00) om lagring av trafikuppgifter m.m. för brottsbekämpande syften

Inledande bestämmelse

1 § I denna förordning ges föreskrifter om lagring av trafikuppgifter m.m. enligt 6 kap. 3 § andra stycket, 6 a, 6 c och 6 d §§ lagen (2003:389) om elektronisk kommunikation.

Definitioner

2 § I denna förordning avses med

1. *Internettelefoni*: telefoni som använder IP-paket via Internet för överföring,
2. *Internetåtkomst*: möjlighet till överföring av IP-paket som ger användaren åtkomst till Internet,
3. *meddelandehantering*: överföring av elektroniskt meddelande som inte är samtal,
4. *misslyckad uppringning*: samtal som kopplats fram utan att få svar eller samtal som kopplats fram utan att nå mottagaren,
5. *mobil telefoni*: elektronisk kommunikationstjänst till mobil nätanslutningspunkt som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan och som inte samtidigt avser meddelandehantering,
6. *slutpunkt*: ändpunkt för varje lagringsskyldigs behandling av kommunikation,
7. *telefoni*: elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan och som inte samtidigt avser meddelandehantering.

Uppgifter som ska lagras

3 § Den som är lagringsskyldig enligt 6 kap. 6 a § lagen (2003:389) om elektronisk kommunikation ska lagra de uppgifter som anges i 4-9 §§.

4 § Vid telefoni ska uppgifter om följande lagras:
– uppringande telefonnummer,
– nummer som slagits och nummer till vilka samtalet styrts,
– uppgifter om abonnent och registrerad användare,
– datum och spårbar tid då kommunikationen påbörjades och avslutades,
– den tjänst som använts, samt
– slutpunkter.

5 § Vid mobil telefoni ska utöver det som anges i 4 § uppgifter om följande lagras:
– uppringande parts abonnemangsidentitet och utrustningsidentitet,
– uppringd parts abonnemangsidentitet och utrustningsidentitet,
– lokaliseringsinformation för kommunikationens början och slut, samt
– datum, spårbar tid och lokaliseringsinformation för den första aktiveringen av en förbetald anonym tjänst.

6 § Vid Internettelefoni ska utöver det som anges i 4 § uppgifter om följande lagras:
– uppringande parts IP-adresser, samt
– uppringd parts IP-adresser.

7 § Vid meddelandehantering ska uppgifter om följande lagras:
– avsändarens och mottagarens meddelandeadress,
– uppgifter om abonnent och registrerad användare,
– datum och spårbar tid för på- och avloggning i meddelandetjänsten,
– datum och spårbar tid för avsändande och mottagande av meddelande, samt
– den tjänst som har använts och spårbar tid för användandet.

8 § Vid Internetåtkomst ska uppgifter om följande lagras:
– användarens IP-adresser,
– uppgifter om abonnent och registrerad användare,
– datum och spårbar tid för på- och avloggning i Internettjänsten,
– typen av Internetanslutning som använts, samt
– slutpunkter.

9 § Vid verksamheter som tillhandahåller kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst ska uppgifter om följande lagras:
– uppgifter om abonnent,
– vilken typ av kapacitet för överföring som har använts och spårbar tid för användandet, samt
– slutpunkter.

10 § Lagringsskyldigheten för uppgifter enligt 4-6 §§ gäller även vid misslyckad uppringning.

Föreskrifter och undantag

11 § Post- och telestyrelsen får efter samråd med Rikspolisstyrelsen och Datainspektionen meddela verkställighetsföreskrifter om säkerhet enligt 6 kap. 3 § andra stycket lagen (2003:389) om elektronisk kommunikation.

12 § Post- och telestyrelsen får efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen i enskilda fall medge undantag från lagringsskyldigheten enligt 6 kap. 6 a § första stycket lagen (2003:389) om elektronisk kommunikation.

13 § Post- och telestyrelsen får efter samråd med Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen och Tullverket meddela föreskrifter om den ersättning som lagringsskyldiga har rätt till enligt 6 kap. 6 d § lagen (2003:389) om elektronisk kommunikation.

Denna förordning träder i kraft den 1 januari 2009.

1 Utredningens uppdrag och arbete

1.1 Vårt uppdrag

Efter bombattentaten i Madrid den 25 mars 2004 fick rådet för rättsliga och inrikes frågor (RIF) i uppdrag av Europeiska rådet att snarast anta gemensamma åtgärder om lagring av trafikuppgifter. Ett antal länder, däribland Sverige, utarbetade förslag som presenterades under sommaren 2004 och som därefter förhandlades.

Europaparlamentet och rådet antog den 15 mars 2006 direktivet 2006/24/EG om lagring av trafikuppgifter (se avsnitt 3). Direktivet syftar till att harmonisera medlemsstaternas regler om de skyldigheter som leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät har att lagra vissa uppgifter som genereras eller behandlas i samband med att en kommunikation sker med fast eller mobil telefoni, eller på Internet. De uppgifter som avses i direktivet är trafik- och lokaliseringsuppgifter samt de uppgifter som behövs för att identifiera en abonnent eller användare.

I det följande används det samlande begreppet trafikuppgifter för samtliga nämnda uppgifter.

Direktivet om lagring av trafikuppgifter syftar till att säkerställa att uppgifterna finns tillgängliga för utredning, avslöjande och åtal som gäller allvarliga brott. Direktivet anger de kategorier av uppgifter som ska lagras. Dessa kategorier är uppdelade på fast och mobil telefoni samt Internetåtkomst, e-post och Internettelefoni. De uppgifter som ska lagras svarar främst på frågorna *vem* kommunicerade med vem, *när* skedde det, *var* befann sig de som kommunicerade och *vilken* typ av kommunikation användes. Uppgifterna får dock inte avslöja innehållet i en kommunikation. Direktivet anger lagringstiden till minst sex månader och högst två år och innehåller därutöver bestämmelser om bl.a. vem som ska lagra uppgifterna och krav på säkerhet.

Direktivet om lagring av trafikuppgifter ålägger medlemsstaterna att genomföra bestämmelserna i nationell rätt senast den 15 september 2007. När det gäller Internetåtkomst, e-post och Internettelefoni finns en möjlighet att skjuta upp genomförandet av direktivet till och med den 15 mars 2009. Den möjligheten har Sverige utnyttjat.

Vårt uppdrag är att lämna förslag till hur direktivet om lagring av trafikuppgifter ska genomföras i svensk rätt (dir. 2006:49, se bilaga 1). Uppdraget skulle redovisas senast den 1 april 2007. Vi drog emellertid tidigt den slutsatsen att det inte var meningsfullt att först föreslå regler om lagring av trafikuppgifter som enbart rörde fast och mobil telefoni för att senare återkomma med förslag rörande övriga delar. I stället behövde förslagen presenteras i ett sammanhang. Detta ledde till att regeringen förlängde uppdraget genom tilläggsdirektiv till den 1 november 2007 (dir. 2007:37, se bilaga 2).

1.2 Vårt arbete

Vårt uppdrag innebär att vi ska lämna förslag till en rättslig reglering om lagring av trafikuppgifter som tillgodoser både behovet av bekämpning av allvarlig brottslighet och skyddet för medborgarnas integritet. Enligt våra direktiv ska vi arbeta med sakkunniga, experter och referensgrupper. Vi ska särskilt uppmärksamma behovet av samråd med berörda myndigheter samt med företrädare för berörda branscher och med näringslivet.

Vi har haft sammanträden och mer informella kontakter med de sakkunniga, experterna och deltagarna i utredningens referensgrupper. I den kretsen finns företrädare för flera av departementen i Regeringskansliet, Datainspektionen, Domstolsverket, Ekobrottsmyndigheten, Konkurrensverket, Post- och telestyrelsen, Rikskriminalpolisen, Säkerhetspolisen, Tullverket, Åklagarmyndigheten, Svenskt Näringsliv, Sveriges Advokatsamfund, Sveriges Kommuner och Landsting samt för flera av leverantörerna på marknaden för elektronisk kommunikation. Vid särskilda möten har synpunkter inhämtats från Post- och telestyrelsen, Rikspolisstyrelsen, Säkerhetspolisen, Åklagarmyndigheten, Integritetsskyddskommittén (Ju 2004:05), Svenskt Näringsliv och Sveriges Advokatsamfund.

Vi har också genomfört en hearing för att få de integritetsfrågor som blir aktuella vid lagring av trafikuppgifter belysta.

Utredningen har haft en referensgrupp med representanter för riksdagspartierna. Utifrån direktivet om lagring av trafikuppgifter och regeringens direktiv rörande vårt arbete har det inom denna referensgrupp funnits en relativt bred enighet i de frågor som behandlas i betänkandet. De synpunkter som har anförts har behandlats i anslutning till de olika delarna i betänkandet.

Vi har följt det arbete som EU:s organ och medlemsstaterna har initierat med anledning av de nationella genomförandena av direktivet. Dessutom har vi inhämtat upplysningar om den rättsliga regleringen och planerade förändringar i den nationella rätten i några av de närliggande EU-länderna, företrädesvis Danmark, Finland och de baltiska staterna. Vi har deltagit vid kommissionens ”genomförandemöten” i Bryssel, haft informella kontakter med tjänstemän i många länder rörande genomförandeåtgärderna i respektive land och möten med företrädare för det danska justitsministeriet och Storbritanniens Home Office.

Vi har även, i enlighet med vad som sägs i direktiven och som framgår i det följande, uppmärksammat sådana pågående kommittéarbeten och lagförslag som har beröringspunkter med uppdraget.

1.3 Betänkandets disposition

I ett inledande avsnitt om bakgrunden m.m. redovisas de nuvarande bestämmelserna i lagen (2003:389) om elektronisk kommunikation (LEK) som gäller behandling av uppgifter och de bestämmelser i den lagen och i rättegångsbalken (RB) som reglerar under vilka förutsättningar trafikuppgifter får lämnas ut till de brottsbekämpande myndigheterna, avsnitt 2. Vi presenterar därefter direktivet om lagring av trafikuppgifter i svensk översättning och redovisar något om genomförandet av direktivet i andra länder, avsnitt 3 och 4.

Ett genomförande av direktivet om lagring av trafikuppgifter aktualiserar flera frågor som gäller skyddet för enskildas personliga integritet. Utgångspunkten för direktivet och för våra förslag är regleringen i Europakonventionen om skydd för privatliv och korrespondens och om skyddet för enskildas personliga integritet. Vi för resonemang som gäller integritetsskydd i anslutning till de förslag vi lämnar. Frågorna behandlas också mer samlat i två särskilda avsnitt, varav det första tar upp regleringen av integritetsskyddet i bl.a. regeringsformen och det sista tar upp våra överväganden om

balansen i våra samlade förslag till genomförande av direktivet, avsnitt 5 och 12.

Frågorna om vilka uppgifter som ska lagras och hur lagringsskyldigheten ska fullgöras, vem som ska ha skyldighet att lagra, under hur lång tid lagringen ska ske och för vilka ändamål de trafikuppgifter som lagras får behandlas av leverantörerna, behandlas i avsnitt 6 och 7. De följande tre avsnitten rör frågorna om hur en säker lagring ska uppnås, dvs. vilken kvalitet och säkerhet som ska finnas för de lagrade trafikuppgifterna, om det behöver ske några förändringar av de straff- och skadeståndsrättsliga bestämmelserna och hur tillsynen ska vara utformad, avsnitt 8-10. I det följande avsnittet finns vår bedömning i frågan om det behöver ske några förändringar av bestämmelserna som ger de brottsbekämpande myndigheterna tillgång till trafikuppgifterna, avsnitt 11. Vi gör därefter en analys av om våra förslag till rättslig reglering tillgodoser kravet på balans mellan intresset av att bekämpa allvarlig brottslighet och skyddet mot integritetsintrång, avsnitt 12. Vilka kostnader som uppkommer och hur de ska fördelas mellan det allmänna och leverantörerna och överväganden i frågan om konkurrens på marknaden finns i avsnitt 13 och 14. För att utgöra underlag för en utvärdering av direktivet om lagring av trafikuppgifter ska det föras nationell statistik i olika avseenden. Frågor som gäller statistik behandlas i avsnitt 15 och genomförandefrågor i avsnitt 16.

2 Bakgrund

2.1 Inledning

Utredningar om allvarlig brottslighet innebär bl.a. en kartläggning av vilka personer som har haft kontakt med varandra, när och var kontakterna ägde rum och hur det gick till. En sedan mycket lång tid använd arbetsmetod för den typen av kartläggning har varit att följa personer genom fysisk (visuell) spaning. Det ingår också sedan gammalt i polisens spaningsarbete att kartlägga en misstänkt persons telefonkontakter med andra. Teknikutvecklingen på området elektronisk kommunikation är av stor betydelse i det moderna samhället och innebär stora möjligheter för medborgarna. Kommunikationssätten blir hela tiden fler och kommunikationen avsätter elektroniska spår. De möjligheter som teknikutvecklingen erbjuder används av de flesta medborgare. Samtidigt innebär teknikutvecklingen nya möjligheter för de personer som begår brott. Misstänkta personer använder tekniska hjälpmedel för att kommunicera med varandra och för att planera, genomföra och dölja brott. Det medför att mer traditionella metoder, som t.ex. fysisk spaning, inte är tillräckliga som verktyg för de brottsbekämpande myndigheterna. Numera har tillgången till spaningsuppgifter i form av trafikuppgifter blivit en helt nödvändig och ordinär arbetsmetod när allvarlig brottslighet utreds.

Utvecklingen inom området elektronisk kommunikation innebär att leverantörerna av tjänster och nät i framtiden inte kommer att ha samma behov av att spara trafikuppgifter för sin egen verksamhet. Det medför att viktig information om allvarlig brottslighet på sikt inte kommer att sparas enligt de bestämmelser som tillåter lagring av trafikuppgifter i dag. Syftet med direktivet om lagring av trafikuppgifter är att säkerställa att trafikuppgifter lagras och finns tillgängliga för att kunna lämnas ut till de brottsbekämpande myndigheterna för att användas i utredningar om allvarlig brottslighet. Som en bakgrund till våra förslag redogör vi i detta avsnitt först för

de nuvarande bestämmelserna om behandling av uppgifter, alltså främst frågan om för vilka ändamål leverantörerna får lagra trafikuppgifter i dag, och därefter för de bestämmelser som ger brottsbekämpande myndigheter tillgång till uppgifterna. Vi går också igenom bestämmelserna om s.k. anpassningsskyldighet, dvs. skyldigheten för leverantörer att i vissa fall anpassa sin verksamhet så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas. Vi kommer därefter in på det uppdrag som Beredningen för rättsväsendets utveckling (BRU) hade och de förslag som beredningen lämnade avseende tillgången till uppgifter om elektronisk kommunikation i brottsbekämpningen.

2.2 Bestämmelserna om behandling av uppgifter

2.2.1 Inledning

Personuppgifter behandlas i en rad olika sammanhang både i allmän och privat verksamhet och en stor del av behandlingen sker på automatisk väg. När moderna kommunikationslösningar används av medborgarna i både privata och andra sammanhang innebär tekniken att trafikuppgifter genereras och behandlas. Trafikuppgifter är ofta men inte alltid personuppgifter.

Behandling av personuppgifter är generellt reglerad i personuppgiftslagen (1998:204, PUL). Därutöver finns en rad olika författningar som reglerar behandling av personuppgifter i olika verksamheter. För rättsväsendets del gäller ett antal registerförfattningar som reglerar respektive myndighets behandling av personuppgifter.

För behandling av trafikuppgifter som också är personuppgifter finns särskilda regler i lagen om elektronisk kommunikation som mer specifikt reglerar behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

2.2.2 Personuppgiftslagen

Europaparlamentet och rådet antog den 24 oktober 1995 direktivet om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet [95/46/EG]). Syftet med direktivet är att garantera en hög skyddsnivå när det gäller enskildas fri- och rättigheter

med avseende på behandling av personuppgifter och en likvärdig skyddsnivå i alla medlemsstater.

Dataskyddsdirektivet genomförs i svensk rätt genom personuppgiftslagen. Syftet med lagen är att skydda fysiska personer som är i livet mot att deras personliga integritet kränks genom felaktig behandling av personuppgifter. Personuppgiftslagen innehåller de generella regler som följer av dataskyddsdirektivet i fråga om behandling av personuppgifter men omfattar också sådant som faller utanför gemenskapsrätten. Personuppgiftslagen är subsidiär till annan lagstiftning, dvs. i den mån det finns särreglering i annan lag eller förordning som avviker från personuppgiftslagen gäller de bestämmelserna.

Med personuppgift avses enligt 3 § all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. En personuppgift är varje upplysning som avser en identifierbar eller identifierad fysisk person. En identifierbar person är någon som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, psykiska, ekonomiska, kulturella eller sociala identitet (prop. 1997/98:44 s. 117 och 163). Vid bedömningen av om en person är identifierbar ska alla hjälpmedel beaktas som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den personuppgiftsansvarige eller av någon annan person. Det krävs endast att en fysisk person är möjlig att identifiera med hjälp av informationen, inte att den personuppgiftsansvarige själv förfogar över samtliga uppgifter som gör identifieringen möjlig.

Den personuppgiftsansvarige ska se till att personuppgifter alltid behandlas på ett korrekt sätt och i enlighet med god sed samt att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifterna får inte behandlas för något ändamål som är oförenligt med det syfte för vilket de samlades in. Fler personuppgifter får inte behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen. Den personuppgiftsansvarige ska se till att de personuppgifter som behandlas är riktiga och om nödvändigt aktuella, att alla rimliga åtgärder vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga med hänsyn till ändamålen med behandlingen samt att personuppgifter inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen (9 §). Med behandling av personuppgifter avses varje åtgärd som vidtas i fråga om uppgifter, som t.ex. att samla in, registrera, organisera,

lagra, bearbeta och sprida uppgifter. Den behandling av personuppgifter som en fysisk person utför som ett led i en verksamhet av rent privat natur faller emellertid enligt 6 § utanför lagen.

Personuppgiftslagen reglerar när en behandling av personuppgifter är tillåten (10 §). Behandlingen är tillåten om den registrerade har lämnat sitt samtycke till behandlingen eller behandlingen är nödvändig för vissa angivna ändamål. De ändamålen är att

a) ett avtal med den registrerade ska kunna fullgöras eller åtgärder som den registrerade begärt ska kunna vidtas innan ett avtal träffas,

b) den personuppgiftsansvarige ska kunna fullgöra en rättslig skyldighet,

c) vitala intressen för den registrerade ska kunna skyddas,

d) en arbetsuppgift av allmänt intresse ska kunna utföras,

e) den personuppgiftsansvarige eller en tredje man till vilken personuppgifter lämnas ut ska kunna utföra en arbetsuppgift i samband med myndighetsutövning, eller

f) ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige eller hos en sådan tredje man till vilken personuppgifterna lämnas ut ska kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.

2.2.3 Telelagen

Telelagen (1993:597) infördes i samband med att verksamheten i Televerket överfördes till Telia AB. I propositionen Ändringar i telelagen m.m. (prop. 1998/99:92 s. 29 f.) redogjorde regeringen för innehållet i det s.k. teledataskyddsdirektivet (97/66/EG). Regeringen nämnde bl.a. att syftet med direktivet var att genom en harmonisering av medlemsstaternas bestämmelser om behandling av personuppgifter säkerställa en likvärdig nivå på integritetsskyddet och en fri rörlighet inom gemenskapen för personuppgifter inom telekommunikationsområdet och för teleutrustning och teletjänster. I direktivet fanns angivet att uppgifter om abonnenter och användare som teleoperatören behandlar för att koppla upp samtal skulle utplånas eller åtminstone avidentifieras vid samtalets slut. Nödvändiga uppgifter för fakturering av abonnenter och för betalning av samtrafikuppgifter fick dock behandlas under preskriptionstiden.

I propositionen föreslog regeringen, mot bakgrund av innehållet i direktivet, vissa ändringar i telelagen. Ändringarna trädde i kraft den 1 juli 1999 och innebar bl.a. följande.

Enligt huvudregeln i 49 § telelagen skulle uppgifter som gällde ett särskilt telemeddelande utplånas eller avidentifieras av teleoperatören vid samtalets slut eller när meddelandet nått mottagaren. Den skyldigheten gällde, enligt paragrafens andra stycke, inte för behandling av sådana uppgifter som var nödvändiga för fakturering av abonnenter och betalning av samtrafikavgifter till dess fordringen var betald eller preskriberad. Om abonnenten hade gett sitt samtycke fick sådana uppgifter behandlas för marknadsföring av teletjänster i den egna verksamheten.

Ytterligare undantag från kravet i 49 § första stycket om omedelbart utplånande eller avidentifiering av uppgifterna fanns i 50 § och gällde för det första meddelanden som omfattades av beslut om hemlig teleavlyssning eller hemlig teleövervakning. För det andra fanns undantag från det s.k. lagringsförbudet i den utsträckning det var nödvändigt för att förhindra eller avslöja obehörig användning av telenätet. Det tredje undantaget i 50 § avsåg det fallet att abonnenten begärde att störande samtal skulle spåras. Uppgifter som identifierade den uppringande abonnenten kunde då lagras och hållas tillgängliga av teleoperatören.

Ett utlämnande av trafikuppgifter till de brottsbekämpande myndigheterna med stöd av 47 § telelagen (motsvarande 6 kap. 22 § LEK) förutsatte att uppgifterna fanns tillgängliga hos teleoperatörerna när de begärdes utlämnade. Eftersom det blev en huvudregel enligt telelagen att trafikuppgifter skulle utplånas eller avidentifieras diskuterades i lagstiftningsärendet om regleringen skulle innebära att de brottsbekämpande myndigheterna i fortsättningen skulle gå miste om viktig information. I det remissförfarande som föregick regeringens proposition om förändringarna i telelagen anförde Rikspolisstyrelsen att skyldigheten att utplåna eller avidentifiera de historiska uppgifterna, i vart fall då teleavlyssning m.m. inte förevarit, skulle hindra polisens möjligheter att utreda brott. I propositionen 1998/99:92 (s. 33) anfördes att regeringen hade viss förståelse för Rikspolisstyrelsens bedömning men det konstaterades att det inte var möjligt att införa vidare undantag från skyldigheten att utplåna uppgifter. Mot bakgrund av Rikspolisstyrelsens remisskritik uttalade regeringen dock att det kunde finnas anledning att i samarbetet inom Europeiska unionens tredje pelare återkomma till frågan om utnyttjande av teleuppgifter i brottsbekämpningssammanhang. Vid behandlingen i riksdagen anförde Trafikutskottet

(1998/99:TU12 s. 7) att utskottet förutsatte att regeringen inom ramen för EU-samarbetet skulle verka för en effektiv brottsbekämpning och för riksdagen redovisa de resultat som därvid uppnåtts.

I 22 § teleförordningen (1997:399) föreskrev regeringen vilka uppgifter rörande ett särskilt telemeddelande som fick behandlas till dess att fordran var betald eller preskriberad. Det gällde uppgifter som var nödvändiga för fakturering av en abonnent eller för betalning av samtrafikavgifter (49 § andra stycket telelagen). Uppgifter fick lagras om abonnentens teleadress, den anropades teleadress, samtalets art, samtalets starttidpunkt och längd eller den överförda datamängden, datum för samtalsanropet, det totala antalet enheter som debiteras för en redovisningsperiod, andra uppgifter om eller i samband med betalningen, såsom förskottsbetalning, avbetalning, betalningspåminnelse och avstängning samt typ av utrustning och abonnentutrustningens nummer eller annan identifikation.

2.2.4 Lagen om elektronisk kommunikation

Allmänt om lagen

År 2000 presenterade EG-kommissionen ett förslag till nytt regelverk för elektronisk kommunikation i syfte att modernisera gemenskapens lagstiftning på området. Förslaget lades fram mot bakgrund av den snabba utvecklingen av teknik och marknader för elektronisk kommunikation. Kommissionens förslag behandlades av Europaparlamentet och rådet. Det regelverk som senare beslutades omfattar flera direktiv, bl.a. direktivet (2002/21/EG) om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektivet), direktivet (2002/20/EG) om auktorisation för elektroniska kommunikationsnät och kommunikationstjänster (auktorisationsdirektivet), direktivet (2002/19/EG) om tillträde till och samtrafik mellan elektroniska kommunikationsnät och tillhörande faciliteter (tillträdesdirektivet), direktivet (2002/22/EG) om samhällsomfattande tjänster och användares rättigheter avseende elektroniska kommunikationsnät och kommunikationstjänster (USO-direktivet) och direktivet (2002/58/EG) om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

För att genomföra dessa direktiv tillsatte regeringen under år 2001 en utredning, Utredningen om elektronisk kommunikation

(den s.k. e-komutredningen). På grundval av utredningens arbete infördes lagen om elektronisk kommunikation. Lagen ersatte i juli 2003 telelagen och lagen (1993:599) om radiokommunikation.

E-komutredningen angav i sitt delbetänkande Lag om elektronisk kommunikation (SOU 2002:60 s. 267) att elektronisk kommunikation ofta används som en samlande benämning på den verksamhet som bedrivs inom det nya område som växer fram mot bakgrund av bl.a. konvergensutvecklingen och Internet. E-komutredningen ansåg att begreppet elektronisk kommunikation behövde konkretiseras men konstaterade att varken ramdirektivet eller de s.k. särdirektiven innehåller någon definition av begreppet. Däremot definieras vad som menas med elektroniska kommunikationsnät och elektroniska kommunikationstjänster i ramdirektivet.

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

Till skillnad mot telelagen är lagen om elektronisk kommunikation tillämplig inte endast på telefoni och datakommunikation utan även på utsändningar till allmänheten av program i ljudradio och TV.

Behandlingen av uppgifter

Europaparlamentets och rådets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation) trädde i kraft den 31 juli 2002 och ersatte teledataskyddsdirektivet. Direktivet 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.

Direktivet om integritet och elektronisk kommunikation genomförs huvudsakligen i 6 kap. LEK (prop. 2002/03:110 s. 69 f. och 248). Bestämmelserna i detta kapitel gäller framför personuppgiftslagen avseende behandling av personuppgifter och integritet vid tillhandahållande av elektroniska kommunikationsnät och elektroniska kommunikationstjänster samt vid abonnentupplysning.

Artikel 6 i direktivet om integritet och elektronisk kommunikation reglerar behandlingen av trafikuppgifter. En trafikuppgift är enligt 6 kap. 1 § LEK en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande. I den definitionen innefattas även sådana lokaliseringsuppgifter som visar den geografiska positionen för en användare av en allmänt tillgänglig elektronisk kommunikationstjänst, t.ex. i vilken cell i ett cellulärt uppbyggt mobilkommunikationssystem, som t.ex. GSM, som en användare befinner sig (prop. 2002/03:110 s. 260). Någon motsvarande definition av trafikuppgift fanns inte i telelagen. Enligt förarbetena till lagen om elektronisk kommunikation (prop. 2002/03:110 s. 389 f.) torde begreppet trafikuppgifter avse samma slag av uppgifter som avsågs i 49 § telelagen, där det talades om uppgifter som angår ett särskilt telemeddelande. Lokaliseringsuppgifter är med andra ord trafikuppgifter under förutsättning att de behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande eller de angår ett särskilt telemeddelande.

Enligt artikel 15 i det angivna direktivet (se vidare avsnitt 6.4) får medlemsstaterna genom lagstiftning begränsa omfattningen av de rättigheter och skyldigheter som anges i bl.a. artikel 6. Det får ske bl.a. när en sådan begränsning är nödvändig i ett demokratiskt samhälle samt lämplig och proportionell för att skydda nationell säkerhet, försvaret och allmän säkerhet samt för förebyggande, undersökning och avslöjande av brott och åtal för brott. En begränsning kan bl.a. innebära att uppgifter får bevaras under en begränsad period.

Bestämmelserna om bevarande av trafikuppgifter finns främst i 6 kap. 5, 6 och 8 §§ LEK och motsvarar i huvudsak den tidigare regleringen i 49 och 50 §§ telelagen. Huvudregeln framgår av 6 kap. 5 § LEK och innebär att trafikuppgifter som avser användare eller abonnenter som är fysiska personer och som lagras eller behandlas på annat sätt av den som bedriver anmälningspliktig verksamhet, ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande.

Liksom telelagen tillåter lagen om elektronisk kommunikation att uppgifterna sparas för viss behandling. Enligt 6 kap. 6 § första stycket LEK får de trafikuppgifter som krävs för abonnentfakturering och betalning av avgifter för samtrafik behandlas till dess att fordran är betald eller preskription har inträtt och det inte längre lagligen går att göra invändningar mot faktureringen eller avgiften. Enligt bestämmelsens andra stycke får uppgifterna också behandlas för att bl.a. marknadsföra elektroniska kommunikationstjänster, om den abonnent eller användare som uppgifterna avser har samtyckt till det. Bestämmelsen i 6 kap. 6 § LEK kompletteras av 35 § förordningen (2003:396) om elektronisk kommunikation, som anger att Post- och telestyrelsen (PTS) får meddela närmare föreskrifter om vilka uppgifter som får behandlas enligt den bestämmelsen i lagen om elektronisk kommunikation (jfr 22 § den upphävda teleförordningen). PTS har inte meddelat några sådana föreskrifter.

Även i 6 kap. 8 § LEK finns bestämmelser som tillåter att trafikuppgifter sparas. Det rör för det första fallet att en myndighet behöver ha tillgång till sådana uppgifter för att lösa tvister. För det andra rör det elektroniska meddelanden som befordras eller har expedierats eller beställts till eller från en viss adress i ett elektroniskt kommunikationsnät som omfattas av beslut om hemlig teleavlyssning eller hemlig teleövervakning. Det tredje fallet gäller när trafikuppgifterna är nödvändiga för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Enligt förarbetena (prop. 2002/03:110 s. 392) får uppgifterna inte sparas längre än vad som är nödvändigt för syftet. Längre tid än ett år bör inte godtas, om det inte föreligger särskild anledning, som att tvist har uppkommit eller förundersökning inletts i ett särskilt fall. I propositionen anfördes också att bestämmelsen även omfattar lagring av uppgifter för utredning och lagföring av brott, förutsatt att det sker i syfte att förhindra eller avslöja en obehörig användning av nätet eller tjänsten i fråga.

Ytterligare undantag från huvudregeln i 6 kap. 5 § LEK om att trafikuppgifter ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande finns i 6 kap. 13 § LEK. Enligt det bestämmelsen får skyddet mot nummerpresentation temporärt åsidosättas för att spåra störande samtal. Det kan vara fråga om hotfulla samtal eller rena okynnessamtal. Om en abonnent begär spårning av sådana samtal, får uppgifter som identi-

fierar den anropande abonnenten lagras och hållas tillgängliga för abonnenten på begäran.

Det finns lokaliseringsuppgifter som inte är trafikuppgifter (6 kap. 9 § LEK). Exempel på sådana uppgifter kan enligt förarbetena vara en positionsbestämning av en mobiltelefon via satellit, framförallt GPS-systemet (prop. 2002/03:110 s. 261). Lokaliseringsuppgifter som inte är trafikuppgifter omfattas inte av regleringen som specifikt gäller trafikuppgifter enligt lagen om elektronisk kommunikation. Det innebär t.ex. att de inte behöver utplånas eller avidentifieras enligt bestämmelsen i 6 kap. 5 § LEK.

2.3 Bestämmelserna om tillgång till trafikuppgifter

2.3.1 Rättegångsbalken

Hemlig teleavlyssning

Våra överväganden rör trafikuppgifter som lämnas ut enligt reglerna i rättegångsbalken om hemlig teleövervakning. Trafikuppgifter avslöjar inte innehållet i de meddelanden som uppgifterna avser. Det är i stället efter domstolsbeslut om hemlig teleavlyssning som de brottsbekämpande myndigheterna kan få tillgång till innehållet i meddelanden. Förutsättningarna för beslut om hemlig teleövervakning och hemlig teleavlyssning är delvis desamma. Vi redogör därför relativt utförligt även för bestämmelserna om hemlig teleavlyssning.

Före andra världskriget saknades regler om telefonavlyssning i brottsutredande syfte. Det antogs att det krävdes Kungl. Majt:s beslut i varje särskilt fall för att avlyssning skulle kunna genomföras. Förslag till regler om telefonavlyssning i samband med brottsutredning lades första gången fram i betänkandet Förslag till rättegångsbalk (SOU 1938:43 och 44, se prop. 1975/76:202 s. 85).

Redan före andra världskriget infördes dock regler om telefonavlyssning i två av de lagar som föranleddes av kriget, nämligen lagen (1939:724) om särskilda tvångsmedel vid utredning rörande brott som avses i 8 eller 19 kap. strafflagen m.m. och lagen (1940:3) om vissa tvångsmedel vid krig eller krigsfara m.m. Båda lagarna fick provisorisk karaktär och skulle gälla till utgången av mars 1941. Giltighetstiden för 1939 års lag förlänges inte medan däremot 1940 års lag successivt förlängdes och upphörde att gälla vid utgången av juni 1945.

Mellan den 1 juli 1945, då 1940 års lag upphörde att gälla och den 1 januari 1948, då rättegångsbalken trädde i kraft, saknades bestämmelser om telefonavlyssning i svensk lag.

Det utrikespolitiska läget ansågs år 1952 påkalla utvidgade möjligheter till bl.a. telefonavlyssning vid vissa brott mot rikets yttre och inre säkerhet. Efter mönster från 1939 och 1940 års lagar tillkom en ny provisorisk lag, lagen (1952:98) med särskilda bestämmelser om tvångsmedel i vissa brottmål (benämnd 1952 års tvångsmedelslag). Lagen har förlängts och gäller enligt det senaste beslutet till utgången av år 2007 (se dock prop. 2007/08:9 och Ds 2007:2).

De nuvarande huvudsakliga bestämmelserna om hemlig teleavlyssning och hemlig teleövervakning finns i 27 kap. 18-30 §§ RB. Hemlig teleavlyssning innebär att telemeddelanden som befordras eller har befordrats till eller från ett visst telefonnummer, en kod eller en annan teleadress avlyssnas eller spelas in i hemlighet genom ett tekniskt hjälpmedel. Bestämmelser som för vissa fall ger rätt att använda hemlig teleavlyssning finns också i 1952 års tvångsmedelslag, lagen (1988:97) om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. och lagen (1991:572) om särskild utlänningskontroll (se avsnitt 2.3.4).

Med telemeddelande avses i rättegångsbalken och i övriga nämnda lagar detsamma som i 6 kap. 19 § tredje stycket LEK, nämligen ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare. Exempel på telemeddelanden som får avlyssnas enligt bestämmelserna om hemlig teleavlyssning är telefonsamtal, telefax, elektronisk post och annan datakommunikation.

För att ett telemeddelande ska få avlyssnas krävs att meddelandet befordras eller har befordrats till eller från ett telefonnummer, en kod eller annan teleadress. Med teleadress avses t.ex. ett abonnemang, en enskild anknytning, adressen för elektronisk post, en kod eller någon annan motsvarande tillförlitlig identifieringsmetod. Elektronisk post får alltså avlyssnas under samma förutsättningar som telefonsamtal, dvs. innehållet i meddelandet görs tillgängligt för de brottsutredande myndigheterna.

Tillstånd till hemlig teleavlyssning kan ges av rätten när förundersökningen rör ett brott för vilket det inte är föreskrivet lindrigare straff än fängelse i två år, anstiftan eller medhjälp, eller försök, förberedelse eller stämpling till ett sådant brott. Tillstånd kan också

ges vid förundersökning angående annat brott, om det med hänsyn till omständigheterna kan antas att brottets straffvärde överstiger fängelse i två år (se 27 kap. 18 § andra stycket RB och prop. 2002/03:74 s. 31 ff.).

Beslutet får avse en teleadress som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte. Exempel på det sistnämnda kan vara en teleadress som innehas av en närstående till en misstänkt eller en teleadress på den misstänktes arbetsplats.

Beslutet får även avse en teleadress som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta (27 kap. 20 § första stycket RB).

Beslutet ska avse telemeddelanden som utväxlas under en i beslutet viss angiven tid.

När åklagarens ansökan om tillstånd till hemlig teleavlyssning har kommit in till rätten, ska rätten så snart som möjligt utse ett offentligt ombud i ärendet. Det offentliga ombudet, som ska vara eller ha varit advokat eller ha varit ordinarie domare, har till uppgift att bevaka enskildas integritetsintressen i ärendet (27 kap. 26-30 §§ RB). Det offentliga ombudet ska lyfta fram alla integritetsaspekter, som t.ex. skyddet för tredje mans integritet.

Hemlig teleövervakning

Bestämmelser om hemlig teleövervakning infördes i rättegångsbalken år 1989. Dessförinnan fick s.k. telefonövervakning, innefattande bl.a. uppgifter om samtal som expedierats eller beställts till eller från en telefonapparat, bara användas i de fall som reglerades i 1952 års tvångsmedelslag och 1988 års lag om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m.

Före sekretesslagens tillkomst år 1980 (se nedan) kunde polisen få uppgifter från Televerket om samtal till och från en viss telefon. Det ansågs kunna ske utan hinder av då gällande sekretessbestämmelser. Polisen använde sig också av denna upplysningskälla i sitt arbete. I propositionen till bestämmelserna om hemlig teleövervakning (prop. 1988/89:124 s. 47 f.) uttalade regeringen dock att sekretesslagen hindrade Televerket att lämna ut sådana uppgifter om

det inte fanns ett författningsstöd för det, som 1952 års lag. Regeringen konstaterade också att när tillstånd till teleavlyssning hade meddelats, torde uppgift om de samtal som ringts till eller från den avlyssnade apparaten ändå lämnas till de brottsutredande myndigheterna. Enligt regeringens motiv i propositionen fanns det en stor fördel från brottsutredningssynpunkt om teleövervakning kunde användas som tvångsmedel vid sidan om teleavlyssning med mindre stränga villkor för användningen.

Hemlig teleövervakning (27 kap. 19-25 §§ RB) innebär att det i hemlighet hämtas in uppgifter om telemeddelanden som befordras eller har befordrats till eller från en teleadress som under den tid som tillståndet avser innehas eller har innehafts av den misstänkte eller annars kan antas ha använts eller komma att användas av den misstänkte. Det är alltså fråga om såväl *realtidsuppgifter* (uppgifter som genereras från det att beslutet om tvångsmedlet börjat verkställas) som *historiska uppgifter*. Hemlig teleövervakning får även avse en teleadress som det finns synnerlig anledning att anta att den misstänkte under den tid som tillståndet avser har ringt till eller på annat sätt kontaktat eller kommer att ringa till eller på annat sätt kontakta (27 kap. 20 § första stycket RB). Uppgifter om innehållet i telemeddelanden (avlyssning) omfattas inte av hemlig teleövervakning.

Liksom vid hemlig teleavlyssning finns bestämmelser som för vissa fall ger rätt att använda hemlig teleövervakning i 1952 års tvångsmedelslag, lagen om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. och lagen om särskild utlänningskontroll (se avsnitt 2.3.4).

Om hemlig teleövervakning avser ett telefonnummer kan en brottsutredande myndighet med hjälp av tvångsmedlet få uppgift om bl.a. till vilka telefonnummer samtal befordras eller har befordrats från det övervakade numret, från vilka telefonnummer samtal befordras eller har befordrats till det numret, vid vilka tidpunkter samtalen sker eller har skett och längden på samtalen. Är det i stället fråga om elektronisk post, finns möjligheten att genom tvångsmedlet få liknande uppgifter, exempelvis till vilka adresser meddelanden har expedierats från den övervakade adressen. Ett beslut om hemlig teleövervakning kan även innebära att ett telemeddelande hindras att nå fram till eller nå från en viss teleadress. Den möjligheten kan användas för att exempelvis förhindra kontakter, t.ex. varnande samtal, mellan personer som är missänkta för brott. Ett annat exempel är att kommunikation med en mobiltelefon förhindras för att tvinga en misstänkt person att i stället använda sig av en

viss annan telefon (SOU 1998:46 s. 477). I fråga om mobiltelefonsamtal är det också möjligt att genom hemlig teleövervakning få reda på från vilket geografiskt område ett telefonsamtal rings och var mottagaren av samtalet befinner sig (lokaliseringsuppgifter).

Tillstånd till hemlig teleövervakning får meddelas av rätten vid förundersökning om brott, samt även anstiftan och medhjälp till brott, för vilket det inte är föreskrivet lindrigare straff än fängelse i sex månader, brott enligt 4 kap. 9 c § brottsbalken (dataintrång), 16 kap. 10 a § brottsbalken (barnpornografibrott som inte är att anse som ringa), 1 § narkotikastrafflagen (1968:64, narkotikabrott) eller brott enligt 6 § första stycket lagen (2000:1225) om straff för smuggling (narkotikasmuggling). Vidare får tillstånd meddelas vid misstanke om försök, förberedelse eller stämpling till nämnda brott (27 kap. 19 § andra stycket RB).

Gemensamma förutsättningar för hemlig teleavlyssning och hemlig teleövervakning enligt rättegångsbalken

Hemlig teleavlyssning och hemlig teleövervakning får användas endast i förundersökning där någon är skäligen misstänkt för ett visst brott och åtgärden är av synnerlig vikt för utredningen om brottet (27 kap. 20 § första stycket RB). Uttrycket synnerlig vikt för utredningen behöver inte nödvändigtvis avse att avlyssningen eller övervakningen ska ge avgörande bevisning som omedelbart kan leda till en fällande dom. Synnerlig vikt för utredningen inrymmer däremot ett kvalitetskrav beträffande de upplysningar som åtgärden kan ge. Det måste vara fråga om uppgifter som har betydelse för att föra utredningen om brottet framåt. Uttrycket omfattar också ett krav på att utredningsläget ska göra avlyssningen eller övervakningen nödvändig (prop. 1988/89:124 s. 44 f.).

Tillståndstiden får inte bestämmas längre än nödvändigt och får inte överstiga en månad, såvitt gäller tid som infaller efter beslutet, alltså vid framtida meddelanden eller uppgifter (27 kap. 21 § andra stycket RB). Tillstånd kan dock förnyas på begäran av åklagaren. Domstolens beslut om tillstånd går enligt 30 kap. 12 § RB genast i verkställighet.

Från tillämpningsområdet för hemlig teleavlyssning och hemlig teleövervakning undantas telemeddelanden som endast befordras eller har befordrats inom ett telenät som med hänsyn till sin begränsade omfattning och omständigheterna i övrigt får anses vara av mindre betydelse från allmän kommunikationssynpunkt (27 kap.

20 § andra stycket RB). Därmed avses bl.a. system för snabbtelefoner, porttelefoner, PC-nät och liknande utrustning inom eller intill en bostad, hörslingor för hörselskadade eller interna system för personsökning i form av fasta installationer. Även interna telekommunikationer på mindre arbetsplatser via t.ex. PC-nät utgör telenät av mindre betydelse. Motsatsen gäller vanligtvis beträffande sådana telenät som är uppkopplade mot och används för kommunikation via allmänt tillgängliga telenät eller större företagsnät. Detsamma gäller fristående datorer som är försedda med modem och datorer i t.ex. små interna nätverk som via andra nätverk kommunicerar med varandra eller med t.ex. elektroniska anslagstavlor, informationsdatabaser eller andra informationssystem. Om kommunikationen endast sker internt inom ett slutet nät bör det krävas att nätet är av större omfattning för att en tvångsåtgärd ska få äga rum. Frågan om ett telenät ska anses vara av mindre betydelse prövas utifrån en samlad bedömning av de olika omständigheter som rör ett telenäts betydelse från allmän kommunikationssynpunkt. Vid bedömningen kan bl.a. antalet anslutningar, geografisk spridning och hur utrustningen fungerar och används ha betydelse (prop. 1994/95:227 s. 27 och 31 och Fitger, Rättegångsbalken 2 s. 27:41).

Beslag och editionsföreläggande avseende telemeddelanden

Det har i praxis förelegat en osäkerhet huruvida beslag och editionsföreläggande kan användas för att få uppgifter som finns om telemeddelanden *hos leverantörer*. Det har förekommit att de brottsutredande myndigheterna har berett sig tillgång till uppgifterna med hjälp av reglerna om husrannsakan och beslag i 27 och 28 kap. RB eller genom att utverka editionsföreläggande enligt 38 kap. 4 § RB. Det rör alltså sådana fall där det annars finns regler om utlämnande av uppgifter enligt rättegångsbalken och numera lagen om elektronisk kommunikation (SOU 1998:46 s. 71 och JO 1997/98 s. 47 ff.). Regeringen har uttalat att uppgifter om telemeddelanden, eller, med det uttryck som används i 6 kap. 20 § första stycket 3 LEK, ”uppgifter som angår ett särskilt elektroniskt meddelande”, hos leverantörer inte kan hämtas in med stöd av editionsföreläggande och husrannsakan i förening med beslag i fall där annars dessa andra regler för utfående av uppgifter gäller. Enligt regeringen får detta anses följa redan av allmänna principer och något lagstiftningsbehov finns därför inte (prop. 2002/03:74 s. 45 f.).

Det bör nämnas att regeringens uttalande inte avser möjligheten för de brottsutredande myndigheterna att genomföra t.ex. husrannsakan i förening med beslag *hos annan än leverantör* för att få fram uppgifterna. Det kan t.ex. röra sig om innehållet i en telefonsvarare som enbart den enskilde förfogar över eller band med inspelade telemeddelanden som förvaras av den enskilde (SOU 1998:46 s. 373).

Teleövervakningsuppgifter hos den enskilde kan finnas t.ex. i en nummerpresentatör eller i en mobiltelefon samtidigt som dessa uppgifter finns i leverantörens system. Det kan röra uppgift om inkomna eller utgående samtal och senast slagna nummer, När det gäller uppgifter som finns *både hos den enskilde och hos leverantören* kan uppgifterna bli åtkomliga för de brottsutredande myndigheterna på båda sätten, dvs. genom t.ex. hemlig teleövervakning eller genom beslag eventuellt i kombination med husrannsakan hos den enskilde (SOU 1998:46 s. 373).

2.3.2 Lagen om elektronisk kommunikation

Tillgången till trafikuppgifter

Vissa bestämmelser i lagen om elektronisk kommunikation knyter an till rättegångsbalkens regler om hemlig teleavlyssning och hemlig teleövervakning. Enligt 6 kap. 19 § LEK ska vissa verksamheter bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs. Innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand. Detta är den s.k. anpassningsskyldigheten (se vidare avsnitt 2.5.2).

I lagen om elektronisk kommunikation, liksom tidigare i telelagen, finns också bestämmelser som ger de brottsbekämpande myndigheterna möjligheter att under särskilt angivna omständigheter utan domstolsprövning få tillgång till bl.a. uppgifter som angår s.k. elektroniska meddelanden. Det rör sig här om *historiska uppgifter*.

Vid utlämnande av sådana uppgifter enligt lagen om elektronisk kommunikation är det i princip fråga om samma typ av uppgifter som myndigheterna kan få genom hemlig teleövervakning.

Regleringen i lagen om elektronisk kommunikation har sin utgångspunkt i att trafikuppgifterna av integritetshänsyn omfattas av tystnadsplikt. När uppgifterna lämnas ut till brottsbekämpande

myndigheter sker det genom särskilda bestämmelser om undantag från tystnadsplikten.

För samtliga uppgifter som omfattas av den lagringsskyldighet direktivet om lagring av trafikuppgifter anger gäller *tystnadsplikten* i 6 kap. 20 § LEK. Den bestämmelsen lyder på följande sätt.

> Den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till
>
> 1. uppgift om abonnemang,
> 2. innehållet i ett elektroniskt meddelande, eller
> 3. annan uppgift som angår ett särskilt elektroniskt meddelande,
>
> får inte obehörigen föra vidare eller utnyttja det han fått del av eller tillgång till.
>
> Sådan tystnadsplikt gäller inte i förhållande till den som har tagit del i utväxlingen av ett elektroniskt meddelande eller som på annat sätt har sänt eller tagit emot ett sådant meddelande.
>
> Tystnadsplikt i fråga om uppgifter som avses i första stycket 1 och 3 gäller inte heller i förhållande till innehavare av ett abonnemang som använts för ett elektroniskt meddelande.

Som följer av bestämmelsens första stycke gäller tystnadsplikten alla leverantörer. Det krävs inte att det nät eller den tjänst som leverantören tillhandahåller är allmänt respektive allmän. Uttrycket i bestämmelsen om vem som träffas av tystnadsplikten (”den som i samband med tillhandahållande”) innebär att tillämpningsområdet inte är begränsat till leverantören utan att också andra aktörer omfattas av tystnadsplikten, t.ex. den som på uppdrag av leverantören utför delar av tillhandahållandet av nätet eller tjänsten (se om detta och om undantag från tystnadsplikten PTS:s ”Sammanställning av lagstiftning och praxis kring utlämnande av teleuppgifter” från 2006-11-28).

Enligt 6 kap. 21 § LEK har leverantörerna dessutom tystnadsplikt för uppgift som hänför sig till användning av vissa hemliga tvångsmedel, nämligen hemlig teleavlyssning, hemlig teleövervakning och kvarhållande av försändelser. Denna tystnadsplikt gäller även mot abonnenten.

Det är främst genom de *undantag* från tystnadsplikten som regleras i 6 kap. 22 § första stycket 2 och 3 LEK som de brottsbe-

kämpande myndigheterna har möjligheter att begära och få ut trafikuppgifter. Bestämmelserna lyder på följande sätt.

> Den som tillhandahåller ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och därvid har fått del av eller tillgång till uppgift som avses i 20 § första stycket skall på begäran lämna
>
> -----
>
> 2. uppgift som avses i 20 § första stycket 1 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet, om fängelse är föreskrivet för brottet och det enligt myndighetens bedömning kan föranleda annan påföljd än böter,
>
> 3. uppgift som avses i 20 § första stycket 3 och som gäller misstanke om brott till åklagarmyndighet, polismyndighet eller någon annan myndighet som ska ingripa mot brottet, om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år,
>
> -----

Uppgift om abonnemang, enligt 6 kap. 20 § första stycket 1 LEK, avser uppgifter som identifierar en abonnent och/eller ett abonnemang, framför allt namn, titel, adress och abonnentnummer (t.ex. telefonnummer). Abonnent är enligt 1 kap. 7 § LEK den som har ingått avtal med en leverantör av allmänt tillgängliga elektroniska kommunikationstjänster om tillhandahållande av sådana tjänster.

Även s.k. IMSI-nummer och IP-adresser har ansetts falla in under kategorin uppgift om abonnemang. Det gäller oavsett om IP-adressen är fast eller dynamisk (jfr dock Ds 2005:6 s. 324). En IP-adress tilldelas när t.ex. ett e-postmeddelande skickas på Internet. Varje leverantör disponerar ett visst antal IP-adresser, som ”lånas ut” till abonnenterna. Detta kan ske på permanent basis (s.k. fasta IP-adresser) eller dynamiskt, där abonnenten tilldelas en IP-adress varje gång uppkoppling sker mot leverantören. En fast eller statisk IP-adress innebär alltså att IP-adressen är fast knuten till ett Internetabonnemang och att samma IP-adress därför tilldelas vid varje tillfälle som uppkoppling sker.

Uppgifterna om abonnemang ska som framgår av bestämmelsen lämnas ut om fängelse är föreskrivet för brottet och brottet enligt den brottsbekämpande myndighetens bedömning kan föranleda annan påföljd än böter.

Annan uppgift som angår ett särskilt elektroniskt meddelande, enligt 6 kap. 20 § första stycket 3 LEK, avser t.ex. uppgift om mellan vilka telefonnummer eller IP-adresser som ett elektroniskt meddelande har förmedlats, när och under hur lång tid förbindelsen var uppkopplad, från vilken basstation ett visst samtal skett samt det s.k. IMEI-numret. Uttrycket uppgift som angår ett särskilt elektroniskt meddelande ska inte förstås så att den brottsbekämpande myndigheten måste specificera enskilda meddelanden, t.ex. genom att ange en viss abonnent och tidpunkt för meddelandet. S.k. basstationstömning, där de brottsbekämpande myndigheterna begär uppgifter som omfattas av tystnadsplikt om t.ex. samtliga de mobiltelefoner som har varit uppkopplade för kommunikation och som då haft kontakt med en basstation i närheten av en brottsplats under en begränsad tid, anses vara annan uppgift som angår ett särskilt elektroniskt meddelande. Det rör sig alltså om uppgifter som genereras när ett samtal eller meddelandeutbyte äger rum, inte uppgifter som enbart rör en påslagen telefon. Uppgifterna ska lämnas ut till de brottsbekämpande myndigheterna om det för brottet inte är föreskrivet lindrigare straff än fängelse i två år. Det innebär att inga försöks-, förberedelse- eller stämplingsbrott omfattas av regleringen (23 kap. 1 och 2 §§ brottsbalken).

När uppgifter lämnas ut enligt lagen om elektronisk kommunikation är det inte domstol som fattar beslut om utlämnande, utan begäran till leverantören kommer direkt från polis- eller åklagarmyndighet eller annan myndighet som ska ingripa mot brottet, t.ex. Tullverket. Det finns inte någon formell begränsning i tiden för den information som får begäras ut, eller med andra ord hur ”gammal” informationen får vara. En praktisk begränsning i möjligheten för de brottsbekämpande myndigheterna att få uppgifter från leverantörer finns dock i den nuvarande skyldigheten för leverantörerna att utplåna eller avidentifiera uppgifter.

Bestämmelserna i lagen om elektronisk kommunikation är inte begränsade till att gälla uppgifter som har anknytning till en person (jfr exempelvis 27 kap. 20 § första stycket RB). Det är med andra ord inte nödvändigt att, som vid hemlig teleavlyssning och hemlig teleövervakning, ha en skäligen misstänkt person för att undantaget från tystnadsplikten ska bli tillämpligt och uppgifterna lämnas ut. Inte heller behöver den teleadress som begäran avser ha en särskild anknytning till en eventuell misstänkt person. Det är tillräckligt med en misstanke om att ett brott med viss svårhetsgrad har begåtts.

Det finns uppgifter hos leverantörerna som inte omfattas av tystnadsplikten enligt 6 kap. 20 § LEK. Det gäller t.ex. uppgift om den s.k. PUK-koden (Personal Unblocking Key, Personlig UpplåsningsKod) och lokaliseringsuppgifter som inte samtidigt är trafikuppgifter (6 kap. 9 § LEK). I sådana fall har leverantören inte någon skyldighet att lämna ut uppgifterna till en brottsbekämpande myndighet enligt bestämmelsen i 6 kap. 22 § LEK. Myndigheten kan i dessa fall få tillgång till uppgifterna genom husrannsakan, beslag och editionsföreläggande. Om myndigheten i stället begär ut uppgifterna får leverantören pröva frågan om utlämnande med tillämpning av andra bestämmelser, t.ex. personuppgiftslagen.

2.3.3 Sekretesslagen

I sekretesslagen finns bestämmelser om sekretess som gäller för myndigheter som driver televerksamhet. Enligt 1 kap. 9 § sekretesslagen ska aktiebolag, handelsbolag, ekonomiska föreningar och stiftelser där kommuner eller landsting utövar ett rättsligt bestämmande inflytande jämställas med myndighet vid tillämpningen av sekretesslagen. Enligt 6 kap. 2 § LEK ska sekretesslagen tillämpas i det allmännas verksamhet i stället för 6 kap. 20-23 §§ LEK, dvs. i stället för bestämmelserna om tystnadsplikten och undantagen från denna.

I 9 kap. 8 § andra stycket sekretesslagen föreskrivs att sekretess gäller för en uppgift som angår ett särskilt telefonsamtal eller annat telemeddelande hos en myndighet som driver televerksamhet. En sådan uppgift som angår misstanke om brott får emellertid, som huvudregel, lämnas till en myndighet som har att ingripa mot brottet, om det är föreskrivet fängelse i minst ett år för brottet (14 kap. 2 § fjärde och femte styckena sekretesslagen). Såväl innehållet i ett telemeddelande som uppgifter om ett telemeddelande (både realtidsuppgifter och historiska uppgifter), t.ex. när och mellan vilka abonnemang som meddelandet har utväxlats, torde kunna lämnas ut (jfr SOU 1992:70 s. 328 och prop. 1992/93:200 s. 311). Det är den utlämnande myndigheten som prövar om det enligt sekretesslagen finns förutsättningar för att lämna ut en uppgift till den brottsbekämpande myndigheten. Liksom för utlämnande enligt lagen om elektronisk kommunikation krävs inget domstolsbeslut. Bestämmelserna i sekretesslagen är inte heller begränsade till att gälla situationer när det finns en skäligen misstänkt person eller till teleadresser med särskild anknytning till denne.

Sedan Televerket som myndighet upphörde att bedriva verksamhet har möjligheten att med stöd av sekretesslagen hämta in uppgifter om telemeddelanden kommit att i princip sakna praktisk betydelse för de brottsbekämpande myndigheternas verksamhet. I stället fick telelagen och senare lagen om elektronisk kommunikation den betydelse som sekretesslagen tidigare hade.

2.3.4 1952 års tvångsmedelslag m.fl.

Som nämndes tidigare finns bestämmelser om hemlig teleavlyssning och hemlig teleövervakning i bl.a. 1952 års tvångsmedelslag. Lagen gäller för vissa allmänfarliga brott och brott mot rikets inre och yttre säkerhet (13, 18 och 19 kap. brottsbalken). Ett sådant brott behöver enligt lagen inte vara så allvarligt att det omfattas av bestämmelserna i 27 kap. 18 och 19 §§ RB för att tillstånd ska kunna ges till hemlig teleavlyssning och hemlig teleövervakning. Dessutom får åklagare i brådskande fall ge tillfälliga tillstånd till tvångsmedlen. Även enligt 1988 års lag om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. får åklagare under vissa förutsättningar fatta sådana beslut. Enligt lagen om särskild utlänningskontroll får domstol ge tillstånd till hemlig teleavlyssning och hemlig teleövervakning även i visst förebyggande syfte.

När vi gör våra överväganden i betänkandet behandlar vi uttryckligen bestämmelserna i rättegångsbalken och lagen om elektronisk kommunikation. Övervägandena har dock gjorts även mot bakgrund av regleringarna i sekretesslagen, 1952 års tvångsmedelslag, 1988 års lag om förfarandet hos kommunerna, förvaltningsmyndigheterna och domstolarna under krig eller krigsfara m.m. och lagen om särskild utlänningskontroll.

Vi har också tagit del av och beaktat innehållet i departementspromemorian Brott och brottsutredning i IT-miljö, Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll (Ds 2005:6) och i propositionen Åtgärder för att förhindra vissa särskilt allvarliga brott (prop. 2005/06:177), med förslag om att bl.a. hemlig teleövervakning under vissa förutsättningar ska kunna användas för att förhindra brott.

2.3.5 Lagen om internationell rättslig hjälp i brottmål

Bestämmelser om internationell rättslig hjälp i brottmål finns i lagen (2000:562) om internationell rättslig hjälp i brottmål (Lirb), i förordningen (2000:704) med samma namn och i tillkännagivande (2005:1207) av överenskommelser som avses i lagen om internationell rättslig hjälp i brottmål. Innehållet i flera internationella överenskommelser som Sverige har tillträtt eller annars är bundet av har arbetats in i den svenska lagen eller förordningen.

Lagen är tillämplig på det internationella rättsliga samarbetet, dvs. på det samarbete som tar sikte på rättsliga förfaranden som gäller utredning om och lagföring för brott. Lagen tillämpas av svenska åklagare och domstolar men är inte tillämplig i det internationella polissamarbetet. I fråga om utlämning, överförande av lagföring och delgivning finns särskilda bestämmelser.

Enligt lagen kan rättslig hjälp bl.a. omfatta hemlig teleavlyssning och hemlig teleövervakning, tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning samt tillstånd till gränsöverskridande hemlig teleavlyssning och hemlig teleövervakning (1 kap. 2 § första stycket 6-8 Lirb).

En ansökan om rättslig hjälp i form av *hemlig teleavlyssning eller hemlig teleövervakning i Sverige* handläggs av åklagare. Åklagaren ska genast pröva om det finns förutsättningar för den begärda åtgärden och ansöka om rättens tillstånd. I förhållande till EU-stater samt Island och Norge får hemlig teleavlyssning eller hemlig teleövervakning verkställas genom omedelbar överföring av telemeddelanden eller uppgifter om telemeddelanden till den ansökande staten om det kan ske under betryggande former. Tillstånd till hemlig teleavlyssning eller hemlig teleövervakning lämnas under samma förutsättningar som gäller för motsvarande åtgärder under en svensk förundersökning enligt rättegångsbalken och enligt de särskilda bestämmelserna i lagen om internationell rättslig hjälp i brottmål (2 kap. 1 § första stycket och 4 kap. 25 och 25 a §§ Lirb). Vid prövningen om åtgärden kan vidtas i Sverige ska gärningen bedömas enligt svensk rätt. Kopplingen i 2 kap. 1 § Lirb till bestämmelserna i rättegångsbalken innebär automatiskt ett krav på dubbel straffbarhet och att de strafftrösklar som gäller enligt rättegångsbalken (27 kap. 18 och 19 §§ RB) även tillämpas gentemot den andra staten. Kravet på dubbel straffbarhet framgår dessutom uttryckligen i 2 kap. 2 § Lirb.

En ansökan om rättslig hjälp i form av *tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning i Sverige* prövas av åkla-

gare. Sådan rättslig hjälp kan lämnas i förhållande till EU-länder samt Island och Norge och bygger på att telemeddelanden kan överföras omedelbart till den ansökande staten samt att meddelanden ska avlyssnas och tas upp där och inte i Sverige. Svenska myndigheters insatser begränsas till att tekniskt hjälpa till med att överföra telemeddelanden till den ansökande statens myndigheter, dvs. att möjliggöra verkställighet av det utländska beslutet. För att en ansökan ska beviljas krävs att beslut om hemlig teleavlyssning eller hemlig teleövervakning har meddelats i den ansökande staten och att överföringen kan ske under betryggande former. Rättslig hjälp i form av tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning i Sverige lämnas i enlighet med bestämmelserna i 2 kap. 1 § andra stycket samt 4 kap. 25 b och 25 c §§ Lirb. Vid denna form av rättslig hjälp krävs inte dubbel straffbarhet.

Tillstånd till *gränsöverskridande hemlig teleavlyssning och hemlig teleövervakning, utan svenskt bistånd, av någon som befinner sig i Sverige*, lämnas av domstol. En utländsk ansökan om sådan rättslig hjälp handläggs av åklagare enligt bestämmelserna i 4 kap. 26-26 b §§ Lirb. Åklagaren ska genast pröva om förutsättningar för åtgärden finns och i så fall ansöka om rättens tillstånd. Av 2 kap. 2 § Lirb framgår att det krävs dubbel straffbarhet.

Den åklagare eller domare som handlägger ansökan om rättslig hjälp prövar också om de förutsättningar som gäller enligt lagen, t.ex. angående ansökans innehåll, krav på dubbel straffbarhet eller viss strafftröskel är uppfyllda. Om så inte är fallet ska ansökan avslås efter att den ansökande utländska myndigheten fått tillfälle att komma in med komplettering (2 kap. 9 § och 15 § andra stycket Lirb).

Avslag på grund av hänsyn till Sveriges suveränitet, rikets säkerhet och svenska allmänna intressen och liknande prövas av regeringen (2 kap. 14 § och 15 § första stycket Lirb). Om en åklagare finner att en ansökan om rättslig hjälp bör avslås på någon sådan grund, ska ansökan, efter att samråd skett med riksåklagaren, överlämnas till Justitiedepartementet.

Om en begäran om rättslig hjälp bifalls, kan särskilda villkor ställas upp som är påkallade med hänsyn till enskilds rätt eller som är nödvändiga från allmän synpunkt, t.ex. att trafikuppgifterna inte får föras vidare till annan stat eller att de ska förstöras efter att de har använts i den utredning de har begärts in för. Villkor får dock inte ställas upp om de strider mot en internationell överenskommelse som är bindande för Sverige (5 kap. 2 § Lirb).

Om trafikuppgifter som den andra staten efterfrågar skulle finnas hos en svensk myndighet, t.ex. hos polisen efter en verkställd hemlig teleövervakning, gäller även sekretesslagens bestämmelser. Enligt 1 kap. 3 § tredje stycket den lagen får sekretessbelagd uppgift inte röjas för utländsk myndighet annat än om utlämnande sker i enlighet med särskild föreskrift i lag eller förordning eller om uppgiften i motsvarande fall skulle få lämnas ut till svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten.

Svenska åklagares och domstolars egna möjligheter att utomlands begära rättslig hjälp styrs i huvudsak av lagstiftningen i den andra staten och av de internationella åtaganden som den staten har gjort i förhållande till Sverige. Förutom att det finns vissa allmänna regler om vad en sådan ansökan ska innehålla och vart den ska skickas, finns vissa särskilda bestämmelser i lagen om internationell rättslig hjälp i brottmål som tar sikte på svenska åklagares handläggning av ärenden om hemlig teleavlyssning och hemlig teleövervakning, tekniskt bistånd med hemlig teleavlyssning och hemlig teleövervakning, samt tillstånd till gränsöverskridande hemlig teleavlyssning och hemlig teleövervakning utomlands.

I enlighet med bestämmelserna i lagen om internationell rättslig hjälp i brottmål får åklagare ansöka hos en utländsk myndighet om rättslig hjälp eller tekniskt bistånd med hemlig teleavlyssning eller hemlig teleövervakning av någon som befinner sig i en annan stat eller i Sverige. Av ansökan ska framgå under vilken tid åtgärden önskas samt sådana uppgifter som behövs för att åtgärden ska kunna genomföras. Den andra staten kan kräva att ansökan ska prövas av domstol i Sverige. Det ankommer då på åklagaren att begära att rätten ska pröva frågan om att tillåta den hemliga teleavlyssningen eller hemliga teleövervakningen (4 kap. 26 § Lirb).

Om svensk domstol beslutat om hemlig teleavlyssning eller hemlig teleövervakning och den person som åtgärden avser befinner sig i en annan EU-stat eller på Island eller i Norge, och Sverige har möjlighet att vidta åtgärden utan bistånd av den andra staten, ska åklagaren ansöka om tillstånd till åtgärden från den andra staten (4 kap. 26 c § Lirb). Ett sådant tillstånd bör om möjligt sökas innan åtgärden har påbörjats eller annars omedelbart sedan det framkommit att den person som åtgärden avser befinner sig i den andra staten. Ansökan om tillstånd till åtgärden görs av åklagare. Av ansökan ska det framgå under vilken tid åtgärden beräknas pågå. An-

sökan ska också innehålla uppgift om det svenska domstolsbeslutet om tvångsmedlet.

2.4 Artikel 2 i rambeslutet 2002/584/RIF om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna

Syftet med direktivet om lagring av trafikuppgifter är att trafikuppgifter ska finnas lagrade och tillgängliga för att kunna lämnas ut och användas för utredning, avslöjande och åtal av allvarlig brottslighet. Enligt direktivet får varje stat avgöra vad som är allvarlig brottslighet. Vi ska enligt våra direktiv överväga om de bestämmelser om lagring av trafikuppgifter som vi föreslår ger anledning att ändra i de bestämmelser i rättegångsbalken och lagen om elektronisk kommunikation som reglerar förutsättningarna för att lämna ut uppgifter till brottbekämpande myndigheter. Enligt ett uttalande från rådet ska medlemsstaterna ta ”vederbörlig hänsyn” till de brott som förtecknas i artikel 2 i rambeslutet om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (2002/584/RIF). Artikeln har följande lydelse.

Artikel 2
Tillämpningsområde för en europeisk arresteringsorder

1. En europeisk arresteringsorder får utfärdas för gärningar som enligt den utfärdande medlemsstatens lagstiftning kan leda till fängelse eller frihetsberövande åtgärd i tolv månader eller mer. Detsamma gäller om ett straff eller annan frihetsberövande åtgärd i minst fyra månader har dömts ut.

2. Följande brott ska medföra överlämnande på grundval av en europeisk arresteringsorder enligt villkoren i detta rambeslut och utan kontroll av om det föreligger dubbel straffbarhet för gärningen, förutsatt att brotten, som de definieras i den utfärdande medlemsstatens lagstiftning, kan leda till fängelse eller annan frihetsberövande åtgärd i minst tre år i den utfärdande medlemsstaten:

– Deltagande i en kriminell organisation.
– Terrorism.

– Människohandel.
– Sexuellt utnyttjande av barn samt barnpornografi.
– Olaglig handel med narkotika och psykotropa ämnen.
– Olaglig handel med vapen, ammunition och sprängämnen.
– Korruption.
– Bedrägeri, inbegripet bedrägeri som riktar sig mot Europeiska gemenskapernas ekonomiska intressen enligt konventionen av den 26 juli 1995 om skydd av Europeiska gemenskapernas finansiella intressen.
– Penningtvätt.
– Penningförfalskning, inklusive förfalskning av euron.
– IT-brottslighet.
– Miljöbrott, inbegripet olaglig handel med hotade djurarter och hotade växtarter och växtsorter.
– Hjälp till olovlig inresa och olovlig vistelse.
– Mord, grov misshandel.
– Olaglig handel med mänskliga organ och vävnader.
– Människorov, olaga frihetsberövande och tagande av gisslan.
– Rasism och främlingsfientlighet.
– Organiserad stöld och väpnat rån.
– Olaglig handel med kulturföremål, inbegripet antikviteter och konstverk.
– Svindleri.
– Beskyddarverksamhet och utpressning.
– Förfalskning och piratkopiering.
– Förfalskning av administrativa dokument och handel med sådana förfalskningar.
– Förfalskning av betalningsmedel.
– Olaglig handel med hormonsubstanser och andra tillväxtsubstanser.
– Olaglig handel med nukleära och radioaktiva ämnen.
– Handel med stulna fordon.
– Våldtäkt.
– Mordbrand.
– Brott som omfattas av den internationella brottmålsdomstolens behörighet.
– Kapning av flygplan eller fartyg.
– Sabotage.

3. Rådet kan, efter att ha hört Europaparlamentet i enlighet med artikel 39.1 i Fördraget om Europeiska unionen, när

som helst enhälligt besluta att lägga till andra typer av brott i förteckningen i punkt 2 i den här artikeln. Mot bakgrund av kommissionens rapport enligt artikel 34.3 ska rådet bedöma om förteckningen bör utvidgas eller ändras.

4. När det gäller andra brott än de som omfattas av punkt 2 kan överlämnandet förenas med villkoret att de gärningar för vilka den europeiska arresteringsordern har utfärdats ska utgöra ett brott enligt den verkställande medlemsstatens lagstiftning, oberoende av brottsrekvisit eller brottets rättsliga rubricering.

I lagen (2003:1156) om överlämnande från Sverige enligt en europeisk arresteringsorder regleras förutsättningarna för utlämnande enligt arresteringsorder. Listan på brottslighet i artikel 2:2 i rambeslutet finns som bilaga till den lagen. I 2 kap. 2 § finns bestämmelser om strafftrösklar och krav på dubbel straffbarhet. Där framgår i andra stycket att om det i arresteringsordern har angetts att en gärning är sådan som finns i bilagan till lagen, den s.k. listan, och det för gärningen enligt den utfärdande medlemsstatens lagstiftning är föreskrivet en frihetsberövande påföljd i tre år eller mer, ska överlämnande beviljas även om gärningen inte motsvarar brott enligt svensk lag.

Våra överväganden i frågan om bestämmelserna om tillgång till trafikuppgifter för de brottsbekämpande myndigheterna behöver förändras finns i avsnitt 11.

2.5 Bestämmelserna om anpassningsskyldighet

2.5.1 Telelagen

Bestämmelserna om anpassningsskyldighet reglerar leverantörernas skyldighet att bedriva en verksamhet så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs.

Anpassningsskyldighet för leverantörer infördes i telelagen genom propositionen 1995/96:180 Leverantörernas skyldigheter vid hemlig teleavlyssning och hemlig teleövervakning. Regeringen uttalade då bl.a. (prop. 1995/96:180 s. 17 ff.) att hemlig teleavlyssning och hemlig teleövervakning är oumbärliga verktyg i den brottsutredande verksamheten bl.a. i kampen mot narkotikan, den organi-

serade brottsligheten och allvarligare ekonomisk brottslighet samt vid brott mot rikets inre och yttre säkerhet, och att det är ytterst angeläget att möjligheterna till verkställighet av tvångsmedlen på teleområdet upprätthålls. Regeringen anförde i detta sammanhang att den faktiska anpassningen av systemen inte kan göras av de brottsutredande myndigheterna själva. Regeringen menade att telesystemet vid varje givet tillfälle bör innehålla de egenskaper som behövs för att ett beslut om hemlig teleavlyssning eller hemlig teleövervakning genast ska kunna verkställas. Den närmare innebörden av leverantörernas skyldighet beskrevs som i praktiken ett krav på att leverantörerna ska använda sig av tekniska hjälpmedel som har vissa egenskaper och att de ska vidta de personella och organisatoriska dispositioner som krävs för att hantera hjälpmedlen.

Av 7 och 17 §§ telelagen följde att den som hade beviljats tillstånd att inom ett allmänt tillgängligt telenät tillhandahålla telefonitjänst till fast nätanslutningspunkt, mobil teletjänst eller nätkapacitet, skulle bedriva verksamheten på sådant sätt att hemlig teleavlyssning och hemlig teleövervakning kunde verkställas och så att verkställandet inte röjdes. Innehållet i och uppgifter om de avlyssnade eller övervakade telemeddelandena skulle göras tillgängliga så att informationen enkelt kunde tas om hand. Tillstånd erfordrades om verksamheten hade en omfattning som med avseende på utbredningsområde, antalet användare eller annat jämförbart förhållande var betydande.

Det som nu har sagts innebär att skyldigheten enligt 17 § telelagen att anpassa verksamheten enbart gällde i förhållande till vissa leverantörer, nämligen de som var skyldiga att ha tillstånd enligt telelagen.

I 15 § andra och tredje styckena telelagen föreskrevs att ett tillstånd enligt 7 § den lagen (tidigare 5 §) skulle förenas med villkor som gällde sättet att fullgöra skyldigheten och att regeringen eller tillsynsmyndigheten meddelade närmare föreskrifter om det sätt på vilket tillståndsvillkoren skulle fullgöras.

2.5.2 Lagen om elektronisk kommunikation

Lagen om elektronisk kommunikation ersatte telelagen från och med den 25 juli 2003. Den ställer upp liknande krav på anpassning som telelagen tidigare gjorde. Bestämmelsen finns i 6 kap. 19 § LEK och har följande lydelse.

En verksamhet ska bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs, om verksamheten avser tillhandahållande av

1. ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen, eller

2. tjänster inom ett allmänt kommunikationsnät vilka består av

a) en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet, eller

b) en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

Innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand.

Med telemeddelande avses ljud, text, bild, data eller information i övrigt som förmedlas med hjälp av radio eller genom ljus eller elektromagnetiska svängningar som utnyttjar särskilt anordnad ledare.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om frågor som avses i första och andra styckena samt får i enskilda fall medge undantag från kravet i första stycket.

Telelagens bestämmelser i nu aktuellt avseende byggde på en *tillståndsplikt*. Lagen om elektronisk kommunikation utgår i stället från en *anmälningsplikt*. För att, som det anges i den citerade bestämmelsen, tillhandahålla ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst fordras i allmänhet endast en anmälan (2 kap. 1 § LEK). Detta har fått till följd att de tillståndsvillkor om anpassningsskyldighet som var kopplade till de gamla tillstånden upphörde att gälla i samband med ikraftträdandet av lagen om elektronisk kommunikation (se SOU 2005:38 s. 269). Den slutsatsen kan dras eftersom det saknas övergångsbestämmelser om fortsatt giltighet av de tillståndsvillkoren i lagen (2003:390) om införande av lagen om elektronisk kommunikation. Detta torde innebära att anpassningsskyldigheten gäller, så att säga,

fullt ut, dvs. att leverantörer som faller under bestämmelsen i 6 kap. 19 § LEK har en skyldighet att se till att aktuella verksamheter bedrivs så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs, allt enligt vad som föreskrivs i 6 kap. 19 § första stycket LEK.

Den enskilde leverantören har dock, enligt 6 kap. 19 § fjärde stycket LEK, en möjlighet att begära undantag från kravet på hur verksamheten ska bedrivas i det nämnda avseendet. Undantagsbestämmelsen, som alltså medger att beslut fattas om en anpassningsskyldighet efter omständigheterna i det enskilda fallet, kom till mot bakgrund av att den anpassningsskyldighet som anges i lagen om elektronisk kommunikation inte är begränsad till verksamheter av viss storlek. Skulle skyldigheten bli allt för betungande för en mindre leverantör, kan undantag medges efter en prövning i det enskilda fallet (prop. 2002/03:110 s. 270).

Enligt 6 kap. 19 § fjärde stycket LEK meddelar regeringen eller den myndighet som regeringen bestämmer föreskrifter rörande anpassningsskyldigheten. I 36 § förordningen om elektronisk kommunikation har regeringen bestämt att PTS, efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen, dels får utfärda verkställighetsföreskrifter, dels får medge undantag i enskilda fall från kravet på hur verksamheten ska bedrivas enligt 6 kap. 19 § första stycket LEK. Verkställighetsföreskrifterna i sig kan inte innehålla generella undantag från anpassningsskyldigheten.

2.6 BRU:s uppdrag och förslag

Genom tilläggsdirektiv (dir. 2003:145) fick BRU i uppdrag att göra en översyn av de regler som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation. Det skedde bl.a. mot bakgrund av att flera för de brottsbekämpande myndigheterna viktiga frågor hade lämnats åt sidan när lagen om elektronisk kommunikation infördes. BRU skulle bl.a. utreda om och i så fall under vilka förutsättningar som trafikuppgifter skulle bevaras hos leverantörerna.

BRU föreslog i betänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38) förändringar i rättegångsbalken och lagen om elektronisk kommunikation.

En del av förslagen rörde rättegångsbalkens terminologi där BRU föreslog bl.a. att begreppen teleavlyssning, teleövervakning, telemeddelande, telenät och teleadress ska förändras för att bättre

anpassas till den tekniska utvecklingen och till lagen om elektronisk kommunikation. BRU föreslog vidare att det domstolsförfarande som tillämpas vid hemlig teleövervakning ska tillämpas även när ”annan uppgift som angår ett särskilt elektroniskt meddelande” lämnas ut enligt lagen om elektronisk kommunikation. En helt nödvändig följd av ett sådant förslag skulle enligt BRU vara att hemlig teleövervakning blir möjlig att använda även i fall där det saknas en skäligen misstänkt person. Dock skulle brottsligheten då vara så allvarlig att den kan ligga till grund för hemlig teleavlyssning. För att undvika att dubbla beslut om tvångsmedel behöver fattas menade BRU också att ett tillstånd till hemlig teleavlyssning ska ge rätt till de uppgifter som erhålls genom beslut om hemlig teleövervakning. När det gäller anpassningsskyldigheten föreslog BRU att den skulle regleras så teknikneutralt som möjligt och därför vara generell med möjlighet för Rikspolisstyrelsen att i enskilda fall medge undantag från skyldigheten.

BRU:s förslag bereds för närvarande inom Justitiedepartementet.

Sedan regeringen beslutat om tilläggsdirektiven till BRU i november 2003 drabbades Europa av det största terroristattentatet sedan andra världskriget. Attentaten i Madrid den 11 mars 2004 tog omkring 200 personers liv och skadade över 1 500. Den händelsen initierade det arbete inom EU som resulterade i att rådet för rättsliga och inrikes frågor (RIF) den 25 mars 2004 fick i uppdrag av Europeiska rådet att snarast anta gemensamma åtgärder om lagring av trafikuppgifter. Ett antal länder, däribland Sverige, utarbetade förslag som presenterades under sommaren 2004 och som därefter förhandlades. Europaparlamentet och rådet antog den 15 mars 2006 direktivet om lagring av trafikuppgifter.

Redan innan direktivet om lagring av trafikuppgifter antogs hade ett flertal länder i Europa regler om lagring av trafikuppgifter för brottsbekämpande syften. BRU angav (SOU 2005:38 s. 327 f.) att tiden för bevarandet var satt till minst ett år i Belgien, maximalt ett år i Danmark och Frankrike, minst tre år i Irland, minst fyra år i Italien, tre månader i Nederländerna, maximalt ett år i Polen och Spanien samt maximalt sex månader i Schweiz. I Storbritannien fanns ett frivilligt åtagande hos leverantörerna att spara trafikuppgifter i ett år.

Det internationella arbete som hade inletts under den tid BRU arbetade med frågan om lagring av trafikuppgifter fick BRU att dra slutsatsen att det inte var meningsfullt att lämna något förslag i den frågan. BRU hade dock kommit så långt i sitt arbete att man redo-

visade vissa bedömningar, bl.a. om behovet av trafikuppgifter i brottsbekämpningen, om lagringstidens längd och om de problem som uppstår i det brottsbekämpande arbetet med frånvaron av en lagringsskyldighet. Vi återkommer till BRU:s bedömningar i de frågorna i avsnitt 6.5.2 och 7.3.1.

3 Direktivet om lagring av trafikuppgifter

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

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 95,

med beaktande av kommissionens förslag,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[1],

i enlighet med förfarandet i artikel 251 i fördraget[2], och

av följande skäl:

---

[1] Yttrande avgivet den 19 januari 2006 (ännu ej offentliggjort i EUT).

[2] Europaparlamentets yttrande av den 14 december 2005 (ännu ej offentliggjort i EUT) och rådets beslut av den 21 februari 2006.

(1) Enligt 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[3] skall medlemsstaterna skydda fysiska personers fri- och rättigheter i samband med behandling av personuppgifter, särskilt deras rätt till privatliv, för att garantera det fria flödet av personuppgifter inom gemenskapen.

(2) I Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)[4] översattes de principer som fastställts i direktiv 95/46/EG till specifika regler för elektronisk kommunikation.

(3) I artiklarna 5, 6 och 9 i direktiv 2002/58/EG fastställs de bestämmelser som gäller för den behandling som nät- och tjänsteleverantörer gör av trafik- och lokaliseringsuppgifter som genereras vid användning av elektroniska kommunikationstjänster. Sådana uppgifter måste raderas eller göras anonyma när de inte längre behövs för överföring, med undantag av uppgifter som behövs för fakturering eller betalning av samtrafikuppgifter. Förutsatt att medgivande ges kan vissa uppgifter också behandlas för marknadsföring eller för att tillhandahålla mervärdestjänster.

(4) I artikel 15.1 i direktiv 2002/58/EG fastställs de villkor på vilka medlemsstaterna får begränsa omfattningen av de rättigheter och skyldigheter som anges i artiklarna 5 och 6 samt artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i det direktivet. Varje sådan begränsning måste anses vara nödvändig, lämplig och proportionell i ett demokratiskt samhälle för den allmänna ordningens skull, dvs. för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet eller för att förebygga, utreda, avslöja och åtala brott eller för obehörig användning av ett elektroniskt kommunikationssystem.

(5) Flera medlemsstater har antagit lagstiftning om leverantörers skyldighet att lagra trafikuppgifter för att kunna förebygga, utreda,

[3] EGT L 281, 23.11.1995, s. 31. Direktivet ändrat genom förordning (EG) nr 1882/2003 (EUT L 284, 31.10.2003, s. 1).
[4] EGT L 201, 31.7.2002, s. 37.

avslöja och åtala brott. Dessa nationella bestämmelser är i stor utsträckning olika.

(6) Skillnader i rättsliga och tekniska bestämmelser i medlemsstaterna avseende lagring av trafikuppgifter i syfte att förebygga, utreda, avslöja och åtala brott utgör hinder för den inre marknaden för elektronisk kommunikation, eftersom tjänsteleverantörer ställs inför olika krav avseende typen av trafik- och lokaliseringsuppgifter som skall lagras liksom villkoren för lagring och lagringstiderna.

(7) I slutsatserna från rådet (rättsliga och inrikes frågor) av den 19 december 2002 understryks det att eftersom omfattningen av elektronisk kommunikation ökat avsevärt är uppgifter om användningen av sådan kommunikation särskilt viktiga och därför ett värdefullt verktyg när det gäller att förebygga, utreda, avslöja och åtala brott, särskilt organiserad brottslighet.

(8) I Europeiska rådets uttalande om kampen mot terrorism av den 25 mars 2004 ges rådet i uppdrag att undersöka åtgärder om fastställande av regler för lagring av trafikuppgifter från kommunikation hos tjänsteoperatörer.

(9) Enligt artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna har alla personer rätt till skydd för sitt privatliv och sin korrespondens. En offentlig myndighets inblandning i utövandet av denna rättighet får bara ske i enlighet med vad som är stadgat i lag och om det är nödvändigt i ett demokratiskt samhälle, bland annat med hänsyn till landets nationella säkerhet eller den allmänna säkerheten, för att förebygga oordning eller brott eller för att skydda andra personers fri- och rättigheter. Eftersom lagring av uppgifter har visat sig vara ett så nödvändigt och effektivt redskap för de brottsbekämpande myndigheternas utredningar i många medlemsstater och framför allt i allvarliga fall som organiserad brottslighet och terrorism är det därför nödvändigt att se till att brottsbekämpande myndigheter får tillgång till lagrade uppgifter under en viss tid i enlighet med de villkor som föreskrivs i detta direktiv. Antagandet av ett instrument om lagring av uppgifter i enlighet med kraven i artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna är därför en nödvändig åtgärd.

(10) Den 13 juli 2005 upprepade rådet i sitt uttalande om fördömande av bombattentaten i London behovet av att så snart som möjligt anta gemensamma åtgärder om lagring av telekommunikationsuppgifter.

(11) Med tanke på hur viktiga trafik- och lokaliseringsuppgifter är för att kunna utreda, avslöja och åtala brott, något som framkommit både genom forskning och genom medlemsstaternas praktiska erfarenheter, är det viktigt att på europeisk nivå säkerställa att uppgifter som vid tillhandahållande av kommunikationstjänster genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller av allmänna kommunikationsnät lagras under en viss tid i enlighet med de villkor som föreskrivs i detta direktiv.

(12) Artikel 15.1 i direktiv 2002/58/EG fortsätter att gälla för sådana uppgifter, inklusive uppgifter relaterade till misslyckade uppringningsförsök, för vilka det inte finns särskilda krav på lagring enligt det här direktivet och som därför faller utanför dess tillämpningsområde, samt för lagring i andra, däribland rättsliga, syften än de som omfattas av det här direktivet.

(13) Detta direktiv avser endast uppgifter som genereras eller behandlas som en konsekvens av en kommunikation eller en kommunikationstjänst och avser inte uppgifter som utgör innehållet i den information som förmedlas vid kommunikationen. Lagring bör ske på ett sådant sätt att man undviker att uppgifter lagras mer än en gång. Uppgifter som genererats eller behandlats i samband med tillhandahållande av de aktuella kommunikationstjänsterna avser uppgifter som är tillgängliga. När det särskilt gäller lagring av uppgifter i samband med Internetbaserad e-post och Internettelefoni får tillämpningsområdet begränsas till leverantörernas eller nätverksleverantörernas egna tjänster.

(14) Den teknik som används för elektronisk kommunikation utvecklas snabbt, och de behöriga myndigheternas legitima krav kan därför komma att ändras. För att få råd och uppmuntra utbyte av erfarenheter om bästa metoder i dessa frågor avser kommissionen att inrätta en grupp bestående av medlemsstaternas brottsbekämpande myndigheter, sammanslutningar inom den elektroniska kommunikationsindustrin, företrädare för Europaparlamentet samt dataskyddsmyndigheter, däribland Europeiska datatillsynsmannen.

(15) Direktiv 95/46/EG och direktiv 2002/58/EG är fullt tillämpliga på uppgifter som lagras i enlighet med detta direktiv. I artikel 30.1 c i direktiv 95/46/EG föreskrivs att arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, vilken inrättats genom artikel 29 i det direktivet, skall konsulteras.

(16) De skyldigheter som i enlighet med artikel 6 i direktiv 95/46/EG åligger tjänsteleverantörerna när det gäller åtgärder för att garantera uppgifternas kvalitet och de skyldigheter i enlighet med artiklarna 16 och 17 i det direktivet som åligger dem när det gäller åtgärder för att garantera sekretess och säkerhet vid behandlingen av uppgifter är fullt tillämpbara för uppgifter som lagras i enlighet med detta direktiv.

(17) Det är nödvändigt att medlemsstaterna antar lagstiftande åtgärder som säkerställer att uppgifter som lagras i enlighet med detta direktiv bara är tillgängliga för behöriga nationella myndigheter i enlighet med nationell lagstiftning, samtidigt som berörda personers grundläggande rättigheter respekteras fullt ut.

(18) Medlemsstaterna är, i detta sammanhang, skyldiga att enligt artikel 24 i direktiv 95/46/EG fastställa sanktioner för överträdelse av de bestämmelser som antagits i enlighet med det direktivet. I artikel 15.2 i direktiv 2002/58/EG ställs samma krav när det gäller de nationella bestämmelser som antagits i enlighet med direktiv 2002/58/EG. Enligt rådets rambeslut 2005/222/RIF av den 24 februari 2005 om angrepp mot informationssystem[1] skall uppsåtligt olagligt intrång i informationssystem, inklusive de uppgifter som lagras däri, straffbeläggas.

(19) Den rätt till ersättning som i enlighet med artikel 23 i direktiv 95/46/EG tillkommer varje person som lidit skada till följd av otillåten behandling eller någon annan handling som är oförenlig med de nationella bestämmelser som antagits till följd av det direktivet gäller också enligt det här direktivet vid otillåten behandling av personuppgifter.

(20) Europarådets konvention om IT-brottslighet från 2001 och Europarådets konvention om skydd för enskilda vid automatisk

[1] EUT L 69, 16.3.2005, s. 67.

databehandling av personuppgifter från 1981 omfattar också uppgifter som lagras i enlighet med detta direktiv.

(21) Eftersom målen med detta direktiv, nämligen att harmonisera leverantörernas skyldighet att lagra vissa uppgifter och säkerställa att de är tillgängliga för utredning, avslöjande och åtal av allvarliga brott såsom de definieras av varje medlemsstat i den nationella lagstiftningen inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och de därför på grund av detta direktivs omfattning och verkningar bättre kan uppnås på gemenskapsnivå, får gemenskapen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(22) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i Europeiska unionens stadga om grundläggande rättigheter. Detta direktiv tillsammans med direktiv 2002/58/EG syftar särskilt att säkerställa full respekt för medborgarnas grundläggande rättigheter med avseende på privatlivet och kommunikationer samt skyddet av deras personuppgifter (artiklarna 7 och 8 i stadgan).

(23) Eftersom skyldigheterna för leverantörerna av elektroniska kommunikationstjänster bör vara proportionerliga kräver direktivet att leverantörerna lagrar endast sådana uppgifter som genereras eller behandlas i samband med att de tillhandahåller sina kommunikationstjänster. I de fall sådana uppgifter inte genereras eller behandlas av leverantörerna finns det inte något krav på att de skall lagra dem. Detta direktiv syftar inte till att harmonisera tekniken för lagring av uppgifter, något som är en fråga som måste lösas på nationell nivå.

(24) I enlighet med punkt 34 i det interinstitutionella avtalet om bättre lagstiftning[1] uppmuntras medlemsstaterna att för egen del och i gemenskapens intresse upprätta egna tabeller som så långt det är möjligt visar överensstämmelsen mellan detta direktiv och införlivandeåtgärderna samt att offentliggöra dessa tabeller.

[1] EUT C 321, 31.12.2003, s. 1.

(25) Detta direktiv påverkar inte medlemsstaternas befogenhet att anta lagstiftningsåtgärder om rätten till tillgång till och användning av uppgifter för de nationella myndigheter de utsett. Frågor om tillgång till de uppgifter som nationella myndigheter lagrar i enlighet med detta direktiv för de verksamheter som avses i artikel 3.2 första ledet i direktiv 95/46/EG faller utanför tillämpningsområdet för gemenskapens lagstiftning. De kan emellertid omfattas av nationell lagstiftning eller nationella åtgärder i enlighet med avdelning VI i fördraget om Europeiska unionen. Sådana lagar eller åtgärder måste till fullo respektera de grundläggande rättigheter som följer av medlemsstaternas gemensamma författningsmässiga traditioner och som är garanterade i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Enligt den tolkning Europeiska domstolen för de mänskliga rättigheterna gjort av artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna måste offentliga myndigheters intrång i rätten till privatliv stå i förhållande till vad som är nödvändigt och proportionerligt och därför tjäna närmare angivna, tydliga och legitima syften samt utövas på ett sätt som är rimligt och relevant och som inte är överdrivet i förhållande till syftet med intrånget.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1
Syfte och tillämpningsområde

1. Syftet med detta direktiv är att harmonisera medlemsstaternas bestämmelser om de skyldigheter som leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät har att lagra vissa uppgifter som de genererat eller behandlat för att säkerställa att uppgifterna är tillgängliga för utredning, avslöjande och åtal av allvarliga brott såsom de definieras av varje medlemsstat i den nationella lagstiftningen.

2. Detta direktiv skall gälla trafik- och lokaliseringsuppgifter om såväl fysiska som juridiska personer och enheter, samt de uppgifter som är nödvändiga för att kunna identifiera abonnenten eller den registrerade användaren. Det skall inte vara tillämpligt på innehållet i elektronisk kommunikation, inklusive sådan information som användaren sökt med hjälp av ett elektroniskt kommunikationsnät.

Artikel 2
Definitioner

1. I detta direktiv skall definitionerna i direktiv 95/46/EG, Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv)[2] samt direktiv 2002/58/EG gälla.

2. I detta direktiv avses med

a) *uppgifter*: trafik- och lokaliseringsuppgifter samt de uppgifter som behövs för att identifiera en abonnent eller användare,

b) *användare*: en fysisk eller juridisk person eller enhet som använder en allmänt tillgänglig elektronisk kommunikationstjänst för privat eller affärsmässigt bruk, utan att nödvändigtvis ha abonnerat på denna tjänst,

c) *telefonitjänst*: uppringning (inbegripet rösttelefoni, röstmeddelanden, konferenssamtal och datatelefoni), extratjänster inbegripet omstyrning och överflyttning av samtal) och meddelandeförmedling och multimedietjänster (inbegripet SMS, EMS och multimedietjänster),

d) *användar-ID*: ett unikt ID som tilldelas personer när de abonnerar på eller registrerar sig på en Internetåtkomsttjänst eller en Internetkommunikationstjänst,

e) *lokaliseringsbeteckning (cell-ID)*: identiteten hos den cell från vilken ett mobiltelefonsamtal påbörjades eller avslutades,

f) *misslyckade uppringningsförsök*: en kommunikation då ett telefonsamtal kopplats men inget svar erhållits eller när det skett ett ingrepp av driften i kommunikationsnätet.

[2] EGT L 108, 24.4.2002, s. 33.

Artikel 3
Skyldighet att lagra uppgifter

1. Genom avvikelse från artiklarna 5, 6 och 9 i direktiv 2002/58/EG skall medlemsstaterna anta åtgärder för att säkerställa lagring enligt bestämmelserna i det här direktivet av de uppgifter som specificeras i artikel 5 i detta, i den utsträckning som de genereras eller behandlas av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät inom statens territorium i samband med att leverantörerna levererar de kommunikationstjänster som berörs.

2. Den lagringsskyldighet som anges i punkt 1 skall inbegripa lagring av sådana uppgifter som anges i artikel 5 rörande misslyckade uppringningsförsök där uppgifter genereras eller behandlas, och lagras (uppgifter rörande telefoni) eller loggas (uppgifter rörande Internet) av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät inom den berörda medlemsstatens jurisdiktion i samband med att de levererar de berörda kommunikationstjänsterna. Detta direktiv skall inte innebära krav på lagring av uppgifter rörande samtal som inte kopplats fram.

Artikel 4
Tillgång till uppgifter

Medlemsstaterna skall anta åtgärder för att säkerställa att uppgifter som lagras i enlighet med detta direktiv endast görs tillgängliga för behöriga nationella myndigheter, i närmare angivna fall och i enlighet med nationell lagstiftning. De förfaranden som skall följas och de villkor som skall uppfyllas för att erhålla tillgång till lagrade uppgifter i enlighet med nödvändighets- och proportionalitetskraven skall fastställas av varje enskild medlemsstat i den nationella lagstiftningen och följa tillämpliga bestämmelser i EU-lagstiftningen och folkrätten, särskilt Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, i enlighet med den tolkning som görs av Europeiska domstolen för mänskliga rättigheter.

Artikel 5

Kategorier av uppgifter som skall lagras

1. Medlemsstaterna skall säkerställa att följande kategorier av uppgifter lagras i enlighet med direktivet:

a) Uppgifter som är nödvändiga för att spåra och identifiera en kommunikationskälla:

1. Telefoni i fasta nät och mobil telefoni:

i) Det uppringande telefonnumret.

ii) Abonnentens eller den registrerade användarens namn och adress.

2. Internetåtkomst, Internetbaserad e-post och Internettelefoni:

i) Tilldelade användar-ID.

ii) Användar-ID och telefonnummer vilka tilldelats kommunikationen i det allmänna telenätet.

iii) Namn på och adress till den abonnent eller registrerade användare som IP-adressen (Internet Protocol), användaridentiteten eller telefonnumret tilldelades vid tidpunkten för kommunikationen.

b) Uppgifter som är nödvändiga för att identifiera slutmålet för en kommunikation:

1. Telefoni i fasta nät och mobil telefoni:

i) Det eller de nummer som slagits (det eller de uppringda telefonnumren), och, i fall som berör tilläggstjänster såsom omstyrning och överflyttning av samtal, det eller de nummer till vilket eller vilka som samtalet styrs.

ii) Abonnentens (abonnenternas) eller den eller de registrerade användarnas namn och adress.

2. Internetbaserad e-post och Internettelefoni:

i) Användar-ID eller telefonnummer som tilldelats den eller de avsedda mottagarna av ett Internettelefonsamtal.

ii) Namn på och adress till abonnenten (abonnenterna) eller den eller de registrerade användarna och det användar-ID som tilldelats den avsedda mottagaren av kommunikationen.

c) Uppgifter som är nödvändiga för att identifiera datum, tidpunkt och varaktighet för en kommunikation:

1. Telefoni i fasta nät och mobil telefoni: datum och tid då kommunikationen påbörjades och avslutades.

2. Internetåtkomst, Internetbaserad e-post och Internettelefoni:

i) Datum och tid för på- respektive avloggning i Internetåtkomsttjänsten inom en given tidszon tillsammans med IP-adressen, oavsett om den är dynamisk eller statisk, som en kommunikation tilldelats av Internetåtkomstleverantören till en kommunikation och abonnents eller registrerad användares användar-ID.

ii) Datum och tid för på- respektive avloggning i den Internetbaserade e-posttjänsten eller Internettelefonitjänsten inom en given tidszon.

d) Uppgifter som är nödvändiga för att identifiera typen av kommunikation.

1. Telefoni i fasta nät och mobil telefoni: Den telefonitjänst som används.

2. Internetbaserad e-post och Internettelefoni: Den Internettjänst som används.

e) Uppgifter som är nödvändiga för att identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

1. Telefoni i fasta nät: det uppringande och det uppringda telefonnumret.

2. Mobil telefoni:

i) Det uppringande och det uppringda telefonnumret.

ii) Den uppringande partens IMSI (International Mobile Subscriber Identity).

iii) Den uppringande partens IMEI (International Mobile Equipment Identity).

iv) Den uppringda partens IMSI.

v) Den uppringda partens IMEI.

vi) Vid förbetalda anonyma tjänster, datum och tid för den första aktiveringen av tjänsten och den lokaliseringsbeteckning (cell-ID) från vilken tjänsten aktiverades.

3. Internetåtkomst, Internetbaserad e-post och Internettelefoni:

i) Det uppringande telefonnumret för uppringda förbindelser.

ii) DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare.

f) Uppgifter som är nödvändiga för att identifiera lokaliseringen av mobil kommunikationsutrustning.

1. Lokaliseringsbeteckning (cell-ID) för kommunikationens början.

2. Uppgifter som identifierar cellernas geografiska placering genom referens till deras lokaliseringsbeteckning (cell-ID) under den period som kommunikationsuppgifterna lagras.

2. Inga uppgifter som avslöjar kommunikationens innehåll får lagras i enlighet med detta direktiv.

Artikel 6
Lagringstider

Medlemsstaterna skall säkerställa att de kategorier av uppgifter som anges i artikel 5 lagras under en period av minst sex månader och högst två år från det datum kommunikationen ägde rum.

Artikel 7
Uppgiftsskydd och datasäkerhet

Utan att det påverkar tillämpningen av de bestämmelser som antagits i enlighet med direktiv 95/46/EG och direktiv 2002/58/EG skall varje medlemsstat säkerställa att leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät som ett minimum respekterar följande principer för datasäkerhet när det gäller uppgifter som lagras i enlighet med det här direktivet:

a) De lagrade uppgifterna skall vara av samma kvalitet och vara föremål för samma säkerhet och skydd som uppgifterna i nätverket.

b) Uppgifterna skall omfattas av lämpliga tekniska och organisatoriska åtgärder för att skyddas mot oavsiktlig eller olaglig förstöring, oavsiktlig förlust eller oavsiktlig ändring, eller otillåten eller olaglig lagring av, behandling av, tillgång till eller avslöjande av uppgifterna.

c) Uppgifterna skall omfattas av lämpliga tekniska och organisatoriska åtgärder, för att säkerställa att tillgång till dem endast ges särskilt bemyndigad personal.

d) Uppgifterna skall förstöras vid slutet av lagringstiden, utom de uppgifter för vilka tillgång har medgivits och som har bevarats.

Artikel 8
Krav för lagring av uppgifter

Medlemsstaterna skall säkerställa att uppgifter som anges i artikel 5 lagras i enlighet med detta direktiv på ett sådant sätt att uppgifterna

och annan nödvändig information som är relaterad till uppgifterna utan dröjsmål kan överföras till de behöriga myndigheterna när de begär det.

Artikel 9
Tillsynsmyndighet

1. Varje medlemsstat skall utse en eller flera offentliga myndigheter som skall ansvara för att inom landets territorium övervaka tillämpningen av de bestämmelser om lagrade uppgifters säkerhet som antagits av medlemsstaterna i enlighet med artikel 7. Dessa myndigheter får vara desamma som de som avses i artikel 28 i direktiv 95/46/EG.

2. De myndigheter som avses i punkt 1 skall vara helt oberoende när de utövar de övervakningsuppgifter som avses i den punkten.

Artikel 10
Statistik

1. Medlemsstaterna skall säkerställa att kommissionen varje år får statistik om lagring av de uppgifter som genereras eller behandlas i samband med allmänt tillgängliga elektroniska kommunikationstjänster eller ett allmänt kommunikationsnät. Denna statistik skall innefatta följande:

— De fall där information skickats till behöriga myndigheter i enlighet med nationell lagstiftning.

— Den tid som gått från det datum då uppgifterna lagrades och det datum då den behöriga myndigheten begärde överförande av uppgifterna.

— De fall där en begäran om uppgifter inte kunde tillgodoses.

2. Sådan statistik skall inte omfatta personuppgifter.

Artikel 11
Ändring av direktiv 2002/58/EG

I artikel 15 i direktiv 2002/58/EG skall följande punkt införas:

”1a. Punkt 1 skall inte tillämpas på uppgifter som specifikt skall lagras enligt 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* för de ändamål som avses i artikel 1.1 i det direktivet.

Artikel 12
Framtida åtgärder

1. En medlemsstat som står inför särskilda omständigheter som föranleder en tidsbegränsad förlängning av den högsta tillåtna lagringstid som avses i artikel 6 får vidta nödvändiga åtgärder. Medlemsstaten skall då omedelbart underrätta kommissionen och informera övriga medlemsstater om de åtgärder som vidtagits i enlighet med denna artikel och ange skälen till att de vidtagits.

2. Kommissionen skall inom sex månader efter den underrättelse som avses i punkt 1 godkänna eller förkasta de berörda nationella åtgärderna, efter att ha kontrollerat huruvida de utgör godtycklig diskriminering eller dolda handelsrestriktioner mellan medlemsstater eller inte och huruvida de utgör ett hinder för en fungerande inre marknad eller inte. Om kommissionen inte fattar något beslut inom denna tidsperiod skall de nationella åtgärderna anses vara godkända.

3. Om en medlemsstats nationella åtgärder som utgör undantag från bestämmelserna i detta direktiv godkänns i enlighet med punkt 2 får kommissionen överväga att föreslå en ändring av detta direktiv.

* EUT L 105, 13.4.2006, s. 54.”

Artikel 13
Prövning, ansvar och sanktioner

1. Varje medlemsstat skall vidta nödvändiga åtgärder för att säkerställa att de nationella åtgärder som genomför kapitel III om rättslig prövning, ansvar och sanktioner i direktiv 95/46/EG genomförs med full respekt för behandlingen av uppgifter i detta direktiv.

2. Varje medlemsstat skall särskilt vidta nödvändiga åtgärder för att säkerställa att sådan avsiktlig tillgång till eller överföring av uppgifter som lagras i enlighet med detta direktiv som är förbjuden enligt nationell lagstiftning som antagits till följd av detta direktiv beläggs med sanktioner, inbegripet administrativa eller straffrättsliga sanktioner, som är effektiva, proportionerliga och avskräckande.

Artikel 14
Utvärdering

1. Senast den 15 september 2010 skall kommissionen till Europaparlamentet och rådet översända en utvärdering av tillämpningen av detta direktiv och dess inverkan på de ekonomiska aktörerna och konsumenterna, med beaktande av den fortsatta utvecklingen av tekniken för elektronisk kommunikation och den statistik som översänts till kommissionen i enlighet med artikel 10, i syfte att avgöra om det är nödvändigt att ändra direktivets bestämmelser, särskilt vad avser listan över uppgifter i artikel 5 och de lagringstider som föreskrivs i artikel 6. Utvärderingsresultaten skall offentliggöras.

2. För detta ändamål skall kommissionen utreda alla synpunkter som inkommer från medlemsstaterna eller den arbetsgrupp som inrättats genom artikel 29 i direktiv 95/46/EG.

Artikel 15
Införlivande

1. Medlemsstaterna skall sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa detta direktiv senast den 15 september 2007. De skall genast underrätta kommis-

sionen om detta. När en medlemsstat antar dessa bestämmelser skall de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen skall göras skall varje medlemsstat själv utfärda.

2. Medlemsstaterna skall till kommissionen överlämna texten till de centrala bestämmelser i nationell lagstiftning som de antar inom det område som omfattas av detta direktiv.

3. Varje medlemsstat får till och med den 15 mars 2009 skjuta upp tillämpningen av detta direktiv i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post. Alla medlemsstater som önskar utnyttja denna bestämmelse skall underrätta rådet och kommissionen om detta i form av en förklaring när detta direktiv antas. Förklaringen skall offentliggöras i Europeiska unionens officiella tidning.

Artikel 16
Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i Europeiska unionens officiella tidning.

Artikel 17
Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den 15 mars 2006.

På Europaparlamentets vägnar	*På rådets vägnar*
J. BORRELL FONTELLES	H. WINKLER
Ordförande	*Ordförande*

Förklaring från Nederländerna i enlighet med artikel 15.3 i direktiv 2006/24/EG

När det gäller Europaparlamentets och rådets direktiv om lagring av uppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG utnyttjar Nederländerna möjligheten att skjuta upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post under högst 18 månader från och med dagen för direktivets ikraftträdande.

Förklaring från Österrike i enlighet med artikel 15.3 i direktiv 2006/24/EG

Österrike förklarar sin avsikt att skjuta upp tillämpningen av detta direktiv i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post under 18 månader från och med den tidpunkt som anges i artikel 15.1.

Förklaring från Estland i enlighet med artikel 15.3 i direktiv 2006/24/EG

I enlighet med artikel 15.3 i Europaparlamentets och rådets direktiv om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG meddelar Estland sin avsikt att utnyttja denna bestämmelse och med 36 månader från och med dagen för antagandet av föreliggande direktiv skjuta upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post.

Förklaring från Förenade kungariket i enlighet med artikel 15.3 i direktiv 2006/24/EG

Förenade kungariket förklarar i enlighet med artikel 15.3 i direktivet om lagring av uppgifter som genererats eller behandlats i sam-

band med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG att Förenade kungariket kommer att skjuta upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post.

Förklaring från Republiken Cypern i enlighet med artikel 15.3 i direktiv 2006/24/EG

Cypern förklarar att landet kommer att skjuta upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post till den dag som anges i artikel 15.3.

Förklaring från Grekland i enlighet med artikel 15.3 i direktiv 2006/24/EG

Grekland förklarar att det med tillämpning av artikel 15.3 kommer att skjuta upp tillämpningen av detta direktiv i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post till 18 månader efter det att den i artikel 15.1 angivna tidsfristen har löpt ut.

Förklaring från Storhertigdömet Luxemburg i enlighet med artikel 15.3 i direktiv 2006/24/EG

I enlighet med bestämmelserna i artikel 15.3 i Europaparlamentets och rådets direktiv 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 förklarar Storhertigdömet Luxemburgs regering att den avser åberopa artikel 15.3 i ovan nämnda direktiv för att få möjlighet att skjuta upp tillämpningen av detta direktiv i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post.

Förklaring från Slovenien i enlighet med artikel 15.3 i direktiv 2006/24/EG

Slovenien ansluter sig till den grupp medlemsstater som har gjort en förklaring i enlighet med artikel 15.3 i Europaparlamentets och rådets direktiv om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät om att skjuta upp tillämpningen av detta direktiv under 18 månader i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post.

Förklaring från Sverige i enlighet med artikel 15.3 i direktiv 2006/24/EG

Sverige vill i enlighet med artikel 15.3 ha möjlighet att skjuta upp tillämpningen av detta direktiv i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post.

Förklaring från Republiken Litauen i enlighet med artikel 15.3 i direktiv 2006/24/EG

I enlighet med artikel 15.3 i utkastet till Europaparlamentets och rådets direktiv 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 (nedan kallat ”direktivet”) förklarar Republiken Litauen att landet när direktivet antagits kommer att skjuta upp dess tillämpning i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post under den period som föreskrivs i artikel 15.3.

Förklaring från Republiken Lettland i enlighet med artikel 15.3 i direktiv 2006/24/EG

Lettland förklarar i enlighet med artikel 15.3 i 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 att det skjuter upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post till och med den 15 mars 2009.

Förklaring från Tjeckien i enlighet med artikel 15.3 i direktiv 2006/24/EG

I enlighet med artikel 15.3 förklarar Tjeckien att man uppskjuter tillämpningen av detta direktiv i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post till 36 månader efter direktivets antagande.

Förklaring från Belgien i enlighet med artikel 15.3 i direktiv 2006/24/EG

Belgien förklarar att landet, i enlighet med den möjlighet som föreskrivs i artikel 15.3 och under en period av 36 månader efter antagandet av detta direktiv, skjuter upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post.

Förklaring från Republiken Polen i enlighet med artikel 15.3 i direktiv 2006/24/EG

Polen förklarar i enlighet med den möjlighet som anges i artikel 15.3 i Europaparlamentets och rådets direktiv om lagring av uppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG att landet kommer att uppskjuta tillämpningen av lagring av kommunikationsuppgifter rörande Internetåt-

komst, Internettelefoni och Internetbaserad e-post med 18 månader från den tidpunkt som anges i artikel 15.1.

Förklaring från Finland i enlighet med artikel 15.3 i direktiv 2006/24/EG

Finland förklarar i enlighet med artikel 15.3 i direktivet om lagring av uppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster och om ändring av direktiv 2002/58/EG att Finland kommer att skjuta upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post.

Förklaring från Tyskland i enlighet med artikel 15.3 i direktiv 2006/24/EG

Tyskland förbehåller sig rätten att skjuta upp tillämpningen av detta direktiv i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post under 18 månader från och med den tidpunkt som anges i artikel 15.1 första meningen.

4 Genomförandet i andra länder

4.1 Vårt uppdrag

Enligt våra direktiv ska vi följa hur direktivet om lagring av trafikuppgifter genomförs i andra länder. Vi har inhämtat upplysningar om den rättsliga regleringen och planerade förändringar i nationell rätt i Danmark, Finland, Norge, de baltiska staterna och i några andra EU-länder. Vi har också deltagit vid de möten som kommissionen har anordnat.

I detta avsnitt redogör vi kortfattat för de nationella förslagen till genomförande i de nämnda länderna. Redovisningen tar i förekommande fall upp frågorna när länderna kommer att ha genomfört direktivet, om direktivet genomförs i sin helhet vid ett och samma tillfälle, om fler uppgifter än de som framgår av artikel 5 i direktivet kommer att lagras, hur lång lagringstiden kommer att vara, vilka leverantörer som ska vara lagringsskyldiga, om det finns möjlighet att medge undantag från lagringsskyldigheten, var uppgifterna ska lagras, vem som ska stå för kostnaderna och vilka bedömningar som görs i konkurrensfrågorna.

Vi har också försökt att få fram uppgifter om hur integritetsfrågorna har förts fram i samband med genomförandet av direktivet. Enligt de uppgifter vi har fått har integritetsfrågorna diskuterats i de enskilda länderna men debatten har inte uppfattats som ett hinder för genomförandet utan tagits till vara för att höja kvaliteten i lagstiftningsarbetet i respektive land.

4.2 Danmark

Danmark genomförde direktivet i sin helhet den 15 september 2007.

Regleringen går i några avseenden utöver artikel 5 i direktivet när det gäller vilka trafikuppgifter som ska lagras. Det avser bl.a.

uppgifter om en ”Internetsessions initierande och avslutande paket” och om lokalisering vid ett mobilsamtals slut.

Lagringstiden är ett år.

Tjänsteleverantörer som är små föreningar (andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf) och som levererar till färre än 100 ”enheter” omfattas inte av lagringsskyldigheten.

Leverantörerna får avtala med annan att fullgöra lagringsskyldigheten.

Leverantörerna står för kostnaderna för att anpassa systemen. De brottsbekämpande myndigheterna betalar en ersättning till leverantören när de begär att uppgifter ska lämnas ut. Ersättningens storlek bestäms efter diskussioner mellan leverantörernas branschorganisation och polisen.

I Danmark har man bedömt dels att direktivet kan påverka de mindre företagens möjligheter att verka på marknaden, dels att möjligheten för en leverantör att avtala med annan om att fullgöra lagringsskyldigheten gör att de negativa effekterna på konkurrensen minskar.

4.3 Finland

Finland kommer att genomföra hela direktivet vid ett tillfälle, troligen under senare hälften av år 2008. Förslaget överlämnas till parlamentet i början av december år 2007. Man bedömer att förslaget kommer att innehålla följande.

Enbart de trafikuppgifter som anges i artikel 5 i direktivet ska lagras.

Lagringstiden ska vara ett år. Många av de uppgifter som ska lagras enligt direktivet lagras redan i dag av leverantörerna i sex månader. Man bedömer att en så kort lagringstid inte skulle medföra någon förbättring för de brottsbekämpande myndigheterna.

Alla leverantörer som är anmälningspliktiga enligt kommunikationsmarknadslagen ska vara lagringsskyldiga. De riktigt små tjänsteleverantörerna är inte anmälningspliktiga och de kommer därför inte att vara lagringsskyldiga.

Leverantörerna ska kunna avtala med annan att fullgöra lagringsskyldigheten.

Staten ska ersätta leverantörernas kostnader för de tekniska investeringar som behövs för att genomföra direktivet. Staten ska också ersätta leverantörerna när uppgifter begärs ut. Utgångspunk-

ten är att leverantörerna och de brottsbekämpande myndigheterna ska komma överens om hur stor ersättningen ska vara. Om de inte kan komma överens beslutar Kommunikationsverket om ersättningens storlek.

Man bedömer att direktivet inte kommer att påverka konkurrensen eftersom staten står för de tillkommande kostnaderna.

4.4 Norge

I Norge är en arbetsgrupp tillsatt för att utreda hur direktivet kan genomföras. Arbetsgruppen består av representanter för Justitiedepartementet, Förnyelse- och administrationsdepartementet, Utrikesdepartementet, Post- och teletillsynen, Datatillsynen och polisen. Under hösten 2007 ska ett förslag sändas på remiss, varefter regeringen fattar beslut om och i så fall på vilket sätt direktivet ska genomföras. Utgångspunkten har hittills varit att direktivet ska genomföras i två etapper, en första etapp avseende fast och mobil telefoni samt Internetåtkomst och resterande i en andra etapp. Arbetsgruppen bedömer att förslaget vad avser fast och mobil telefoni kommer att innehålla följande.

Enbart de trafikuppgifter som anges i artikel 5 i direktivet ska lagras.

Lagringstiden ska vara ett år.

De leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation ska vara lagringsskyldiga. Eventuellt ska det finnas möjlighet till undantag för små leverantörer.

Uppgifterna ska lagras hos varje leverantör med möjlighet att avtala med annan om att tillhandahålla lagringskapacitet.

Arbetsgruppen har inte kunnat ange vad förslaget kommer att innehålla i kostnadsdelen.

Arbetsgruppen har bedömt att direktivet kan påverka konkurrensen genom att de små leverantörerna kan få stora investeringskostnader i nödvändig teknik samtidigt som de får enstaka förfrågningar från de brottsbekämpande myndigheterna.

4.5 Estland

Direktivet kommer att genomföras i två etapper. En första etapp rör fast och mobil telefoni. I den delen är ett förslag nu under beredning, och man förväntar sig omfattande diskussioner. Man bedömer att förslaget bör kunna träda i kraft under första halvåret år 2008. I en andra etapp genomförs direktivet såvitt avser Internetåtkomst, Internettelefoni och Internetbaserad e-post. Det ska ske senast den 15 mars 2009. Man bedömer att förslaget i sin helhet kommer att innehålla följande.

Enbart de trafikuppgifter som anges i artikel 5 i direktivet ska lagras.

Lagringstiden ska vara ett år.

Samtliga leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät ska vara lagringsskyldiga. Det ska inte finnas någon möjlighet till undantag.

Uppgifterna ska lagras hos varje leverantör.

Leverantörerna ska stå för investeringskostnaderna och erhålla ersättning från de brottsbekämpande myndigheterna när uppgifter lämnas ut.

4.6 Lettland

Lettland har sedan år 2003 en lagringsskyldighet med en lagringstid på tre år. Direktivet kommer att genomföras i två etapper. En första etapp rör fast och mobil telefoni som genomförs under oktober 2007. I en andra etapp genomförs direktivet såvitt avser Internetåtkomst, Internettelefoni och Internetbaserad e-post. Det ska ske den 15 mars 2009. Förslaget i sin helhet innehåller följande.

Enbart de trafikuppgifter som anges i artikel 5 i direktivet ska lagras.

Lagringstiden ska vara 18 månader.

Samtliga leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät ska vara lagringsskyldiga. Det ska inte finnas någon möjlighet till undantag.

Uppgifterna ska lagras hos varje leverantör.

Leverantörerna ska som i dag stå för alla kostnader som lagringsskyldigheten medför.

4.7 Litauen

Direktivet föreslås bli genomfört den 1 december 2007 när det gäller fast och mobil telefoni och den 15 mars 2009 i övriga delar. Förslaget i sin helhet innehåller följande.

Enbart de trafikuppgifter som anges i artikel 5 i direktivet ska lagras.

Lagringstiden ska vara ett år.

Samtliga leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät ska vara lagringsskyldiga. Det ska inte finnas någon möjlighet till undantag.

Leverantörerna ska kunna avtala med annan att fullgöra lagringsskyldigheten.

Leverantörerna ska stå för samtliga kostnader. Tidigare har leverantörerna fått kompensation för uppgifter som de har lagrat för längre period än vad de har behövt för egna ändamål. Den möjligheten ska nu tas bort.

Eftersom alla leverantörer står för kostnaderna bedömer man att det inte blir någon påverkan på konkurrensen.

4.8 Irland

Irland har sedan år 2002 en lagringsskyldighet avseende telefoni och har inte utnyttjat möjligheten att skjuta upp genomförandet av direktivet avseende Internet. Hela direktivet kommer därför att genomföras vid ett och samma tillfälle. Om direktivet kan genomföras i s.k. secondary legislation kommer det att genomföras den 1 januari 2008. Om direktivet ska genomföras i s.k. primary legislation kommer det att ske under år 2008. I primary legislation, som antas av parlamentet, är det möjligt att göra ändringar i förhållande till direktivet. I secondary legislation har befogenheterna delegerats till en minister eller en myndighet, vilket innebär att några ändringar eller tillägg inte kan göras. Man bedömer att förslaget kommer att ha följande innehåll.

Enbart de trafikuppgifter som anges i artikel 5 i direktivet ska lagras.

Den nuvarande lagringstiden om tre år ska behållas för fast och mobil telefoni. Beträffande Internetuppgifter ska lagringstiden vara sex månader.

Lagring ska utföras av de leverantörer som de brottsbekämpande myndigheterna bestämmer. Denna ordning ska ses mot bak-

grund av att man i Irland sedan länge har ett system där leverantörerna frivilligt lagrar trafikuppgifter för brottsbekämpande ändamål och att det således finns en vilja hos leverantörerna att lagra uppgifter som kan vara till nytta för de brottsbekämpande myndigheterna.

Uppgifterna ska lagras hos varje leverantör.

Leverantörerna ska som i dag stå för alla kostnader som lagringsskyldigheten medför. Leverantörerna har inga invändningar mot att stå för kostnaderna så länge det är lika för samtliga leverantörer. Någon ersättning ska inte utgå till leverantörerna vid utlämnande av uppgifter.

4.9 Spanien

Spanien har inte utnyttjat möjligheten att skjuta upp genomförandet av direktivet avseende Internet. Hela direktivet bedöms bli genomfört den 1 december 2007. Förslaget ska enligt uppgift ha följande innehåll.

Enbart de trafikuppgifter som anges i artikel 5 i direktivet ska lagras.

Lagringstiden ska vara ett år.

Samtliga leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät ska vara lagringsskyldiga. Det ska inte finnas någon möjlighet till undantag.

Uppgifterna ska lagras hos varje leverantör.

Leverantörerna ska stå för samtliga kostnader.

Man har inte haft några diskussioner om huruvida direktivet påverkar konkurrensen.

4.10 Storbritannien

I Storbritannien finns sedan år 2001 en frivillig lagring av trafikuppgifter avseende fast och mobil telefoni. Direktivet genomfördes den 1 oktober 2007 avseende fast och mobil telefoni. Det är osäkert när direktivet kommer att genomföras avseende Internet. Beträffande fast och mobil telefoni gäller följande.

Enbart de uppgifter som anges i artikel 5 i direktivet ska lagras.

Lagringstiden ska vara ett år.

Det finns inte några undantag från lagringsskyldigheten. Däremot kommer man enligt uppgift inte att vidta några åtgärder mot

de leverantörer som inte lagrar uppgifter, om det är frågan om leverantörer som inte bedöms ha en verksamhet som genererar eller behandlar trafikuppgifter som är intressanta för de brottsbekämpande myndigheterna.

Leverantörerna kan avtala med annan att fullgöra lagringsskyldigheten.

Det allmänna står för alla kostnader som uppkommer för att lagra trafikuppgifter.

Eftersom det allmänna står för alla kostnader gör man den bedömningen att direktivet inte påverkar konkurrensen mellan stora och små företag. Däremot bedöms det system för ersättning som man tillämpar kunna påverka konkurrensen inom Europa.

4.11 Tjeckien

Det finns ett förslag om att direktivet ska genomföras i sin helhet den 1 januari 2008. Förslaget har enligt uppgift följande innehåll.

Enbart de trafikuppgifter som anges i artikel 5 i direktivet ska lagras.

Lagringstiden ska vara sex månader.

Samtliga leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät ska vara lagringsskyldiga med undantag för de leverantörer som endast har e-posttjänster.

Uppgifterna ska lagras hos varje leverantör.

En kostnadsfördelning ska finnas, enligt vilken leverantörerna ska stå för de tekniska investeringar som behövs och få ersättning av de brottsbekämpande myndigheterna dels för redovisade och godkända avskrivningar rörande lagringskostnaderna, dels när uppgifter begärs ut. Om leverantören och de brottsbekämpande myndigheterna inte kommer överens om vilka avskrivningskostnader som ska ersättas, ska ersättningen bestämmas av motsvarigheten till svenska PTS. Ersättningen för utlämnande av trafikuppgifter bestäms i författning och varierar beroende på vilken typ av uppgift som begärs ut och om uppgiften lämnas ut automatiserat eller om manuella insatser krävs.

Det har inte förekommit några diskussioner om vad direktivet kan få för effekter på konkurrensen.

4.12 Tyskland

Direktivet avseende fast och mobil telefoni föreslås bli genomfört den 1 januari 2008 och avseende Internet den 1 januari 2009. Förslaget i sin helhet har följande innehåll.

Enbart de trafikuppgifter som anges i artikel 5 i direktivet ska lagras.

Lagringstiden ska vara sex månader. Den tyska författningen medger inte en längre lagringstid.

Lagringsskyldigheten ska gälla för alla leverantörer som har fler än 10 000 kunder.

Leverantörerna ska kunna avtala med annan att fullgöra lagringsskyldigheten.

Leverantörerna ska stå för kostnaderna för att anpassa systemen. De brottsbekämpande myndigheterna ska betala en ersättning till leverantören när de begär att uppgifter ska lämnas ut.

Det har inte förekommit några diskussioner om vad direktivet kan få för effekter för konkurrensen.

5 Skyddet för den personliga integriteten

5.1 En stor mängd trafikuppgifter ska lagras

Direktivet om lagring av trafikuppgifter innebär att det blir en regel att vissa trafikuppgifter ska lagras under den tid och på det sätt som närmare preciseras av de olika bestämmelser vi föreslår för genomförandet av direktivet. Till skillnad mot vad som gäller i dag när varje leverantör själv har att bedöma vilka uppgifter som behöver sparas för tillåtna ändamål och hur länge det behöver ske, ska samtliga de trafikuppgifter som anges i direktivet lagras under en viss bestämd tid. Genomförandet av direktivet kan sägas öka förutsättningarna för en högre grad av säkerhet för enskilda genom att enhetliga bestämmelser införs om vad som ska lagras samt under vilken tid och på vilket sätt det ska ske. En direkt följd av genomförandet kommer också att bli att avsevärt fler uppgifter ska lagras och att lagringen i många fall kommer att pågå under längre tid än i dag.

Det är svårt att uppskatta den mängd trafikuppgifter som kommer att lagras vid varje given tidpunkt. En utgångspunkt för bedömningen kan vara antalet abonnemang. Den 31 december 2006 fanns det i Sverige 5 551 000 abonnemang för fast telefoni, 9 607 000 för mobil telefoni och 3 471 000 kunder med Internetaccess. Under år 2007 har antalet abonnemang ökat ytterligare.

Kommunikation via elektroniska kommunikationstjänster och nät är numera en integrerad del i de flesta människors livsmönster. Teknikutvecklingen innebär nya möjligheter till kommunikationslösningar. Det innebär att även om lagringsskyldigheten begränsas till trafikuppgifter som de brottsbekämpande myndigheterna kan ha tillgång till i dag och som avser fast och mobil telefoni samt Internetåtkomst, e-post och Internettelefoni kan man utgå från att

antalet trafikuppgifter per dygn som ska lagras kommer att bli mycket stort.

5.2 Lagring av trafikuppgifter påverkar integriteten

Den lagring av trafikuppgifter som ska genomföras till följd av direktivet innebär att mycket stora informationsmängder rörande enskildas kommunikation kommer att lagras under en viss tid. Man kan utgå från att endast en ytterst begränsad del av de lagrade trafikuppgifterna kommer att begäras utlämnade för att användas vid bekämpningen av allvarlig brottslighet. Merparten av trafikuppgifterna kommer således att vara lagrade utan att de används för de brottsbekämpande syftena.

Trafikuppgifter är i många fall uppgifter om enskildas personliga förhållanden och korrespondens och det är mot bakgrund av uppgifternas integritetskänsliga karaktär som bestämmelserna i rättegångsbalken om hemlig teleövervakning och i lagen om elektronisk kommunikation om tystnadsplikt och undantag från tystnadsplikten har utformats. Att få ut trafikuppgifter för utredning om brott har ansetts vara särskilt känsligt från integritetssynpunkt och förutsättningarna för utlämnande är noggrant reglerade.

Enligt vår mening är dock inte frågan om integritetsskyddet vid lagring av trafikuppgifter begränsad till de situationer där trafikuppgifter lämnas ut till de brottsbekämpande myndigheterna. En utgångspunkt för våra resonemang är att en generell lagring av trafikuppgifter i den omfattning som direktivet förutsätter påverkar både enskildas upplevelse av att få sin privata sfär inskränkt och integritetsskyddet för medborgarna i allmänhet. Intrånget i integriteten sker enligt vår mening redan genom att det allmänna säkrar tillgången till trafikuppgifterna genom lagringen.

Redan existensen av ett regelsystem som innebär att uppgifter om människors kommunikation med fast och mobil telefoni eller Internet ska lagras har således en påverkan på enskildas integritetsskydd och upplevelse av integritetsintrång. Det innebär med nödvändighet att den frihet att kommunicera som bör finnas mellan människor som använder kommunikationstjänster upplevs som inskränkt. Lagringen utgör i sig ett intrång i såväl privatliv som korrespondens och kan komma i konflikt såväl med den rätt till skydd för privatlivet var och en har enligt artikel 8 i Europakonven-

tionen som med det grundlagsskydd som denna rätt har enligt 2 kap. 6 § regeringsformen (se avsnitt 5.6).

5.3 Risker för integriteten

Vid den hearing om integritetsfrågor som utredningen genomförde i juni 2007 lyftes behovet av tillgång till trafikuppgifter i bekämpningen av allvarlig brottslighet fram liksom att regelsystemet i dag innebär att trafikuppgifter för brottsbekämpning lämnas ut endast efter det att hänsyn till integritetsaspekter har tagits. Huvuddelen av hearingen behandlade de integritetsaspekter som enligt deltagarna bör beaktas vid genomförandet av direktivet om lagring av trafikuppgifter. Vi sammanfattar i detta avsnitt de synpunkterna så fullständigt som möjligt och utan några egna ställningstaganden.

Vid hearingen framfördes att generella åtgärder som innebär att uppgifter om enskilda samlas in är mer problematiska från integritetssynpunkt än specifika åtgärder i enskilda fall. Lagringsskyldigheten innebär att trafikuppgifter som på något sätt rör praktiskt taget alla medborgare kommer att finnas lagrade. Uppgifterna kan ge kännedom om förhållanden av privat natur som man inte vill att andra ska få insyn i. Det är vetskapen om att dessa uppgifter finns lagrade och kan tas fram och granskas under lagringstiden och risken för att de läcker ut till obehöriga som är det allvarliga bekymret från integritetssynpunkt. Lagstiftningen riskerar att få en psykologisk verkan som innebär att människor blir rädda och misstänksamma och i högre grad upplever att de lever i ett kontrollsamhälle. Det kan påverka tilltron till myndigheterna. Därmed uppkommer en risk för att lagstiftningen ändrar människors attityder och beteendemönster. Man kommer att tänka sig för på ett annat sätt än tidigare innan man använder sin telefon eller sin dator.

Det framhölls att dessa effekter är den stora integritetsskadan och inte det förhållandet att vissa uppgifter i ett begränsat antal fall kan begäras ut av de brottsbekämpande myndigheterna i anledning av en utredning om misstänkt allvarlig brottslighet.

Flera synpunkter på risker för läckage framfördes också av deltagarna. En ökad informationsvolym innebär allmänt sett en ökad risk för att informationen läcker eller sprids till obehöriga. Uppgifter kan komma ut genom bristande säkerhetsrutiner eller genom medvetna åtgärder. De trafikuppgifter som kommer att finnas lagrade har naturligtvis inte bara intresse i vissa fall för brottsbekämp-

ningen. Den betydande informationsmängd som kommer att finnas lagrad har också ett intresse i många andra sammanhang. Uppgifter om enskildas kommunikationer som kommer i orätta händer kan medföra intrång i integriteten på olika sätt och i olika grad beroende på vilka uppgifter det är frågan om. Man pekade också på de risker som kan uppkomma om trafikuppgifter lagras i eller förs över till andra länder.

Även risken för att trafikuppgifter kommer att användas för andra ändamål belystes under hearingen. Lagrade trafikuppgifter möjliggör kartläggningar av olika slag och kan ha ett betydande ekonomiskt värde samtidigt som de kan orsaka stora skador från integritetssynpunkt. Uppgifterna kan också ha stor betydelse från konkurrenssynpunkt och orsaka förskjutningar i den fria konkurrensen på olika marknader.

Vid hearingen framfördes också att det finns en risk för att de brottsbekämpande myndigheterna kan komma att utnyttja trafikuppgifter i mycket högre utsträckning än tidigare. Mot det anfördes att trafikuppgifterna behövs för utredning om allvarlig brottslighet och att de leder till att fler allvarliga brott klaras upp och att fler brottsoffer därmed kan få upprättelse.

En annan faktor som berördes vid hearingen är risken för ändamålsglidning, dvs. risken för att när systemet för lagring av trafikuppgifter väl finns och fungerar kommer det att användas för andra syften än det ursprungligen var tänkt för.

När det gäller regleringen av lagring av trafikuppgifter lades särskild tyngd vid behovet av ett säkert, öppet och transparent regelsystem som innebär att medborgarna kan bedöma vilka trafikuppgifter som kommer att lagras och hur länge samt hur uppgifterna används i brottsbekämpningen. Det pekades särskilt på behovet av förhandskontroll och efterhandskontroll i form av uppföljning och andra rättsäkerhetsgarantier som en viktig förutsättning för medborgarnas förtroende både för regelsystemet och det allmännas tillämpning av det.

5.4 Balans mellan brottsbekämpning och integritetsskydd ska uppnås

Bestämmelser om lagring av trafikuppgifter håller på att genomföras eller har genomförts i alla länder i EU. Det följer av Sveriges medlemskap i unionen att direktivet om lagring av trafikuppgifter

ska genomföras även här. Vår uppgift är att föreslå hur genomförandet ska regleras.

Direktivet innehåller inte bara en uppräkning av vilka trafikuppgifter som ska lagras utan också flera artiklar som ska garantera en rimlig proportion mellan intresset av att allvarliga brott utreds och lagförs och integritetsskyddet. Det gäller t.ex. den längsta acceptabla lagringstiden, att uppgifterna ska utplånas vid slutet av den tiden och att uppgifterna ska skyddas mot olika åtgärder som är skadliga från integritetsskyddssynpunkt.

I svensk rätt är skyddet för enskildas integritet reglerat i bl.a. 2 kap. 6 § regeringsformen. Därutöver gäller Europakonventionen som svensk rätt. Det innebär att den nationella reglering som genomför direktivet måste ha sin utgångspunkt i de krav som ställs på skydd för den personliga integriteten i grundlagen och konventionen. I vårt uppdrag ingår att belysa de integritetsaspekter som aktualiseras vid genomförandet av direktivet. Vi ska också beakta de bestämmelser om integritetsskydd som följer av dataskyddsdirektivet (95/46/EG) och direktivet om integritet och elektronisk kommunikation (2002/58/EG) samt de bestämmelser i svensk rätt som genomför dessa direktiv. I vårt uppdrag ligger också att följa det arbete som den s.k. artikel 29-gruppen kan komma att initiera med anledning av de nationella genomförandena av direktivet om lagring av trafikuppgifter.

5.5 Integritetsskydd enligt artikel-29 gruppen och Europeiska datatillsynsmannen

5.5.1 Artikel 29-gruppen

Av artikel 29 i dataskyddsdirektivet framgår att det ska inrättas en arbetsgrupp på gemenskapsnivå för skydd av enskilda personer i samband med behandling av personuppgifter. Artikel 29-gruppen har övervägt integritetsfrågor i anledning av de nationella genomförandena av direktivet om lagring av trafikuppgifter. Gruppen har anfört att det är av yttersta vikt att direktivet genomförs på ett sådant sätt att effekterna på privatlivet begränsas och att genomförandet åtföljs av åtgärder som skyddar den personliga integriteten. Gruppen har också understrukit behovet av en harmoniserad tolkning av direktivets bestämmelser och vikten av harmonisering av de nationella genomförandena av direktivet för att säkerställa samma

skyddsnivå för alla EU-medborgare. Därför vill gruppen se ett enhetligt genomförande av direktivet i hela EU. För att detta ska kunna ske och för att uppfylla kraven i artikel 8 i Europakonventionen ska medlemsstaterna genomföra lämpliga och specifika skyddsåtgärder. Gruppen föreslår att minst följande skyddsåtgärder ska beaktas:

1) Uppgifterna bör endast lagras i särskilda syften och termen ”allvarliga brott” bör tydligt definieras och avgränsas. All ytterligare behandling bör uteslutas eller strikt begränsas genom särskilda skyddsåtgärder.

2) Uppgifterna ska bara vara tillgängliga för särskilt utsedda myndigheter som ansvarar för brottsbekämpning och överlämnas när det krävs för utredning, avslöjande och lagföring av de brott som anges i direktivet. En förteckning över vilka de särskilt utsedda myndigheterna är bör offentliggöras.

3) De uppgifter som ska lagras bör begränsas till ett minimum och alla ändringar av förteckningen över dessa uppgifter ska omfattas av ett strängt nödvändighetstest.

4) Utredning, avslöjande och lagföring av de brott som anges i direktivet får inte medföra någon storskalig datautvinning på basis av lagrade uppgifter avseende rese- och kommunikationsmönster för personer som de brottsutredande myndigheterna inte misstänker.

5) Tillgång till uppgifter bör i princip beviljas av de rättsliga myndigheterna efter en bedömning från fall till fall, utom i de länder där sådan tillgång regleras i lag. I tillämpliga fall bör det i handlingarna om beviljande av tillgång anges vilka typer av uppgifter som behövs i det aktuella fallet.

6) Tillhandahållare av allmänna elektroniska kommunikationstjänster eller kommunikationsnätverk bör inte ha rätt att bearbeta data som enbart lagras med hänsyn till den allmänna ordningen, enligt direktivet om lagring av uppgifter, för andra ändamål, särskilt inte för egna syften.

7) Särskilt systemen för lagring av data med hänsyn till den allmänna ordningen ska hållas logiskt åtskilda från de system som används för affärsverksamheten.

8) Miniminormer ska utformas avseende de tekniska och organisatoriska säkerhetsåtgärder som tillhandahållarna ska vidta, och de ska hänvisa närmare till de allmänna kraven i direktivet om lagring av uppgifter.

5.5.2 Europeiska datatillsynsmannen

Med stöd i förordningen om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EG nr 45/2001) har en oberoende tillsynsmyndighet med namnet Europeiska datatillsynsmannen inrättats. Datatillsynsmannens uppdrag är att säkerställa att fysiska personers grundläggande fri- och rättigheter, särskilt deras rätt till privatliv, respekteras med avseende på behandling av personuppgifter av gemenskapsinstitutionerna och gemenskapsorganen. Datatillsynsmannen deltar också i artikel 29-gruppens arbete.

Datatillsynsmannen avgav i anledning av förslaget till direktiv om lagring av trafikuppgifter ett yttrande till kommissionen (2005/C 298/01). Datatillsynsmannen hänförde sig till vikten av att medlemsstaternas brottsbekämpande organ förfogar över alla nödvändiga rättsinstrument, särskilt i kampen mot terrorism och andra allvarliga brott och menade att en adekvat tillgång till vissa trafikuppgifter kan vara ett avgörande redskap för de brottsbekämpande organen och bidra till människors fysiska säkerhet. Datatillsynsmannen menade också att om man betraktar förslaget endast ur ett uppgiftsskyddsperspektiv bör trafikuppgifter över huvud taget inte bevaras i brottsbekämpande syfte. Därför är det enligt datatillsynsmannen viktigt att direktivet inte leder till att människor berövas sin grundläggande rätt till integritetsskydd.

Datatillsynsmannen menade att lagring av trafikuppgifter endast kan motiveras enligt gemenskapsrätten om proportionalitetsprincipen respekteras och lämpliga skyddsåtgärder vidtas. För att förslaget ska vara lämpligt och effektivt krävs enligt datatillsynsmannen att det finns effektiva sökmotorer så att myndigheterna har riktad och snabb tillgång till de uppgifter som behövs i ett specifikt fall. Av förslaget ska därför enligt datatillsynsmannen framgå att leverantörerna är skyldiga att installera den nödvändiga tekniska strukturen, inklusive sökmotorer. Därutöver bör förslaget för att vara proportionerligt begränsa lagringstiderna och antal uppgifter som ska lagras och det måste återspegla styrkta behov från brottsbekämpningens sida. Det måste också säkerställas att det är omöjligt att komma åt uppgifternas innehåll. Slutligen bör förslaget innehålla lämpliga skyddsåtgärder. Som lämpliga skyddsåtgärder angav datatillsynsmannen åtgärder som säkerställer att tillgången till och vidareanvändningen av uppgifterna begränsas enbart till särskilda

omständigheter och för ett begränsat antal särskilda ändamål. Vidare ska databaserna skyddas på lämpligt sätt för att motverka ”dumpning” eller utnyttjande av uppgifterna. Det måste också garanteras att uppgifterna utplånas effektivt när bevarandetiden löpt ut och det ska införas krav på att leverantörerna utplånar uppgifterna automatiskt och minst en gång om dagen.

5.6 Grundläggande regler i svensk rätt om skyddet för den personliga integriteten

5.6.1 Regeringsformen

I 1 kap. 2 § fjärde stycket regeringsformen anges att det allmänna ska värna den enskildes privatliv och familjeliv. I 2 kap. finns bestämmelser som skyddar medborgarna mot ingrepp från det allmänna.

I 2 kap. 3 § andra stycket finns en grundläggande bestämmelse om integritetsskydd vid automatiserad behandling. Regeln slår fast att varje medborgare i den utsträckning som närmare anges i lag ska skyddas mot att dennes personliga integritet kränks genom att uppgifter registreras med hjälp av automatisk databehandling. Personuppgiftslagen är en sådan lag som avses i bestämmelsen. Integritetsskyddet ges inte bara gentemot det allmänna utan också gentemot enskilda.

Bestämmelsen i 2 kap. 6 § innebär att varje medborgare gentemot det allmänna är skyddad mot bl.a. husrannsakan och liknande intrång, undersökning av brev eller andra förtroliga försändelser samt mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. Skyddet för förtroligt meddelande omfattar meddelanden som sänds med posten eller på annat sätt som brev, telegram, bandinspelningar eller i sådan form att det kan bli föremål för beslag.

Det skydd som ges av 2 kap. 6 § får enligt 2 kap. 12 § endast begränsas genom lag och endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. Begränsningarna får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett begränsningarna och får inte heller sträcka sig så långt att de utgör ett hot mot den fria åsiktsbildningen, som är en av folkstyrelsens grundvalar. Dessutom får begränsningar inte göras

enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning.

Mot bakgrund av hur de integritetsskyddande bestämmelserna i regeringsformen är utformade anses främst fyra allmänna principer gälla för användande av tvångsåtgärder mot enskilda. Dessa är legalitets-, ändamåls-, behovs- och proportionalitetsprinciperna.

Legalitetsprincipen finns direkt uttryckt i 2 kap. 12 §. Ändamålsprincipen innebär att en myndighets befogenhet att använda tvångsmedel ska var bunden till det ändamål för vilket tvångsmedlet har beslutats. Behovsprincipen innebär att en tvångsåtgärd inte bör företas, om det inte är nödvändigt med hänsyn till syftet med åtgärden och en mindre ingripande åtgärd är tillräcklig. Proportionalitetsprincipen innebär att ett tvångsmedel får tillgripas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär, dvs. om tvångsåtgärden i fråga om art, styrka, räckvidd och varaktighet står i rimlig proportion till vad som står att vinna med åtgärden.

De nu behandlade bestämmelserna i regeringsformen gäller för svenska medborgare. Om inte annat är föreskrivet är utlänning här i riket likställd med svenska medborgare i angivet hänseende (2 kap. 22 §).

5.6.2 Europakonventionen

Sedan år 1995 gäller den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) som svensk lag. I 2 kap. 23 § regeringsformen finns ett förbud mot att meddela lag eller annan föreskrift i strid med Sveriges åtaganden på grund av konventionen.

Lagring av trafikuppgifter berör främst artikel 8 om rätten till respekt för privatliv, familjeliv, hem och korrespondens, men också artikel 10 om rätten till yttrandefrihet och artikel 13 om rätten till ett effektivt rättsmedel.

Det saknas möjlighet att inom ramen för denna redovisning fullödigt redovisa för europeisk praxis med angivande av enskilda domar och beslut. Den följande redovisningen är således sammanfattande. För kompletterande uppgifter hänvisas till Hans Danelius, Mänskliga rättigheter i europeisk praxis, 2 uppl., år 2002 samt till de i det följande angivna rättsfallen.

Artikel 8:1 stadgar att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Innebörden i denna artikel är att staten ska avhålla sig från ingrepp på individnivå och i form av mer generella inskränkningar av medborgarnas integritetsskydd. Artikeln innebär också ett åläggande för staten att vidta positiva åtgärder för att skydda enskildas privata sfär. De krav på skyddsåtgärder som ställs på staten måste vara rimliga. I huvudsak kan det förväntas att staten utfärdar lagar och förordningar som ger ett tillfredsställande skydd (Danelius s. 261).

Skyddet får inskränkas enligt artikel 8:2 men endast under vissa förutsättningar. Inskränkningen måste ha stöd i lag och får göras endast om det i ett demokratiskt samhälle är nödvändigt med hänsyn till statens säkerhet, den allmänna säkerheten, landets ekonomiska välstånd eller till förebyggande av oordning eller brott eller till skydd för hälsa eller moral eller personers fri- och rättigheter. Kravet på att inskränkningen ska ha lagstöd anses innebära att inskränkningen måste vara utformad med en sådan precision att den är i rimlig utsträckning förutsebar. Om lagen ger de rättstillämpande organen ett tolkningsutrymme och en rätt till skönsmässig bedömning är det inte oförenligt med kravet på förutsebarhet under förutsättning att gränserna för den skönsmässiga bedömningen är tillräckligt klara för att ge den enskilde skydd mot godtyckliga ingrepp. Lagen måste också vara tillgänglig för allmänheten.

Att ingreppet måste vara nödvändigt innebär inte enligt Europadomstolen att det ska vara oundgängligt. Däremot måste det föreligga ett angeläget samhälleligt behov. Vid bedömningen av nödvändigheten tillämpas proportionalitetsprincipen. Den innebär en avvägning mellan hur stort ingreppet i den enskildes rätt är och hur starkt det behov är som ska tillgodoses genom ingreppet. Det är endast om det finns ett rimligt förhållande mellan dessa två faktorer som ingreppet är proportionerligt och det är endast då ingreppet kan anses nödvändigt i ett demokratiskt samhälle (Danelius s. 58 och 263 f.).

Begreppet privatliv ska förstås i bred mening. Det tar i första hand sikte på enskilda individers rätt till personlig utveckling och rätten att etablera och utveckla relationer till andra människor. Även yrkesmässiga aktiviteter kan omfattas av rätten till respekt för privatlivet. Hemlig teleavlyssning utgör som utgångspunkt ett ingrepp i rätten till respekt för privatlivet men också i rätten till korrespondens. Detsamma gäller hemlig teleövervakning även om

myndigheterna då inte tar del av innehållet i förmedlade telemeddelanden.

Rätten till respekt för korrespondens har en vid betydelse och omfattar många slag av medelbar kommunikation med andra. Med korrespondens avses brev och andra försändelser med post och överföring av meddelanden med hjälp av telefon, telefax, radio och datorer (Danelius s. 270).

Genom Europadomstolens praxis har begreppet rätten till respekt för privat- och familjeliv, hem och korrespondens fått en tydligare avgränsning.

Europadomstolen har funnit att hantering av flera av de typer av uppgifter som enligt artikel 5 i direktivet om lagring av trafikuppgifter ska lagras utgör ett intrång i den skyddade rättigheten enligt artikel 8 i Europakonventionen. Av domstolens praxis framgår att lagring av information om en person anses utgöra ett intrång i privatlivet, trots att informationen inte innehåller några känsliga uppgifter (Amann mot Schweiz). Detsamma gäller för s.k. samtalsmätning som inbegriper användning av utrustning som automatiskt registrerar uppringda nummer på en telefon samt tidpunkt och längd för varje samtal (Malone mot Storbritannien). Domstolen har också funnit att ett inhämtande av uppgifter om vilka samtal som har ringts från en viss telefon utgör ett intrång i den skyddade rätten i artikel 8 (P.G. och J.H. mot Storbritannien). Det framgår också av domstolens praxis (Amann mot Schweiz) att det är ett intrång i artikel 8 om en registrerad uppgift om en enskild person inte förstörs vid den tidpunkt som angetts i lag.

Trots att domstolen har funnit att ett intrång i den enskildes rätt till privat- och familjeliv, hem och korrespondens föreligger kan intrånget vara berättigat om kraven på proportionalitet i artikel 8:2 är uppfyllda. Det går således inte att säga att vissa ingrepp alltid utgör en kränkning av rättigheten i artikel 8:1. Däremot kan de utgöra ett ingrepp i artikel 8:1 som med stöd av 8:2 är konventionsenligt. Så har domstolen t.ex. ansett i rättsfallet P.G. och J.H. mot Storbritannien när polisen i spaningssyfte inhämtat upplysningar från ett telefonbolag om vilka samtal som hade ringts från ett visst telefonnummer. Däremot har domstolen i avgörandet Amann mot Schweiz menat att det inte funnits lagstöd för att uppgifter om Amanns telefonsamtal registrerats i ett kortregister och att den enskilde alltså kunde anpassa sitt handlade till lagens krav. Också i rättsfallet Malone mot Storbritannien menade domstolen att den registrering av telefonnummer som hade företagits inte svarade

mot kravet på laglighet då de regler som tillämpats var otydliga och kunde tolkas på olika sätt.

5.7 Våra fortsatta överväganden

Lagringen av trafikuppgifter medför ett intrång i den personliga integriteten. Vi behandlar därför integritetsfrågor i samband med flera av våra resonemang. En utgångspunkt för våra överväganden är att lagringen av trafikuppgifter ska regleras så att systemet blir transparent och gör det möjligt för medborgarna att förutse vilka uppgifter som ska lagras och hur de typiskt sett används i brottsbekämpningen. Detta innebär att regleringen av vilka trafikuppgifter som ska lagras ska vara klar och tydlig och medge lagring endast om det följer av direktivet eller kan motiveras med stöd av artikel 15.1 i direktivet om integritet och elektronisk kommunikation. Vi behandlar dessa frågor i avsnitt 6.

Det är också en viktig utgångspunkt att integritetsfrågor beaktas vid bedömning av var lagring ska ske och av vilka, lagringstiden och andra villkor för lagringen. Vi behandlar dessa frågor i avsnitt 7.

För att lagringen ska fungera som det är tänkt samtidigt som skyddet för enskildas integritet hålls på en hög nivå, måste en rad olika frågor som gäller lagringen och skyddet av de lagrade trafikuppgifterna övervägas. Det sker i avsnitt 8.

Ytterligare en utgångspunkt för vårt arbete är att det ska finnas regler som innebär att missbruk av systemet beivras och att den som får sin integritet kränkt kan få ersättning. Dessa frågor och tillsynsfrågor behandlas i avsnitt 9 och 10.

De brottsbekämpande myndigheternas möjligheter att få tillgång till trafikuppgifter är begränsade i syfte att nå en godtagbar balans mellan intresset av att bekämpa allvarlig brottslighet och intresset av integritetsskydd. Den lagring av trafikuppgifter som nu ska genomföras innebär att det finns anledning att på nytt överväga om de nuvarande reglerna upprätthåller denna balans. Dessa och ytterligare frågor behandlas i avsnitt 11. I avsnitt 12 gör vi en sammanfattande analys av hur integritetsfrågor och intresset av att bekämpa allvarlig brottslighet balanseras i våra förslag om genomförande av direktivet.

6 Trafikuppgifter som ska lagras

6.1 Sammanfattning av våra förslag och bedömningar

- Tillgång till trafikuppgifter är av avgörande betydelse för bekämpning av allvarlig brottslighet.
- Lagringsskyldigheten ska genomföras så att den omfattar de uppgifter som de brottsbekämpande myndigheterna kan ha tillgång till i dag.
- Regleringen ska vara tydlig och väl avgränsad och utformad så att den så långt det är möjligt blir oberoende av den tekniska utvecklingen.
- Lagringsskyldigheten innebär inte en uttömmande uppräkning av vilka uppgifter som de brottsbekämpande myndigheterna har rätt att få från leverantörerna.
- Den enskilde leverantörens lagringsskyldighet ska enbart omfatta uppgifter som denne någon gång genererar eller behandlar.
- De uppgifter som ska lagras får inte avslöja kommunikationens innehåll.
- Lagringsskyldigheten ska struktureras i kategorierna telefoni, meddelandehantering, Internetåtkomst och anslutningsform.
- Vid *telefoni* ska följande uppgifter lagras:
  – Uppringande telefonnummer
  – Nummer som slagits och nummer till vilka samtalet styrts
  – Uppgifter om abonnent och registrerad användare
  – Datum och spårbar tid då kommunikationen påbörjades och avslutades
  – Den tjänst som använts
  – Slutpunkter
- Vid *mobil telefoni* ska *dessutom* följande uppgifter lagras:
  – Den uppringande och den uppringda partens abonne-

mangsidentitet och utrustningsidentitet
– Lokaliseringsinformation för kommunikationens början och slut
– Datum, spårbar tid och lokaliseringsinformation för den första aktiveringen av en förbetald anonym tjänst

- Vid *Internettelefoni* ska *dessutom* följande uppgifter lagras:
  – Uppringande parts IP-adresser
  – Uppringd parts IP-adresser
- Vid *meddelandehantering* ska följande uppgifter lagras:
  – Avsändarens och mottagarens meddelandeadress
  – Uppgifter om abonnent och registrerad användare
  – Datum och spårbar tid för på- och avloggning i meddelandetjänsten
  – Datum och spårbar tid för avsändande och mottagande av meddelandet
  – Den tjänst som har använts och spårbar tid för användandet
- Vid *Internetåtkomst* ska följande uppgifter lagras:
  – Användarens IP-adresser
  – Uppgifter om abonnent och registrerad användare
  – Datum och spårbar tid för på- och avloggning i Internettjänsten
  – Typen av Internetanslutning som använts
  – Slutpunkter
- Vid verksamheter som tillhandahåller kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst *(anslutningsform)* ska följande uppgifter lagras:
  – Uppgifter om abonnent
  – Vilken typ av kapacitet för överföring som har använts och spårbar tid för användandet
  – Slutpunkter
- Lagringsskyldigheten ska gälla även vid misslyckad uppringning.
- Lagringsskyldigheten för uppgifter om abonnents och registrerad användares person- och organisationsnummer liksom för uppgifter om datum och spårbar tid då kommunikationen påbörjades och avslutades vid Internettelefoni och datum och spårbar tid för avsändande och mottagande av meddelande vid meddelandehantering följer av direktivet om lagring av trafikuppgifter.

- Lagringsskyldigheten för uppgifter om lokalisering vid mobilsamtals slut och för uppgifter som inte lagras eller loggas vid misslyckad uppringning går utöver direktivet om lagring av trafikuppgifter. Behovet av att dessa uppgifter finns tillgängliga för brottsbekämpningen är så starkt att det överväger det integritetsintrång som lagringen medför och lagringsskyldigheten kan således motiveras utifrån artikel 15.1 i direktivet om integritet och elektronisk kommunikation.

6.2 Vårt uppdrag

Enligt våra direktiv ska vi ta ställning till hur direktivet om lagring av trafikuppgifter ska genomföras i svensk rätt och lämna förslag till de författningsändringar som behövs. En utgångspunkt ska vara att de brottsbekämpande myndigheterna ska få tillgång till de uppgifter som behövs i utredningar om allvarlig brottslighet. Regleringen ska ske med hänsyn till den tekniska utvecklingen inom området för elektronisk kommunikation.

Vissa typer av trafikuppgifter omfattas inte av direktivet om lagring av trafikuppgifter. Vårt uppdrag i den delen är att utifrån artikel 15.1 i direktivet om integritet och elektronisk kommunikation (2002/58/EG) analysera de brottsbekämpande myndigheternas behov av att få tillgång till trafikuppgifter som inte uttryckligen följer av direktivets lagringsskyldighet och utifrån proportionalitetskravet motivera eventuella förslag om ytterligare lagringsskyldighet. Vårt förslag ska emellertid inte omfatta andra trafikuppgifter än sådana som myndigheterna kan ha tillgång till i dag och som avser fast och mobil telefoni, samt Internetåtkomst, e-post och Internettelefoni.

6.3 Uppgifter som omfattas av direktivet om lagring av trafikuppgifter

Artikel 5 i direktivet om lagring av trafikuppgifter anger sex syften för vilka uppgifter ska lagras. Lagringsskyldigheten rör uppgifter som är nödvändiga för att

- spåra och identifiera en kommunikationskälla
- identifiera slutmålet för en kommunikation

- identifiera datum, tidpunkt och varaktighet för en kommunikation
- identifiera typen av kommunikation
- identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt
- identifiera lokaliseringen av mobil kommunikationsutrustning

I anslutning till respektive syfte anges de kategorier av uppgifter som ska lagras (se nedan). I artikel 5 anges också att inga uppgifter som avslöjar kommunikationens innehåll får lagras i enlighet med direktivet.

6.3.1 Uppgifter för spårning och identifiering av kommunikationskälla

Telefoni i fasta nät och mobil telefoni

För telefoni i fasta nät och mobil telefoni anges i artikel 5 att uppgifter om

- det uppringande telefonnumret, och om
- abonnentens eller den registrerade användarens namn och adress

ska lagras.

Internetåtkomst, Internetbaserad e-post och Internettelefoni

För Internetåtkomst, Internetbaserad e-post och Internettelefoni anges i artikel 5 att uppgifter om

- tilldelade användar-ID
- användar-ID och telefonnummer vilka tilldelats kommunikationen i det allmänna telenätet, och om
- namn på och adress till den abonnent eller registrerade användare som IP-adressen (Internet Protocol), användaridentiteten eller telefonnumret tilldelades vid tidpunkten för kommunikationen

ska lagras.

6.3.2 Uppgifter för identifiering av slutmålet för en kommunikation

Telefoni i fasta nät och mobil telefoni

För telefoni i fasta nät och mobil telefoni anges i artikel 5 att uppgifter om

- det eller de nummer som slagits (det eller de uppringda telefonnumren), och, i fall som berör tilläggstjänster såsom omstyrning och överflyttning av samtal, det eller de nummer till vilket eller vilka samtalet styrs, och om
- abonnentens (abonnenternas) eller den eller de registrerade användarnas namn och adress

ska lagras.

Internetbaserad e-post och Internettelefoni

För Internetbaserad e-post och Internettelefoni anges i artikel 5 att uppgifter om

- användar-ID eller telefonnummer som tilldelats den eller de avsedda mottagarna av ett Internettelefonsamtal, och om
- namn på och adress till abonnenten (abonnenterna) eller den eller de registrerade användarna och det användar-ID som tilldelats den avsedda mottagaren av kommunikationen

ska lagras.

6.3.3 Uppgifter för identifiering av datum, tidpunkt och varaktighet för en kommunikation

Telefoni i fasta nät och mobil telefoni

För telefoni i fasta nät och mobil telefoni anges i artikel 5 att uppgifter om

- datum och tid då kommunikationen påbörjades och avslutades

ska lagras.

Internetåtkomst, Internetbaserad e-post och Internettelefoni

För Internetåtkomst, Internetbaserad e-post och Internettelefoni anges i artikel 5 att uppgifter om

- datum och tid för på- respektive avloggning i Internetåtkomsttjänsten inom en given tidszon tillsammans med IP-adressen, oavsett om den är dynamisk eller statisk, som en kommunikation tilldelats av Internetåtkomstleverantören till en kommunikation och abonnents eller registrerad användares användar-ID, och om
- datum och tid för på- respektive avloggning i den Internetbaserade e-posttjänsten eller Internettelefonitjänsten inom en given tidszon

ska lagras.

6.3.4 Uppgifter för identifiering av kommunikationstyp

Telefoni i fasta nät och mobil telefoni

För telefoni i fasta nät och mobil telefoni anges i artikel 5 att uppgifter om

- den telefonitjänst som används

ska lagras.

Internetbaserad e-post och Internettelefoni

För Internetbaserad e-post och Internettelefoni anges i artikel 5 att uppgifter om

- den Internettjänst som används

ska lagras.

6.3.5 Uppgifter för identifiering av kommunikationsutrustning, eller den utrustning som tros ha använts

Telefoni i fasta nät

För telefoni i fasta nät anges i artikel 5 att uppgifter om

- det uppringande och det uppringda telefonnumret

ska lagras.

Mobil telefoni

För mobil telefoni anges i artikel 5 att uppgifter om

- det uppringande och det uppringda telefonnumret,
- den uppringande partens IMSI (International Mobile Subscriber Identity),
- den uppringande partens IMEI (International Mobile Equipment Identity),
- den uppringda partens IMSI,
- den uppringda partens IMEI, och om
- datum och tid för den första aktiveringen av en förbetald anonym tjänst och den lokaliseringsbeteckning (cell-ID) från vilken tjänsten aktiverades

ska lagras.

Internetåtkomst, Internetbaserad e-post och Internettelefoni

För Internetåtkomst, Internetbaserad e-post och Internettelefoni anges i artikel 5 att uppgifter om

- det uppringande telefonnumret för uppringda förbindelser, och om
- DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare

ska lagras.

6.3.6 Uppgifter för lokalisering av mobil kommunikationsutrustning

För lokalisering av mobil kommunikationsutrustning anges i artikel 5 att uppgifter om

- lokaliseringsbeteckning (cell-ID) för kommunikationens början, och
- uppgifter som identifierar cellernas geografiska placering genom referens till deras lokaliseringsbeteckning (cell-ID) under den period som kommunikationsuppgifterna lagras,

ska lagras.

6.4 Lagring av trafikuppgifter som inte omfattas av direktivet

Enligt direktivet om lagring av trafikuppgifter ska vissa angivna uppgifter lagras. Vårt uppdrag är att föreslå en reglering som innebär att dessa uppgifter lagras och som samtidigt innebär att lagringsskyldigheten omfattar de uppgifter som de brottsbekämpande myndigheterna kan ha tillgång till i dag. Det innebär att vi behöver analysera de brottsbekämpande myndigheternas behov av att få tillgång till trafikuppgifter som inte anges i direktivet om lagring av trafikuppgifter och om en vidare lagringsskyldighet kan motiveras utifrån artikel 15.1 i direktivet om integritet och elektronisk kommunikation. Den artikeln har följande lydelse.

Artikel 15
Tillämpningen av vissa bestämmelser i direktiv 95/46/EG

> 1. Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv 95/46/EG. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i denna punkt. Alla åtgärder som avses i denna punkt ska vara i enlighet med de allmänna principerna i gemenskapslagstiftningen, inklusive principerna i artikel 6.1 och 6.2 i Fördraget om Europeiska unionen.

Direktivet om lagring av trafikuppgifter innehåller ett tillägg till artikel 15 på så sätt att en punkt 1a införs. Den nya punkten har följande lydelse.

> 1a. Punkt 1 ska inte tillämpas på uppgifter som specifikt ska lagras enligt 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 (EUT L 105, 13.4.2006, s. 54) för de ändamål som avses i artikel 1.1 i det direktivet.

6.5 Behovet av trafikuppgifter för brottsbekämpningen

Bedömning och förslag: Tillgång till trafikuppgifter är av avgörande betydelse för bekämpning av allvarlig brottslighet.

Lagringsskyldigheten ska genomföras så att den omfattar de uppgifter som de brottsbekämpande myndigheterna kan ha tillgång till i dag.

6.5.1 Antal utlämnanden av trafikuppgifter

Som framgår i avsnitt 2.3 kan de brottsbekämpande myndigheterna få tillgång till historiska trafikuppgifter om de finns tillgängliga hos leverantörerna. Det får ske efter domstolsbeslut om hemlig teleövervakning enligt rättegångsbalken, där det krävs att det finns en person som är skäligen misstänkt för brott med ett minimistraff om sex månaders fängelse eller för viss särskilt angiven brottslighet. Det får också ske utan domstolsbeslut genom att leverantörernas tystnadsplikt för trafikuppgifter enligt lagen om elektronisk kommunikation bryts, vilket kräver att utredningen gäller brott med ett minimistraff som är två års fängelse.

Möjligheten att använda hemlig teleövervakning enligt rättegångsbalken för att få ut historiska trafikuppgifter har funnits sedan den 1 oktober 2004. Av regeringens skrivelse 2006/07:28 Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2005 framgår att 1 027 tillstånd till hemlig teleövervakning meddelades det nämnda året. I skrivelsen anges de brottstyper för vilka tillstånd lämnades. Tillstånd meddelades uteslutande vid grova brott (se avsnitt 11.4). Skrivelsen till riksdagen som rör tvångsmedelsanvändningen för år 2006 har ännu inte lämnats. Av Åklagarmyndighetens och Rikspolisstyrelsens redovisning till regeringen framgår dock att det under året meddelades 1 119 tillstånd till hemlig teleövervakning.

Det förs inte någon statistik över utlämnande av trafikuppgifter enligt lagen om elektronisk kommunikation. BRU lämnade i maj 2005 i sitt betänkande (SOU 2005:38 s. 185) uppgifter om lagens tillämpning. BRU anförde att exakt statistik saknas om i hur många fall per år som de brottsbekämpande myndigheterna begär trafikuppgifter från leverantörerna enligt lagen om elektronisk kommunikation, men enligt en grov uppskattning kunde det röra sig om drygt 4 000 fall årligen. Enligt BRU torde möjligheten att få ut historiska trafikuppgifter enligt lagen om elektronisk kommunikation vara den mest använda metoden när de brottsbekämpande myndigheterna vill få tillgång till sådana trafikuppgifter och det krävs då att utredningen gäller brott vars minimistraff är två års fängelse. För uppgift om abonnemang (t.ex. namn, adress, telefonnummer och IP-adress) krävs dock enbart att fängelse är föreskrivet och att det i det enskilda fallet kan föranleda annan påföljd än böter.

Det finns inte heller nu någon statistik över i hur många fall årligen som de brottsbekämpande myndigheterna begär ut trafikuppgifter enligt lagen om elektronisk kommunikation (”annan uppgift som angår ett särskilt elektroniskt meddelande”). Enligt de nya uppskattningar som polisen har gjort har antalet fall ökat avsevärt från år 2004 och var ca 8 000 under år 2006.

6.5.2 Tidigare överväganden om behovet

BRU konstaterade att trafikuppgifter används på något sätt i nästan samtliga utredningar av grövre brott och bedömde att tillgången till uppgifterna är av fundamental betydelse för utredningsverksamheten och ofta har en direkt koppling till att förundersökningarna över huvud taget kan föras framåt. BRU angav bl.a. följande (s. 323-325).

> Uppgifterna används i princip i *varje* utredning rörande grova brott, som mord, människorov, grovt rån, grov mordbrand, allmänfarlig ödeläggelse (t.ex. bankboxsprängningar), grov våldtäkt, människohandel för sexuella ändamål, grovt barnpornografibrott och grovt narkotikabrott samt brott som faller inom Säkerhetspolisens område, exempelvis terroristbrott.
>
> Arbetet med att utreda brottslighet av den karaktär som nu är aktuell inleds ofta med en kontroll av de trafikuppgifter

som har genererats i anslutning till en brottsplats eller annan plats och sådana uppgifter som kan knytas till en målsägande eller en eventuell misstänkt person. Det krävs många gånger ett relativt omfattande arbete för att få fram vilka av dessa uppgifter som över huvud taget kan vara intressanta i utredningen.

I utredningsarbetet kan polisen på olika sätt ”lägga pussel” med trafikuppgifterna, kanske sammanställda med annan information, t.ex. uppgifter från vittnen och informatörer, och på så sätt få fram vilka personer som kan misstänkas för brottsligheten samt när, var och hur brottet planerades och genomfördes och vad gärningsmännen gjorde därefter. Genom kontakterna och intensiteten i kontakterna mellan särskilda mobiltelefoner, som senare kanske kan knytas till bestämda individer, är det alltså möjligt att klarlägga hur gärningsmännen har agerat och vilka personer som har varit inblandade i brottsligheten. Dessutom kan uppgifterna i många fall resultera i att personer avförs från utredningen genom att misstankarna mot dem visar sig sakna substans.

När det gäller planeringsskedet är det genom tillgång till trafikuppgifter möjligt att ta reda på t.ex. hur gärningsmännen sammanträffade och hur de rekognoserade vid gömställen, längs flyktvägar och vid brottsplatsen samt hur de införskaffade brottsverktyg och stal flyktbilar. Uppgifterna kan som sagt också klarlägga skeenden inte enbart vid själva brottstillfället utan även vid flykten. Det sistnämnda kan bl.a. leda till att gärningsmännens kontakter med varandra blir utredda, att gömställen upptäcks, eventuellt medan gärningsmännen fortfarande befinner sig på platsen, att stulna pengar, flyktbilar eller annat gods påträffas liksom att bortförda personer eller döda kroppar hittas.

I detta sammanhang är det också viktigt att framhålla den brottslighet som på olika sätt kan relateras till Internet. Enligt uppgift från Rikskriminalpolisen är avsaknad av en skäligen misstänkt person det normala utgångsläget i utredningar av Internetrelaterad brottslighet. Möjligheten att uppträda anonymt och t.ex. knyta anonyma kontakter är mycket stor, exempelvis via olika chattjänster. Gärningsmän kan alltså få kontakt med tilltänkta brottsoffer utan att röja sin identitet. Ett sådant tillvägagångssätt har enligt polisen observerats bl.a. i våldtäkts- och mordfall. Ett gott utredningsresultat vid brott där anonyma kontakter har knutits via Internet bygger

till stor del på att polisen får tillgång till historiska trafikuppgifter, eftersom de uppgifterna är det enda som kan länka samman målsäganden och gärningsmannen. Möjligheten att vara anonym på Internet ger också problem vid andra typer av brott, där det i första hand inte är fråga om att knyta samman en målsägande och en gärningsman utan där Internet används som annat verktyg vid brottsligheten. Det har också då mycket stor betydelse att de brottsutredande myndigheterna får tillgång till uppgifter om exempelvis det IP-nummer som var aktuellt vid ett visst tillfälle, för att kunna gå vidare i utredningarna och t.ex. identifiera en skäligen misstänkt person.

Här måste också framhållas att den kraftigt ökade användningen av kryptering gör att betydelsen av tillgång till trafikuppgifter i brottsutredningarna ökar, eftersom krypteringen i princip innebär att de brottsutredande myndigheterna inte kommer åt innehållet i meddelanden genom hemlig teleavlyssning.

Det ska tilläggas att tillgång till trafikuppgifter från operatörer i Sverige är helt nödvändig även i det internationella samarbetet mellan brottsutredande myndigheter.

Det är vår bestämda uppfattning att betydelsen av att de brottsutredande myndigheterna får tillgång till trafikuppgifter i förundersökningar särskilt rörande grövre brott inte kan överskattas. Tillgången till uppgifterna är av fundamental betydelse för brottsutredningsverksamheten och har ofta en direkt koppling till att förundersökningarna över huvud taget kan föras framåt. Det gäller inte minst i de fall där det från början saknas en skäligen misstänkt person.

Det måste poängteras att betydelsen av tillgången till trafikuppgifterna omöjligen kan uppskattas utifrån hur många gånger som uppgifterna åberopas som bevisning i domstol. I de fall tillgången till uppgifterna för utredningen framåt leder de oftast till att andra omständigheter och annan bevisning kan fås fram, vilka i sin tur ligger till grund för åtalet och åberopas i rättegången. Med andra ord är det ofta så att uppgifterna ”sätter polisen på spåret” och utgör en grundläggande vägledning för det vidare utredningsarbetet. Den information som kan fås från beslagtagna datorer eller mobiltelefoner är inte på minsta vis tillräcklig för att täcka det stora behov som finns hos de brottsutredande myndigheterna av tillgång till uppgifterna i nästan samtliga utredningar av grövre brott.

Mot den bakgrunden analyserade BRU de problem som uppkommer med nuvarande ordning som innebär att det inte finns någon skyldighet att lagra trafikuppgifter för brottsbekämpande ändamål. BRU konstaterade att detta många gånger medför stora problem för myndigheterna att få tillgång till de uppgifter som behövs, att det förhållandet i sin tur leder till allvarliga problem med effektiviteten i utredningsarbetet och att konsekvenserna från brottsbekämpningssynpunkt, särskilt vid grövre brottslighet, i längden kan bli oacceptabla (SOU 2005:38 s. 329-330).

6.5.3 Exempel på vad trafikuppgifter kan ge för information

Vi har bett de brottsbekämpande myndigheterna att utifrån verkliga händelser komma med exempel på vilken information trafikuppgifter kan ge i utredningar. Vi sammanfattar exemplen på följande sätt.

Mord: Gärningsmän har identifierats och knutits till varandra och till platser genom trafikuppgifter.

Människorov: En målsägande hölls fängslad under flera dagar och kunde lokaliseras genom trafikuppgifter.

Människohandel: Gärningsmän har identifierats och knutits till varandra och till platser genom trafikuppgifter. Likaså har transportvägar, förfalskningscentraler, platser för prostitution och kontaktnät utomlands klarlagts.

Olaga hot (grovt brott): Vid en fritagning från anstalt med automatvapen gick det att med hjälp av trafikuppgifter lokalisera gärningsmännen.

Dataintrång: Gärningsmän har identifierats och knutits till varandra genom trafikuppgifter.

Våldtäkt: Gärningsmän har identifierats genom trafikuppgifter. Exempelvis kunde en underårig målsägande ange att gärningsmannen under övergreppet, som skedde i bil, hade fått två samtal till sin mobiltelefon utan att besvara dessa. Genom de uppgifterna blev det möjligt att identifiera gärningsmannen, som också kunde bindas till andra liknande brott några år tidigare.

Grov stöld: Genom trafikuppgifter kunde en stöld av en container med cigaretter klaras upp genom att kontakterna mellan fem gärningsmän blev klarlagda. Brottet var först rubricerat som rån men trafikuppgifterna gjorde klart att det var ett ”insiderjobb”.

Grov stöld/grovt häleri: Trafikuppgifter från en misstänkts telefon ledde till att ett nätverk av personer som utförde inbrott ”på

beställning” kunde identifieras. Dessutom kunde ”hälericentralen” lokaliseras.

Grovt rån: Gärningsmän har identifierats och knutits till varandra och till platser genom trafikuppgifter.

Utpressning (grovt brott): Vid utredning av annat brott kunde det genom trafikuppgifter klarläggas att det pågick en utpressning, som inte var anmäld till polisen. Gärningsmannen kunde identifieras. I ett annat fall kunde gärningsmännen identifieras genom trafikuppgifter som tillkommit i samband med överlämnandet av pengar.

Mordbrand: Vid mordbränder mot flera restauranger har gärningsmän identifierats och knutits till varandra och till platser genom trafikuppgifter.

Grovt narkotikabrott: Gärningsmän har identifierats och knutits till varandra och till platser (t.ex. gömställen) genom trafikuppgifter.

Grov narkotikasmuggling: Genom trafikuppgifter kunde tullen binda telefoner till misstänkta personer och se hur dessa hade rört sig, vilka de haft kontakt med och när kommunikationen ägt rum. Uppgifterna kunde användas för att få hemlig teleavlyssning, som i sin tur användes framgångsrikt för att identifiera misstänkta personer, smugglingsvägar och tidpunkter för smugglingar. Trafikuppgifterna var också avgörande i det internationella samarbetet. – Genom trafikuppgifter rörande ett s.k. anonymt kontantkort, som användes för att ringa till en kurirs telefon, kunde sex gärningsmän och ett gömställe identifieras. Dessutom kunde nästa smugglingsparti tas i beslag och tidigare smugglingsresor klarläggas. – Vid en smugglingsresa kunde inte bara kuriren utan även personer i en följebil knytas till smugglingen med hjälp av trafikuppgifter.

Grovt skattebrott m.m.: Gärningsmän har identifierats och knutits till varandra och till platser. Följande typexempel kan nämnas vid grovt skattebrott och grova förmögenhetsbrott. En huvudman som inte vill synas utåt beordrar vissa personer att göra olika saker. Tillgången till trafikuppgifter leder till att man kan visa att huvudmannens telefon vid vissa tidpunkter haft kontakt med någon annan misstänkts telefon. Utifrån flera sådana uppgifter kan man sedan se mönster om att kontakt funnits vid intressanta tidpunkter, t.ex. vid penninguttag. Uppgifterna kan indikera att den annars osynlige huvudmannen är den som styr aktiviteten. Ett flertal samtal, som varar längre än försumbar tid, kan inte förklaras som felringningar. Det kan också vara värdefullt att få tillgång till lokaliseringsinformation för att t.ex. visa att personer träffats. Ofta kan

den sortens information kombineras med fysisk spaning. Uppgifterna kan användas för att försöka påvisa att personer som påstår sig ha haft kontakt med varandra i vart fall inte har haft kontakt som visar sig genom trafikuppgifter. Trafikuppgifter visar också det motsatta, att personer har varit i kontakt med varandra och när det skedde.

6.5.4 Vår bedömning

Behovet av att använda trafikuppgifter vid utredning av allvarlig brottslighet har sin grund i medborgarnas anspråk på en effektiv brottsbekämpning. Människor måste kunna ha tillit till att brottsbekämpningen leder till att allvarliga brott klaras upp och till att den som begått ett allvarligt brott kan åtalas och dömas.

När medel, verktyg och metoder som behövs för en effektiv brottsbekämpning diskuteras hänvisas det ofta till polisens eller de andra brottsbekämpande myndigheternas behov. Det är också dessa myndigheter som har djupa insikter om vad som behövs i brottsbekämpningen och som preciserar behovet. Utgångspunkten för bedömningen av vilka nya medel, verktyg eller metoder som behövs i brottsbekämpningen måste dock vara medborgarnas behov. Det är medborgarna i allmänhet och brottsoffren som för sin trygghet respektive upprättelse ställer anspråk på en effektiv brottsbekämpning.

Behovet av att allvarlig brottslighet utreds och lagförs måste ställas mot medborgarnas grundläggande krav på integritet och skydd mot integritetsintrång. Den rättsliga regleringen på tvångsmedelsområdet speglar den avvägning som lagstiftaren har gjort mellan dessa båda medborgarintressen. I avsnitt 5 har vi redovisat de utgångspunkter som bör gälla för att kravet på ett gott integritetsskydd ska tillgodoses vid genomförandet av direktivet om lagring av trafikuppgifter.

Vi ska utifrån direktivet om lagring av trafikuppgifter föreslå en reglering som innebär att trafikuppgifter lagras just för att kunna användas vid bekämpning av allvarlig brottslighet. Hittills har de brottsbekämpande myndigheterna kunnat få trafikuppgifter om de har funnits tillgängliga hos leverantörerna. Det nuvarande regelsystemet innebär att trafikuppgifter får sparas endast om det finns skäl för det främst utifrån förhållandet mellan leverantören och dennes abonnenter eller kunder. Direktivet innebär att de uppgifter som leverantörerna lagrar i dag ska kompletteras med uppgifter

som lagras för brottsbekämpande syften och att det kommer att finnas en bestämd tidsram för hur länge uppgifterna ska lagras.

En närmast självklar utgångspunkt för bedömningen av vilket behov det finns av trafikuppgifter för brottsbekämpningen måste vara det förhållandet att trafikuppgifter sedan mycket lång tid används och är helt avgörande i de brottsbekämpande myndigheternas arbete. Trafikuppgifterna leder bl.a. till att oklara förhållanden kan redas ut, till att samband mellan olika personer kan klargöras, till att personer kan knytas till platser som är viktiga för utredningen av brottet, till ett säkrare underlag i förundersökning och vid åtal och till att utredningen kan inriktas på det som är intressant och snabbt avföra både misstankar och misstänkta som inte ska omfattas av utredningen. De exempel på situationer där trafikuppgifter har använts vid utredning om allvarliga brott visar enligt vår mening att tillgången till trafikuppgifter är ett nödvändigt och träffsäkert verktyg vid utredningar av allvarlig brottslighet.

Teknikutvecklingen och internationaliseringen innebär hela tiden nya möjligheter för dem som begår brott. Brotten kan planeras och utföras mer anonymt och utan direkt kontakt mellan dem som är inblandade. Tekniken och internationaliseringen utnyttjas också för att dölja brotten och försvåra upptäckt. Olika slags lösningar för elektronisk kommunikation kan därmed användas direkt som ett brottsverktyg och som en del i brottsplanen.

Möjligheten att lagra trafikuppgifter innebär att de ”elektroniska spår” som finns i samband med brottet kan användas för att på ett konkret och rättssäkert sätt föra utredningen om brottet framåt. För de flesta medborgare torde det te sig naturligt att den teknik som kan spåras i samband med att ett allvarligt brott har begåtts också används för att utreda brottet.

BRU gjorde den generella bedömningen att tillgången till trafikuppgifter är av fundamental betydelse för brottsutredningsverksamheten och att tillgången ofta har en direkt koppling till att förundersökningarna över huvud taget kan föras framåt. Vi instämmer i den slutsatsen. I de allra flesta fall finns inte några godtagbara alternativa metoder att använda. Fysisk spaning och ”öppna” tvångsmedel som husrannsakan kan i vissa lägen vara ett gott komplement till den information som trafikuppgifter kan ge, men många gånger är sådana metoder av både praktiska och utredningsmässiga skäl inte möjliga att genomföra. För att de brottsbekämpande myndigheterna ska kunna fullgöra sitt uppdrag måste de alltså få tillgång till de trafikuppgifter som anges i direktivet.

De brottsbekämpande myndigheterna har dessutom anfört att det finns behov av att fler trafikuppgifter än de som anges i direktivet lagras. Ett genomförande av direktivet får inte leda till att de brottsbekämpande myndigheterna får sämre förutsättningar än i dag att bekämpa allvarlig brottslighet. Vår utgångspunkt är att lagringsskyldigheten enligt direktivet ska genomföras så att den omfattar de trafikuppgifter som de brottsbekämpande myndigheterna kan ha tillgång till i dag och som avser fast och mobil telefoni, samt Internetåtkomst, e-post och Internettelefoni. Vi återkommer till frågan om de brottsbekämpande myndigheternas ytterligare behov i avsnitt 6.8.2, 6.13 och 6.14.

6.6 Hur bör lagringsskyldigheten struktureras?

6.6.1 Utgångspunkter

Förslag och bedömning: Regleringen ska vara tydlig och väl avgränsad och utformad så att den så långt det är möjligt blir oberoende av den tekniska utvecklingen.

Lagringsskyldigheten innebär inte en uttömmande uppräkning av vilka uppgifter som de brottsbekämpande myndigheterna har rätt att få från leverantörerna.

Den enskilde leverantörens lagringsskyldighet ska enbart omfatta uppgifter som denne någon gång genererar eller behandlar.

De uppgifter som ska lagras får inte avslöja kommunikationens innehåll.

Teknikneutrala och tydliga regler

När direktivet om lagring av trafikuppgifter ska genomföras i svensk rätt hade den enklaste lösningen varit att utforma författningstexten i mycket nära anslutning till skrivningarna i direktivet. Samtidigt kan en sådan lösning medföra problem på sikt. Mot bakgrund av den snabba teknikutvecklingen måste direktivet tolkas. Vi kan redan i dag konstatera att vissa av de uttryck som används, t.ex. IMSI och IMEI, kommer att vara föråldrade ganska snart. Direktivets uttryck om att det specifikt ska vara de uppgifter som anges i direktivet som ska omfattas av lagringsskyldighet (jfr artikel 11 i direktivet om lagring av trafikuppgifter som innebär en ändring av artikel 15 i direktivet om integritet och elektronisk kommunika-

tion) bör därför förstås så att lagringsskyldigheten ska omfatta de olika typer av uppgifter som framgår av artikel 5.

Utgångspunkten enligt våra direktiv är att de föreslagna bestämmelserna så långt det är möjligt ska vara oberoende av den tekniska utvecklingen, samtidigt som vi ska beakta behovet av tydliga och väl avgränsade regler. I det följande lämnar vi förslag till hur en mer teknikneutral lösning bör utformas.

Författningsgivning som reglerar integritetskänsliga uppgifter brukar ske genom lag (jfr prop. 1990/91:60 s. 50 och 1997/98:44 s. 41). Det är också med den utgångspunkten som det nuvarande regelsystemet kring trafikuppgifter är utformat.

Rättegångsbalken och lagen om elektronisk kommunikation reglerar inte i detalj vilka uppgifter som de brottsbekämpande myndigheterna har rätt att få ut, annat än att det ska vara fråga om ”uppgift om telemeddelanden” respektive ”uppgift som angår ett särskilt elektroniskt meddelande”. Regleringarna är med andra ord teknikneutrala och anger inte i detalj vilka typer av uppgifter det är fråga om. På samma vis innehåller varken lagen om elektronisk kommunikation, förordningen med samma namn eller föreskrifter från PTS någon uppräkning i detalj av vilka typer av uppgifter som leverantörerna får spara för exempelvis abonnentfakturering (6 kap. 6 § LEK och 35 § nämnda förordning).

För att en tydlig reglering som är så teknikneutral som möjligt ska åstadkommas blir det nödvändigt att ha bestämmelser som rör lagringsskyldigheten i olika avseenden både i lag, förordning och myndighetsföreskrifter. I lag ska bl.a. de bestämmelser finnas som ger åligganden för enskilda (8 kap. 3 § regeringsformen). Som vi utvecklar senare i betänkandet rör det bl.a. skyldigheten för leverantörer att lagra trafikuppgifter för brottsbekämpande syften och leverantörernas skyldighet att lagra uppgifterna på ett säkert sätt. Detaljregleringen och den mer tekniska beskrivningen av vilka trafikuppgifter som ska lagras behöver inte finnas i lag. Det blir en mer lämplig och teknikneutral reglering som står sig över tid om det i lag tas in en bestämmelse om att regeringen i förordning reglerar den mer tekniska beskrivningen av lagringsskyldigheten. Förordningen om elektronisk kommunikation reglerar i stort sett enbart PTS verksamhet som tillsynsmyndighet. Vi bedömer att bestämmelser som preciserar vilka trafikuppgifter som ska lagras inte passar i den förordningen. I stället föreslår vi en särskild förordning om lagring av trafikuppgifter m.m. för brottsbekämpande syften. Den reglering som innebär en mycket hög detaljnivå, t.ex. rörande

de säkerhetsåtgärder som leverantörerna ska vidta för att skydda uppgifterna, bör ske i föreskrifter från tillsynsmyndigheten.

Uppgifter som genereras eller behandlas ska lagras

I artikel 3 i direktivet om lagring av trafikuppgifter anges att det enbart är de trafikuppgifter som den enskilde leverantören genererar eller behandlar som omfattas av lagringsskyldigheten. Leverantören kommer alltså inte att ha skyldighet att ”skaffa sig” alla de uppgifter lagringsskyldigheten omfattar utan lagringsskyldigheten för leverantören omfattar endast de trafikuppgifter som genereras eller behandlas i verksamheten. Direktivet innebär därmed inget hinder mot exempelvis anonyma kontantkort. Finns däremot uppgifterna någon gång hos leverantören och genereras eller behandlas, även om det bara rör sig om en ytterst kort tid, ska de lagras. Detta gäller oavsett om uppgifterna lagras redan i dag av leverantören eller inte.

De uppgifter som lagringsskyldigheten omfattar enligt direktivet om lagring av trafikuppgifter får inte avslöja kommunikationens innehåll (artikel 5). De förslag till lagring av trafikuppgifter som vi föreslår utgår från detta.

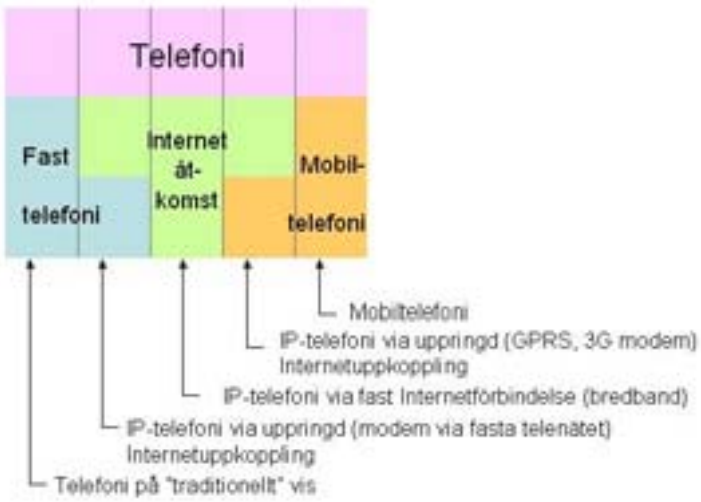
6.6.2 Strukturen

Förslag: Lagringsskyldigheten ska struktureras i kategorierna telefoni, meddelandehantering, Internetåtkomst och anslutningsform.

Tydligheten i regleringen är viktig för att medborgarna i så hög utsträckning som möjligt ska kunna förstå vad lagringsskyldigheten omfattar och för att de berörda aktörerna ska förstå vad som faller in under regleringen och därmed kunna fullgöra sina skyldigheter. En klart och tydligt avgränsad reglering ser vi som en av de faktorer som bidrar till ett gott integritetsskydd och till att upprätthålla god konkurrens och skapa ett gott innovationsklimat och en mångfald på marknaden.

Mot bakgrund av teknikutvecklingen, där olika sektorer gradvis växer samman (konvergensen), överskådligheten och förståelsen (inte minst från berörda aktörer) har vi valt att arbeta efter en författningsmässig lösning där de olika teknikområdena är uppdelade på ett mer teknikneutralt och framtidsorienterat sätt än vad som

följer direkt av direktivet om lagring av trafikuppgifter. Direktivet utgår från att de olika områdena har ett ”vertikalt” förhållande till varandra, exempelvis så skiljs fast, mobil och Internettelefoni åt. I den tekniska realiteten är många lösningar i dagsläget kombinationer. Som exempel kan nämnas att en fast telefon eller en mobiltelefon kan användas för Internetåtkomst med vars hjälp Internettelefoni kan användas. Utan att gå in på tekniska detaljer är ett annat exempel att ett och samma samtal kan gå från en mobiltelefon till en fast telefon och transitering (trunking) kan ske med hjälp av Internettelefoni mellan mobilnätet och det fasta telenätet. För att åskådliggöra något av komplexiteten kan följande bild avseende telefoni användas.



Ett sätt att få en så teknikneutral reglering som möjligt som låter regleringen bättre avspegla hur systemen rent faktiskt fungerar, är att anlägga ett mer ”horisontellt” synsätt vid tolkningen och genomförandet av direktivet. Därmed kan det skapas en struktur som bättre kommer att stå sig över tiden. Exempelvis kommer nya kommunikationstjänster att kunna omfattas av författningstexten på ett mycket mer tydligt sätt. De förändringar i regelverket som kan komma att krävas i framtiden blir med vår lösning mer begränsade än vad de annars hade blivit.

Vårt sätt att strukturera de uppgifter som ska lagras utgår från följande uppdelning i författningstexten.

1. Telefoni
2. Meddelandehantering
3. Internetåtkomst
4. Anslutningsform

6.6.3 Telefoni

Begreppet telefonitjänst definieras i 1 kap. 7 § LEK som en elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan, inklusive nödsamtal. Samtal definieras i samma bestämmelse som förbindelse för överföring av tal som medger tvåvägskommunikation i vad som för användaren uppfattas som realtid.

Många Internettelefonitjänster medger inte alltid att nödsamtal genomförs. Den definition av telefonitjänst som används i lagen om elektronisk kommunikation blir därför för snäv för att kunna användas i detta sammanhang. Telefoni enligt vårt förslag bör därför definieras som i 1 kap. 7 § LEK men utan kravet att nödsamtal ska kunna genomföras.

I artikel 2 i direktivet om lagring av trafikuppgifter definieras telefonitjänst som uppringning (inbegripet rösttelefoni, röstmeddelanden, konferenssamtal och datatelefoni), extratjänster (inbegripet omstyrning och överflyttning av samtal) och meddelandeförmedling och multimedietjänster (inbegripet SMS, EMS och multimedietjänster).

Vid telefoni finns en uppringande och en uppringd part som kan anges med olika typer av ”adresser”, t.ex. användar-ID eller s.k. E.164-nummer (”vanligt telefonnummer”).

PTS beskriver telefoninummerplanen och dess principer på följande sätt.

> Telefoninummerplan specificerar formatet och strukturen på de nummerserier som används i planen. Dessa nummerserier är uppdelade i grupper, främst genom nationella destinationskoder (NDC), för att kunna identifiera specifika delar som används för identifikation, dirigering och debiteringsändamål för att identifiera abonnenter, användare och tjänster.

Telefoninummerplanen innehåller inte prefix, suffix eller annan extra information som behövs för att fullfölja en samtalsuppkoppling. Sådan information, såsom internationellt prefix 00, nationellt prefix 0 och operatörsprefix 95XX, ingår i nummertagningsplanen som anger hur nummerplanen används.

Ur nummerplanens nummerserier tilldelar PTS antingen enskilda nummer (inom 11X-serien) eller nummerblock till främst operatörer och tjänsteleverantörer genom utfärdande av tillstånd.

Majoriteten av numren i telefoninummerplanen är s.k. E.164-nummer som därmed är nåbara från andra länder genom internationell nummertagning och med en nummerlängd om maximalt 15 siffror i det internationella formatet. Utöver dessa E.164-nummer innehåller även den nationella telefoninummerplanen, som är den nationella implementeringen av den internationella E.164-nummerplanen, andra nationella telefonnummer som inte är nåbara från andra länder och här avses främst korta servicenummer i 11X-serien.

Sverige tillämpar en öppen plan med nationellt prefix 0. En öppen plan innebär att landet är indelat i olika geografiska områden, riktnummerområden, inom vilka det är möjligt att slå endast abonnentnumret. En nummerplan där det fullständiga telefonnumret inklusive riktnummer måste slås, kallas sluten plan.

Tre grundläggande principer gäller för den svenska nummerplanens struktur och hantering:

Alla nummerserier ska vara öppna och kunna nås från alla elektroniska kommunikationsnät.

Det ska vara möjligt med nummerportabilitet mellan tjänsteleverantörer.

Det ska i nummerhänseende vara möjligt att nå sådana nät och tjänster hos olika tjänsteleverantörer på likvärdigt sätt.

Telefoni enligt vårt förslag ska omfatta fall där E.164-nummer används, dvs. nummer ur en telefoninummerplan. Definitionen av telefoni inkluderar därmed fast och mobil telefoni och de flesta Internettelefonitjänster. Internettelefoni som använder andra ”adresser” som identifiering kommer inte att omfattas. En konsekvens av vår tolkning kan bli att en del kommunikationstjänster för överföring av tal i realtid inte kommer att falla under lagringsskyldighe-

ten. Med telefoni avses inte kommunikation som omfattas av begreppet meddelandehantering (se avsnitt 6.10).

Som framgår i det följande har vi för telefoni utformat en generell del som gäller för fast, mobil och Internettelefoni. Utöver denna del behöver det särskilt anges att vissa uppgifter är specifika för mobil respektive Internettelefoni.

6.6.4 Meddelandehantering

Vi har valt att använda begreppet meddelandehantering för att beskriva överföring av elektroniskt meddelande som främst SMS, MMS och elektronisk post. Det är alltså tjänster som framför allt använder protokoll som SMTP (Simple Mail Transfer Protocol, RFC 2821 och RFC 2822, IETF) och SMPP (Short Message Peer v5.0, SMS Forum). Det förhållandet att det i dag är möjligt att skicka SMS såväl från en mobil som en fast telefon och via elektronisk post tydliggör att den horisontella struktur vi har valt är att föredra framför den vertikala som finns i direktivet om lagring av trafikuppgifter.

6.6.5 Internetåtkomst

Internetåtkomst avser möjligheten att överföra s.k. IP-paket med hjälp av olika tekniker (anslutningsform) och ger användaren åtkomst till Internet. I praktiken innebär detta att användaren tilldelas en eller flera IP-adresser för kommunikation. IP-adresserna kan vara fasta eller dynamiska (DHCP).

6.6.6 Anslutningsform

Den kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst har vi valt att beteckna anslutningsform. Exempel på anslutningsform är DSL (vilket i sin tur kan ske med hjälp av leverantörer av t.ex. bitströmsaccess), fiberoptiska anslutningar, 3G (UMTS), GSM (GPRS), vanliga traditionella telefonmodem och WLAN (trådlöst nät).

6.7 Vilka uppgifter ska lagras vid telefoni?

Förslag: Vid telefoni ska följande uppgifter lagras:
– Uppringande telefonnummer
– Nummer som slagits och nummer till vilka samtalet styrts
– Uppgifter om abonnent och registrerad användare
– Datum och spårbar tid då kommunikationen påbörjades och avslutades
– Den tjänst som använts
– Slutpunkter

6.7.1 Uppringande telefonnummer

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- det uppringande telefonnumret
- tilldelade användar-ID
- användar-ID och telefonnummer vilka tilldelats kommunikationen i det allmänna telenätet

Uppgifter om uppringande telefonnummer är nödvändiga för att spåra och identifiera en kommunikationskälla och för att identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

6.7.2 Nummer som slagits och nummer till vilka samtalet styrts

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- det eller de nummer som slagits (det eller de uppringda telefonnumren), och, i fall som berör tilläggstjänster såsom omstyrning och överflyttning av samtal, det eller de nummer till vilket eller vilka samtalet styrs
- användar-ID eller telefonnummer som tilldelats den eller de avsedda mottagarna av ett Internettelefonsamtal
- uppringda telefonnummer

Uppgifter om nummer som slagits och nummer till vilka samtalet styrts är nödvändiga för att identifiera slutmålet för en kommuni-

kation och för att identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

6.7.3 Uppgifter om abonnent och registrerad användare

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- abonnentens eller den registrerade användarens namn och adress
- namn på och adress till den abonnent eller registrerade användare som IP-adressen (Internet Protocol), användaridentiteten eller telefonnumret tilldelades vid tidpunkten för kommunikationen
- abonnentens (abonnenternas) eller den eller de registrerade användarnas namn och adress
- namn på och adress till abonnenten (abonnenterna) eller den eller de registrerade användarna och det användar-ID som tilldelats den avsedda mottagaren av kommunikationen

Uppgifter om abonnent eller registrerad användare är nödvändiga för att spåra och identifiera en kommunikationskälla och för att identifiera slutmålet för en kommunikation.

Namn och adress är inte unika begrepp för att identifiera en viss person eller organisation. Mot den bakgrunden och med tanke på att leverantörerna ibland använder andra begrepp för att registrera kunder och användare, ska lagringsskyldigheten innefatta inte enbart namn och adress utan även person- och organisationsnummer, vilket är uppgifter som i vårt land används för att säkert identifiera någon. Vi ser inte detta som en lagringsskyldighet utöver direktivet om lagring av trafikuppgifter (se vidare avsnitt 6.14).

Det kan nämnas att uppgift om personnummer får behandlas utan samtycke bara när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl (22 § PUL). Den bestämmelsen hindrar enligt vår bedömning inte att lagringsskyldigheten avser även person- eller organisationsnummer.

6.7.4 Datum och spårbar tid då kommunikationen påbörjades och avslutades

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- datum och tid då kommunikationen påbörjades och avslutades
- datum och tid för på- respektive avloggning i den Internetbaserade e-posttjänsten eller Internettelefonitjänsten inom en given tidszon

Uppgifter om datum och spårbar tid då kommunikationen påbörjades och avslutades är nödvändiga för att identifiera datum, tidpunkt och varaktighet för en kommunikation.

Som nyss nämndes anger direktivet om lagring av trafikuppgifter att syftet med att lagra dessa uppgifter är att identifiera datum, tidpunkt och varaktighet för en *kommunikation*. För telefoni i fasta nät och för mobil telefoni anger direktivet att för det syftet ska uppgift om datum och tid då kommunikationen påbörjades och avslutades lagras (se den första citerade punkten ovan). För Internettelefoni anger direktivet att uppgift om på- och avloggningstidpunkter ska lagras. Det är möjligt att vara ”påloggad” under mycket långa tidsperioder. På- och avloggning innebär alltså inte nödvändigtvis start- och slutpunkt för en kommunikation. Syftet med direktivet är att säkerställa att de brottsbekämpande myndigheterna kan få tillgång till trafikuppgifter av betydelse för utredningsarbetet. Det är orimligt att tänka sig att på- och avloggningstidpunkterna, mellan vilka det kan förflyta år, skulle vara av sådan vikt för det arbetet att det är dessa tidpunkter som avses i direktivet och inte de tidpunkter som på ett mycket mer direkt sätt kan knytas till en persons handlingar, dvs. tidpunkterna för själva kommunikationen. Mot den bakgrunden bör direktivets uttryck att det är uppgifter om kommunikationen som ska lagras tolkas så att det är själva kommunikationens början och slut som avses även vid Internettelefoni (se vidare avsnitt 6.14).

6.7.5 Den tjänst som använts

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- den telefonitjänst som används
- den Internettjänst som används

Uppgifter om den tjänst som använts är nödvändiga för att identifiera typen av kommunikation.

I artikel 2 i direktivet om lagring av trafikuppgifter definieras telefonitjänst som uppringning (inbegripet rösttelefoni, röstmeddelanden, konferenssamtal och datatelefoni), extratjänster (inbegripet omstyrning och överflyttning av samtal) och meddelandeförmedling och multimedietjänster (inbegripet SMS, EMS och multimedietjänster). Någon motsvarande definition av begreppet Internettjänst finns inte i direktivet.

Vårt sätt att strukturera lagringsskyldigheten innebär att under den här aktuella rubriken faller den del av telefonitjänst som inte avser meddelandehantering.

Med tjänst avses t.ex. röstbrevlåda, vidarekoppling och/eller omstyrning.

6.7.6 Slutpunkter

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- det uppringande telefonnumret för uppringda förbindelser
- DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare

Uppgifter om slutpunkter är nödvändiga för att identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

Med slutpunkt avses den tekniska utrustningen i en fysisk ändpunkt som står under leverantörens kontroll, såsom telefonväxlar, routers, portnummer, utrustningsidentitet, MAC-adresser och abonnemangsidentitet.

6.8 Vilka ytterligare uppgifter ska lagras vid mobil telefoni?

Förslag: Vid mobil telefoni ska dessutom följande uppgifter lagras:
– Den uppringande och den uppringda partens abonnemangsidentitet och utrustningsidentitet
– Lokaliseringsinformation för kommunikationens början och slut
– Datum, spårbar tid och lokaliseringsinformation för den första aktiveringen av en förbetald anonym tjänst
Bedömning: En lagringsskyldighet för lokaliseringsinformation avseende kommunikationens slut går utöver direktivet om lagring av trafikuppgifter men kan motiveras utifrån en avvägning mellan brottsbekämpningsintresset och integritetsskyddet enligt direktivet om integritet och elektronisk kommunikation.

6.8.1 Den uppringande och den uppringda partens abonnemangsidentitet och utrustningsidentitet

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- den uppringande partens IMSI (International Mobile Subscriber Identity)
- den uppringande partens IMEI (International Mobile Equipment Identity)
- den uppringda partens IMSI
- den uppringda partens IMEI

Uppgifter om den uppringande och den uppringda partens abonnemangsidentitet och utrustningsidentitet är nödvändiga för att identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

IMSI och IMEI är alltför tekniska begrepp för att kunna stå sig över tiden. De begrepp som i stället används är abonnemangsidentitet och utrustningsidentitet.

6.8.2 Lokaliseringsinformation för kommunikationens början och slut

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- lokaliseringsbeteckning (cell-ID) för kommunikationens början
- uppgifter som identifierar cellernas geografiska placering genom referens till deras lokaliseringsbeteckning (cell-ID) under den period som kommunikationsuppgifterna lagras

Lokaliseringsinformation är enligt vår mening ett bättre uttryck än direktivets lokaliseringsbeteckning. Uppgifter om lokaliseringsinformation för kommunikationens början är nödvändiga för att identifiera lokaliseringen av mobil kommunikationsutrustning.

En mobiltelefon har regelbundet kontakt med kommunikationsnätet även när telefonen enbart är påslagen utan att något samtal äger rum. Även under sådana omständigheter genereras således lokaliseringsinformation. De uppgifterna omfattas dock inte av direktivet om lagring av trafikuppgifter. När en mobiltelefon används för åtkomst till Internet kallas anslutningsformen UMTS eller GPRS för 3G respektive GSM. I sådana fall ska lokaliseringsinformation lagras enligt vad som följer av avsnitt 6.11.5 eller 6.12.2.

Av direktivet följer alltså att lokaliseringsinformation för kommunikationens *början* ska lagras.

De brottsbekämpande myndigheterna har anfört att de också har behov av att få lokaliseringsinformation avseende kommunikationens *slut*. Införandet av en skyldighet att lagra lokaliseringsinformation avseende kommunikationens slut förutsätter att det finns ett behov av uppgifterna för brottsbekämpningsändamål och att lagringsskyldigheten bedöms vara en nödvändig åtgärd enligt de överväganden som ska göras enligt artikel 15.1 i direktivet om integritet och elektronisk kommunikation.

Mobiltelefoner används ofta i samband med brott, både före, under och efter gärningen. Ett exempel är grova rån där mobiltelefoner används som sambandsutrustning under transporten fram till den plats där brottet ska begås, under själva brottets utförande och under flykten från brottsplatsen. Att de brottsbekämpande myndigheterna i sådana sammanhang enbart ska kunna få uppgifter om var mobiltelefonen funnits inledningsvis innebär enligt myndighe-

terna en klar begränsning i det brottsbekämpande arbetet. Det borde enligt myndigheterna finnas en lagringsskyldighet för lokaliseringsuppgifter inte bara för kommunikationens början utan också för dess *slut* och för *pågående kommunikation* en gång per minut.

Vi kan konstatera att lokaliseringsinformation för kommunikationens början många gånger inte alls är tillräckligt för de brottsbekämpande syftena. Det framstår som självklart att också lokaliseringsinformation för kommunikationens slut är nödvändig. I annat fall skulle det vara för enkelt att i en kriminell verksamhet vilseleda myndigheterna med klart negativa följder för utredningsarbetet. Detta har också beaktats i exempelvis den danska regleringen, som föreskriver lagringsskyldighet för lokaliseringsuppgifter även rörande kommunikationens slut. Vi anser att lagringen är motiverad och proportionerlig och föreslår en sådan lagringsskyldighet även för kommunikationens slut.

De brottsbekämpande myndigheterna har också framfört ett behov av lokaliseringsinformation för pågående kommunikation, eftersom en gärningsman mycket väl kan ha påbörjat och avslutat kommunikationen på andra platser än brottsplatsen. Vill man som brottsling försvåra utredningsarbetet vore det enkelt att påbörja ett samtal på en plats och låta det samtalet pågå, kanske under avsevärd tid, under det att man förflyttar sig och på så sätt undviker att lämna efter sig lokaliseringsinformation, t.ex. rörande rån och smugglingsresor med narkotika.

Om lagring skulle genomföras för uppgifter om pågående kommunikation skulle det i princip innebära att alla mobilanvändares rörelser under pågående samtal skulle lagras med jämna mellanrum, t.ex. varje minut eller en gång i timmen. Det torde av de flesta uppfattas som ett stort intrång i den personliga integriteten. Det skulle också föra med sig stora lagringsvolymer och kostnader. Även om vi delar uppfattningen att informationen skulle vara mycket värdefull från brottsbekämpningssynpunkt anser vi att det behovet inte uppväger det integritetsintrång som uppkommer om lokaliseringsinformation skulle lagras för pågående kommunikation och inte ens om den informationen begränsades till lokalisering en gång i timmen. Vi föreslår därför inte någon lagringsskyldighet för lokaliseringsinformation under pågående kommunikation.

6.8.3 Datum, spårbar tid och lokaliseringsinformation för den första aktiveringen av en förbetald anonym tjänst

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- vid förbetalda anonyma tjänster, datum och tid för den första aktiveringen av tjänsten och den lokaliseringsbeteckning (cell-ID) från vilken tjänsten aktiverades

Uppgifter om datum, spårbar tid och lokaliseringsinformation för den första aktiveringen av en förbetald anonym tjänst är nödvändiga för att identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

Som anges i avsnitt 6.8.2 är lokaliseringsinformation ett bättre uttryck att använda än direktivets lokaliseringsbeteckning.

6.9 Vilka ytterligare uppgifter ska lagras vid Internettelefoni?

Förslag: Vid Internettelefoni ska dessutom följande uppgifter lagras:
– Uppringande parts IP-adresser
– Uppringd parts IP-adresser

6.9.1 Uppringande och uppringd parts IP-adresser

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- tilldelade användar-ID
- namn på och adress till den abonnent eller registrerade användare som IP-adressen (Internet Protocol), användaridentiteten eller telefonnumret tilldelades vid tidpunkten för kommunikationen
- användar-ID eller telefonnummer som tilldelats den eller de avsedda mottagarna av ett Internettelefonsamtal
- datum och tid för på- respektive avloggning i Internetåtkomsttjänsten inom en given tidszon tillsammans med IP-adressen, oavsett om den är dynamisk eller statisk, som en kommunikation tilldelats av Internetåtkomstle-

verantören till en kommunikation och abonnents eller registrerad användares användar-ID

Uppgifter om uppringande och uppringd parts IP-adresser är nödvändiga för att spåra och identifiera en kommunikationskälla och slutmålet för en kommunikation (avsedd mottagare) samt för att identifiera datum, tidpunkt och varaktighet för en kommunikation.

6.10 Vilka uppgifter ska lagras vid meddelandehantering?

Förslag: Vid meddelandehantering ska följande uppgifter lagras:
– Avsändarens och mottagarens meddelandeadress
– Uppgifter om abonnent och registrerad användare
– Datum och spårbar tid för på- och avloggning i meddelandetjänsten
– Datum och spårbar tid för avsändande och mottagande av meddelandet
– Den tjänst som har använts och spårbar tid för användandet

6.10.1 Avsändarens och mottagarens meddelandeadress

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- tilldelade användar-ID
- namn på och adress till den abonnent eller registrerade användare som IP-adressen (Internet Protocol), användaridentiteten eller telefonnumret tilldelades vid tidpunkten för kommunikationen
- användar-ID eller telefonnummer som tilldelats den eller de avsedda mottagarna av ett Internettelefonsamtal.
- namn på och adress till abonnenten (abonnenterna) eller den eller de registrerade användarna och det användar-ID som tilldelats den avsedda mottagaren av kommunikationen

Uppgifter om avsändarens och mottagarens meddelandeadress (t.ex. e-postadresser och telefonnummer) är nödvändiga för att spåra och identifiera en kommunikationskälla och för att identifiera slutmålet för en kommunikation.

6.10.2 Uppgifter om abonnent och registrerad användare

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- abonnentens eller den registrerade användarens namn och adress
- namn på och adress till den abonnent eller registrerade användare som IP-adressen (Internet Protocol), användaridentiteten eller telefonnumret tilldelades vid tidpunkten för kommunikationen
- abonnentens (abonnenternas) eller den eller de registrerade användarnas namn och adress
- namn på och adress till abonnenten (abonnenterna) eller den eller de registrerade användarna och det användar-ID som tilldelats den avsedda mottagaren av kommunikationen

Uppgifter om abonnent och registrerad användare är nödvändiga för att spåra och identifiera en kommunikationskälla och för att identifiera slutmålet för en kommunikation. Det rör sig om namn, adress samt person- eller organisationsnummer, dvs. samma uppgifter som vid telefoni, Internetåtkomst och anslutningsform (se avsnitt 6.7.3, 6.11.2 och 6.12.1).

6.10.3 Datum och spårbar tid för på- och avloggning i meddelandetjänsten samt för avsändande och mottagande av meddelandet

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- datum och tid då kommunikationen påbörjades och avslutades
- datum och tid för på- respektive avloggning i den Internetbaserade e-posttjänsten eller Internettelefonitjänsten inom en given tidszon

Uppgifter om datum och spårbar tid för på- och avloggning i meddelandetjänsten samt för avsändande och mottagande av meddelandet är nödvändiga för att identifiera datum, tidpunkt och varaktighet för en kommunikation.

Vi har i avsnitt 6.7.4 redogjort för vår tolkning av direktivet vad gäller begreppet kommunikation i förhållande till på- och avloggning. Samma resonemang blir tillämpligt även här vad avser avsändande och mottagande av meddelandet.

6.10.4 Den tjänst som har använts och spårbar tid för användandet

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- datum och tid för på- respektive avloggning i Internetåtkomsttjänsten inom en given tidszon tillsammans med IP-adressen, oavsett om den är dynamisk eller statisk, som en kommunikation tilldelats av Internetåtkomstleverantören till en kommunikation och abonnents eller registrerad användares användar-ID
- datum och tid för på- respektive avloggning i den Internetbaserade e-posttjänsten eller Internettelefonitjänsten inom en given tidszon
- den telefonitjänst som används
- den Internettjänst som används

Uppgifter om den tjänst som har använts och spårbar tid för användandet är nödvändiga för att identifiera datum, tidpunkt och varaktighet för en kommunikation och för att identifiera typen av kommunikation.

I artikel 2 i direktivet om lagring av trafikuppgifter definieras telefonitjänst som uppringning (inbegripet rösttelefoni, röstmeddelanden, konferenssamtal och datatelefoni), extratjänster (inbegripet omstyrning och överflyttning av samtal) och meddelandeförmedling och multimedietjänster (inbegripet SMS, EMS och multimedietjänster).

Vårt sätt att strukturera lagringsskyldigheten innebär att under den här aktuella rubriken faller den del av telefonitjänst som avser meddelandehantering. För den del som vi betecknar som telefoni hänvisas till avsnitt 6.7.5.

Med tjänst avses exempelvis vidaresändning och/eller omstyrning. Uppgifterna ska lagras oavsett om ett meddelandeutbyte har skett eller inte.

6.11 Vilka uppgifter ska lagras vid Internetåtkomst?

Förslag: Vid Internetåtkomst ska följande uppgifter lagras:
– Användarens IP-adresser
– Uppgifter om abonnent och registrerad användare
– Datum och spårbar tid för på- och avloggning i Internettjänsten
– Typen av Internetanslutning som använts
– Slutpunkter

6.11.1 Användarens IP-adresser

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- tilldelade användar-ID
- namn på och adress till den abonnent eller registrerade användare som IP-adressen (Internet Protocol), användaridentiteten eller telefonnumret tilldelades vid tidpunkten för kommunikationen

Uppgifter om användarens IP-adresser är nödvändiga för att spåra och identifiera en kommunikationskälla.

6.11.2 Uppgifter om abonnent och registrerad användare

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- namn på och adress till den abonnent eller registrerade användare som IP-adressen (Internet Protocol), användaridentiteten eller telefonnumret tilldelades vid tidpunkten för kommunikationen

Uppgifter om abonnent och registrerade användare är nödvändiga för att spåra och identifiera en kommunikationskälla. Det rör sig om namn, adress samt person- eller organisationsnummer, dvs. samma uppgifter som vid telefoni, meddelandehantering och anslutningsform (se avsnitt 6.7.3, 6.10.2 och 6.12.1).

6.11.3 Datum och spårbar tid för på- och avloggning i Internettjänsten

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- datum och tid för på- respektive avloggning i Internetåtkomsttjänsten inom en given tidszon tillsammans med IP-adressen, oavsett om den är dynamisk eller statisk, som en kommunikation tilldelats av Internetåtkomstleverantören till en kommunikation och abonnents eller registrerad användares användar-ID

Uppgifter om datum och spårbar tid för på- och avloggning i Internettjänsten är nödvändiga för att identifiera datum, tidpunkt och varaktighet för en kommunikation.

6.11.4 Typen av Internetanslutning som använts

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- det uppringande telefonnumret för uppringda förbindelser
- DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare

Uppgifter om typen av Internetanslutning som använts är nödvändiga för att identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

6.11.5 Slutpunkter

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- det uppringande telefonnumret för uppringda förbindelser
- DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare

Uppgifter om slutpunkter är nödvändiga för att identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

Med slutpunkt avses den tekniska utrustningen i en fysisk ändpunkt som står under leverantörens kontroll, såsom telefonväxlar, routers, portnummer, utrustningsidentitet, MAC-adresser och abonnemangsidentitet. Dessutom innefattas i direktivets begrepp ”annan slutpunkt” uppgifter om leverantören av anslutningsform, dvs. den som tillhandahåller den kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst. Många Internetleverantörer tillhandahåller Internetåtkomst via förhyrd anslutningsform. För att de brottsbekämpande myndigheterna ska kunna få de uppgifter som behövs, krävs att myndigheterna också får kännedom om vem de ska vända sig till med en begäran om uppgifterna.

6.12 Vilka uppgifter ska lagras vid verksamheter som tillhandahåller kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst (anslutningsform)?

Förslag: Vid verksamheter som tillhandahåller kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst ska följande uppgifter lagras:
– Uppgifter om abonnent
– Vilken typ av kapacitet för överföring som har använts och spårbar tid för användandet
– Slutpunkter

6.12.1 Uppgifter om abonnent

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- namn på och adress till den abonnent eller registrerade användare som IP-adressen (Internet Protocol), användaridentiteten eller telefonnumret tilldelades vid tidpunkten för kommunikationen
- DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare

Uppgifter om abonnent är nödvändiga för att spåra och identifiera en kommunikationskälla och för att identifiera avsändarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

Det rör sig om namn, adress samt person- eller organisationsnummer, dvs. samma uppgifter som vid telefoni, meddelandehantering och Internetåtkomst (se avsnitt 6.7.3, 6.10.2 och 6.11.2).

6.12.2 Vilken typ av kapacitet för överföring som har använts och spårbar tid för användandet samt slutpunkter

Direktivet om lagring av trafikuppgifter anger uttryckligen att följande uppgifter ska lagras.

- det uppringande telefonnumret för uppringda förbindelser
- DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare

Uppgifter om typen av kapacitet som har använts vid en viss tidpunkt och slutpunkter är nödvändiga för att identifiera användarnas kommunikationsutrustning, eller den utrustning som de tros ha använt.

Exempel på kapacitet för överföring är DSL (vilket i sin tur kan ske med hjälp av leverantörer av t.ex. bitströmsaccess), fiberoptiska anslutningar, 3G (UMTS), GSM (GPRS), vanliga traditionella telefonmodem och WLAN (trådlöst nät).

Direktivet använder som synes begreppet ”DSL eller annan slutpunkt”. Där innefattas den teknik som många Internetåtkomstleverantörer har som sina respektive slutpunkter. Med slutpunkt avses den tekniska utrustningen i en fysisk ändpunkt som står under leverantörens kontroll, såsom telefonväxlar, routers, portnummer, utrustningsidentitet, MAC-adresser och abonnemangsidentitet.

6.13 Misslyckad uppringning m.m.

Förslag: Lagringsskyldigheten ska gälla även vid misslyckad uppringning.
Bedömning: En lagringsskyldighet för misslyckad uppringning innefattar uppgifter som inte lagras eller loggas av leverantören och går utöver direktivet om lagring av trafikuppgifter men kan motiveras utifrån en avvägning mellan brottsbekämpningsintresset och integritetsskyddet enligt direktivet om integritet och elektronisk kommunikation.

6.13.1 Misslyckad uppringning

Misslyckad uppringning tas upp i artikel 3 i direktivet om lagring av trafikuppgifter. Med detta avses att samtal kopplas men att ingen svarar på uppringningen. Misslyckad uppringning kan också bero på att det skett ett ingrepp av driften i kommunikationsnätet så att samtal har kopplats fram utan att nå mottagaren. Det sistnämnda kan leda till att den som försöker ringa får ett meddelande om att abonnenten inte kan nås för tillfället.

Enligt direktivet ska lagringsskyldighet gälla misslyckad uppringning under förutsättning att uppgifterna lagras eller loggas av leverantören (artikel 3).

De brottsbekämpande myndigheterna har anfört att de har behov av trafikuppgifter som gäller misslyckad uppringning. De har uppgivit att i dagsläget lagras/loggas uppgifter rörande misslyckad uppringning hos vissa leverantörer men inte hos andra. Myndigheterna har också berättat att sådana uppgifter allmänt sett är lika viktiga som uppgifter om ”lyckade” samtal. Det är med andra ord lika viktigt att få reda på t.ex. vem som *försökte* kontakta vem, när försöket gjordes, var personen befann sig och vilken typ av kommunikation som användes, som att få reda på vem som *lyckades* kontakta vem etc. Uppgifter om misslyckad uppringning kan lika väl som ett lyckat samtal ge de brottsbekämpande myndigheterna information som t.ex. identifierar gärningsmän och knyter dessa till varandra och till platser. Exempelvis används ”misslyckad uppringning” som ett kommunikationssätt mellan gärningsmän vid genomförandet av brott.

En lagringsskyldighet avseende misslyckad uppringning utöver direktivet om lagring av trafikuppgifter kan införas endast om det är motiverat utifrån de överväganden som ska göras enligt artikel 15.1 i direktivet om integritet och elektronisk kommunikation.

Vi instämmer med de brottsbekämpande myndigheterna i bedömningen att det finns ett lika stort behov av uppgifter rörande misslyckad uppringning som rörande de samtal som har lyckats. Vi ser inte heller att en på det sättet utformad generell lagringsskyldighet för sådana uppgifter skulle vara mer integritetskränkande än den lagringsskyldighet som gäller trafikuppgifter rörande samtal som lyckats och trafikuppgifter om misslyckad uppringning som har lagrats eller loggats. Dessutom skulle den begränsning som ligger i direktivet kunna leda till att de brottsbekämpande myndigheterna inte får tillgång till uppgifter som de får i dag. Vi föreslår därför att lagringsskyldigheten ska gälla vid misslyckad uppringning

fullt ut utan den begränsning som ligger i direktivet om att uppgifterna inte bara ska vara behandlade utan även lagrade eller loggade av leverantören.

6.13.2 Samtal som inte kopplas fram

I artikel 3 tas även en annan typ av ”misslyckade samtal” upp, nämligen samtal som inte kopplats fram. Det rör t.ex. situationer där det inträffat något tekniskt fel och inget meddelande lämnas om att abonnenten inte kan nås. Uppgifter om sådana samtal omfattas uttryckligen inte av direktivet om lagring av trafikuppgifter. De brottsbekämpande myndigheterna har uppgett att det inte finns något påtagligt behov av en lagringsskyldighet för sådana uppgifter och vårt förslag omfattar inte lagringsskyldighet i dessa fall.

6.14 Sammanfattning av våra bedömningar om lagringsskyldighet utöver direktivet m.m.

Bedömning: Lagringsskyldigheten för uppgifter om abonnents och registrerad användares person- och organisationsnummer liksom för uppgifter om datum och spårbar tid då kommunikationen påbörjades och avslutades vid Internettelefoni och datum och spårbar tid för avsändande och mottagande av meddelande vid meddelandehantering följer av direktivet om lagring av trafikuppgifter.

Den lagringsskyldighet utöver direktivet som vi föreslår för uppgifter om lokalisering vid mobiltsamtals slut och för uppgifter som inte lagras eller loggas vid misslyckad uppringning motiveras av behovet av dessa uppgifter i brottsbekämpningen och av att detta behov överväger det integritetsintrång som lagringen medför. Lagringsskyldigheten kan således motiveras utifrån artikel 15.1 i direktivet om integritet och elektronisk kommunikation.

På några punkter har vi föreslagit en lagringsskyldighet utöver direktivet om lagring av trafikuppgifter. Det rör lokaliseringsinformation för kommunikationens slut vid mobil telefoni och uppgifter om misslyckad uppringning även om uppgifterna inte lagras eller loggas av leverantören.

I några fall har vi diskuterat om uppgifterna omfattas av lagringsskyldigheten enligt direktivet. Det gäller uppgifter om person- eller organisationsnummer för abonnent och registrerad användare

(avsnitt 6.7.3, 6.10.2, 6.11.2 och 6.12.1) samt uppgifter om datum och spårbar tid då kommunikationen påbörjades och avslutades vid Internettelefoni och samma typer av uppgifter för avsändande och mottagande av meddelandet vid meddelandehantering (avsnitt 6.7.4 och 6.10.3). Vi har tolkat direktivet så att dessa uppgifter omfattas av lagringsskyldigheten. Om lagringsskyldighet för dessa uppgifter inte kan anses följa av direktivet måste lagringsskyldigheten motiveras utifrån artikel 15.1 i direktivet om integritet och elektronisk kommunikation.

Att personer och organisationer blir riktigt identifierade i samband med trafikuppgifterna är av grundläggande betydelse i utredningsarbetet och rör inte minst säkerheten för den enskilde. Det är inte en rimlig ordning att de brottsbekämpande myndigheterna ska behöva nöja sig med att få ut uppgifter som kanske helt saknar logisk knytning till ett verkligt namn. Vi gör den bedömningen att myndigheterna inte kommer att få tillgång till de uppgifter som behövs i det brottsbekämpande arbetet om en lagringsskyldighet för de nämnda uppgifterna inte skulle införas. Mot bakgrund av hur frekvent person- och organisationsnummer används i det svenska samhället kan vi inte heller se att integritetssynpunkter hindrar att lagringsskyldighet införs. Att uppgifter lagras om person- eller organisationsnummer som kan kopplas till abonnenten eller den registrerade användaren, kan därför enligt vår bedömning motiveras även utifrån de överväganden som ska göras enligt artikel 15.1 i direktivet om integritet och elektronisk kommunikation.

Uppgifter om när kommunikationen påbörjades och avslutades vid Internettelefoni och den typen av uppgifter för avsändande och mottagande av meddelande vid meddelandehantering är minst lika viktiga för de brottsbekämpande myndigheterna som samma typer av uppgifter vid fast och mobil telefoni, som på ett mer uttryckligt sätt anges i direktivet om lagring av trafikuppgifter. Vi gör även här den bedömningen att myndigheterna inte kommer att få tillgång till de uppgifter som behövs i det brottsbekämpande arbetet om en lagringsskyldighet för de nämnda uppgifterna inte skulle införas. Mot bakgrund av att samma typer av uppgifter ska lagras vid fast och mobil telefoni ser vi inte heller att integritetssynpunkter hindrar att lagringsskyldighet införs. Lagringsskyldigheten kan därför enligt vår bedömning motiveras även utifrån de överväganden som ska göras enligt artikel 15.1 i direktivet om integritet och elektronisk kommunikation.

Direktivet om lagring av trafikuppgifter omfattar fast och mobil telefoni, Internetåtkomst, e-post och Internettelefoni. Däremot

omfattas inte besök på websidor (”surfning”), besök på ”chattsidor” (”chattrum”) och användning av File Transfer Protocol, FTP (t.ex. överföring/nedladdning av filer) av lagringsskyldigheten enligt direktivet. De brottsbekämpande myndigheterna har uttryckt ett stort behov av att få tillgång till sådana uppgifter. Det ska nämnas att sådana uppgifter omfattas av den danska regleringen.

Med tiden blir det allt svårare att skilja de nämnda kommunikationstjänsterna åt. Exempelvis använder ”chattjänster” sig av både tal, text och bild. Gränserna mellan vad som faller in under de olika begreppen suddas alltmer ut. Vårt uppdrag begränsar dock de förslag som vi får presentera till uppgifter som avser fast och mobil telefoni, samt Internetåtkomst, e-post och Internettelefoni. Vi lämnar därför inte några förslag i sådana delar.

7 Lagringsskyldighetens fullgörande

7.1 Sammanfattning av våra förslag och bedömningar

- Lagring ska inte ske i ett centralt lager hos t.ex. staten.
- De leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation ska vara skyldiga att lagra trafikuppgifter.
- Tillsynsmyndigheten får efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen i enskilda fall medge undantag från lagringsskyldigheten.
- Uppgifterna ska lagras i ett år från det datum kommunikationen ägde rum.
- Vid lagringstidens slut ska uppgifterna utplånas, om inte de brottsbekämpande myndigheterna vid den tiden har begärt tillgång till uppgifterna men ännu inte fått ut dem eller leverantören annars har rätt att fortsätta behandla uppgifterna.
- Leverantörerna ska bedriva verksamheten så att uppgifterna enkelt kan tas om hand och lämnas ut utan dröjsmål.
- Trafikuppgifter som har lagrats för brottsbekämpande syften får behandlas av leverantörerna endast för att lämnas ut efter beslut om hemlig teleövervakning eller enligt bestämmelserna i lagen om elektronisk kommunikation, eller för att annan fullgör lagringen.

7.2 Var ska trafikuppgifter lagras och av vem?

7.2.1 Inledning

Frågan om var lagring av trafikuppgifter ska ske och vem som ska vara lagringsskyldig hänger samman med frågan om uppgifterna ska lagras på ett eller flera ställen. I våra direktiv anges som en målsätt-

ning att trafikuppgifterna ska lagras hos enbart en nät- eller tjänsteleverantör och inte hos flera leverantörer samtidigt. I skäl 13 i ingressen i direktivet om lagring av trafikuppgifter anges också att lagring bör ske på ett sådant sätt att man undviker att uppgifterna lagras mer än en gång och att tillämpningsområdet får begränsas till leverantörernas egna tjänster särskilt vid e-post och Internettelefoni. Innebörden av det sistnämnda är att leverantörerna inte ska åläggas att, så att säga, spara andra leverantörers uppgifter.

De trafikuppgifter som är aktuella att lagra kan genereras eller behandlas på flera ställen i en ”kommunikationskedja”. I många fall har de leverantörer som är inblandade i en del av en kommunikationskedja ingen vetskap om vilka andra leverantörer som också deltar. Trafikuppgifterna finns således inte samlade hos en enda tjänsteleverantör utan ett telefonsamtal (fast, mobilt eller med Internettelefoni) kan ofta involvera flera olika leverantörer med ”delansvar” för ”framföringen”. En del av de uppgifter som omfattas av direktivet om lagring av trafikuppgifter kommer därmed att kunna finnas hos flera leverantörer samtidigt eller kanske enbart hos någon av dem.

För att åstadkomma att lagring sker endast en gång av respektive uppgift och hos enbart en leverantör, skulle varje leverantör behöva ha ett system för att finna ut vilka andra leverantörer som genererat eller behandlat uppgifter i samband med en kommunikation. När det har skett behöver leverantörerna reda ut vilka uppgifter som båda har rörande exempelvis varje enskilt kommunikationstillfälle och komma överens om vem som ska lagra uppgifterna. Det är av praktiska, tekniska, sekretessmässiga och kostnadsmässiga skäl oerhört svårt, för att inte säga omöjligt, att skapa ett sådant system.

7.2.2 Ska lagring ske i ett centralt lager?

Förslag: Lagring ska inte ske i ett centralt lager hos t.ex. staten.

Ett alternativ för lagring av trafikuppgifter på ett ställe kunde vara att leverantörerna skickar de uppgifter som ska lagras till någon form av centralt lager. Det skulle innebära att antingen staten eller en leverantör lagrar samtliga trafikuppgifter som alla leverantörer genererar eller behandlar.

Fördelen med ett centrallager för de trafikuppgifter som ska lagras enligt direktivet är att alla säkerhetsåtgärder som behövs för att

skydda uppgifterna i lagret kan vidtas på ett enda ställe. För de brottsbekämpande myndigheterna skulle det också vara effektivt att behöva vända sig till enbart ett ställe när trafikuppgifter begärs ut. För leverantörerna skulle ett centrallager bli fördelaktigt om deras uppgift skulle inskränka sig till att söka och spara de trafikuppgifter som ska lagras och sända dem vidare till centrallagret.

Från integritetssynpunkt skulle ett centrallager dock bli problematiskt eftersom det skulle innebära att stora informationsmängder om enskilda personer skulle finnas samlade på ett enda ställe. Ett centrallager skulle också föra med sig tekniska komplikationer. Om varje leverantör som genererar eller behandlar trafikuppgifter som ska lagras skulle skicka dem till centrallagret, skulle det bli antingen ett antal dubbellagringar eller behövas teknisk utrustning som kunde identifiera vilka trafikuppgifter som redan lagrats och sortera bort de överflödiga. Det är också svårt att tänka sig någon annan lösning än att staten skulle bli ansvarig för centrallagret. Verksamheten skulle därmed behöva skötas av en statlig myndighet eller uppdras åt en privat aktör. Oavsett vilken form som valdes skulle det ställa stora krav på kunnande både i fråga om den teknik som finns hos leverantörerna och den teknik som behövs för själva lagringen och säkerhetsåtgärderna. Det skulle innebära att staten skulle behöva bygga upp en egen kompetens på områden där leverantörerna redan har en hög kompetens. En central lagring skulle också ställa mycket stora krav på lagringsvolym och säkra lösningar för överförande av uppgifterna från leverantörerna.

Alternativet är en lösning som innebär att trafikuppgifter ska lagras där de genereras eller behandlas. Det innebär visserligen att trafikuppgifter i vissa fall kommer att lagras på flera ställen men fördelarna med ett sådant system överväger ändå alternativet med ett centrallager. Genom att de leverantörer som genererar och behandlar uppgifterna också lagrar dem säkerställs att lagringen sker så enkelt och säkert som möjligt med utnyttjande av den kunskap om teknik som varje leverantör har. Vi bedömer också att lagring hos leverantörerna är ett klart bättre alternativ från integritetssynpunkt eftersom det minskar riskerna för att uppgifter om enskilda kan sammanställas. Vid lagring hos leverantörerna kommer trafikuppgifterna inte att vara omedelbart läsbara och i många fall kommer den enskilde leverantören bara att ha viss information som måste ställas samman med trafikuppgifter som lagrats av någon annan leverantör för att en enskild persons kommunikation ska kunna utläsas. Den ordningen innebär visserligen att de brottsbekämpande myndigheterna ofta behöver inhämta trafikuppgifter från

flera olika håll för att få tillgång till alla uppgifter och därmed få helhetsbilden. Vi är medvetna om att det inte är riktigt effektivt från brottsbekämpningssynpunkt men anser att fördelarna från integritetssynpunkt väl uppväger de nackdelar som myndigheterna får och vi föreslår därför att lagring ska ske hos leverantörerna.

7.2.3 Vilka leverantörer ska vara lagringsskyldiga?

Förslag: De leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation ska vara skyldiga att lagra trafikuppgifter.

Tillsynsmyndigheten får efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen i enskilda fall medge undantag från lagringsskyldigheten.

Direktivet om lagring av trafikuppgifter omfattar leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster *eller* allmänna kommunikationsnät. Det innebär att en leverantör av kommunikationstjänst inte samtidigt behöver leverera ett nät för att omfattas av skyldigheten att lagra trafikuppgifter (se t.ex. artikel 1 och 3). En motsatt ordning skulle få allvarliga konsekvenser för det brottsbekämpande arbetet. T.ex. skulle en leverantör som både tillhandahåller en tjänst och äger nät mycket lätt kunde undvika skyldigheten genom att organisera dessa båda verksamheter i olika bolag. Lagringsskyldigheten gäller alltså leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät. Det innebär att inte alla leverantörer blir lagringsskyldiga.

Begreppet elektronisk kommunikationstjänst specificeras inte i direktivet om lagring av trafikuppgifter. Däremot finns en definition i 1 kap. 7 § LEK som anger att det är fråga om en tjänst som vanligen tillhandahålls mot ersättning och som helt eller huvudsakligen utgörs av överföring av signaler i elektroniska kommunikationsnät. I samma bestämmelse definieras allmänt kommunikationsnät som elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster.

Direktivets uttryck om lagringsskyldigheten ansluter till 2 kap. 1 § LEK, där det anges att allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster endast får tillhanda-

hållas efter anmälan till tillsynsmyndigheten (PTS). Av 2 kap. 2 § LEK framgår att någon anmälan inte behöver göras för verksamheter som enbart består i att överföra signaler via tråd för utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen och att PTS får meddela föreskrifter om ytterligare undantag från anmälningsplikten. Sådana föreskrifter har inte meddelats.

I propositionen utvecklade regeringen anmälningsplikten på följande sätt (prop. 2002:03/110 s. 362).

> Bestämmelsen innebär att det ställs krav på alla som avser att tillhandahålla allmänna kommunikationsnät för kommersiellt bruk eller allmänt tillgängliga elektroniska kommunikationstjänster att göra en anmälan till tillsynsmyndigheten innan de påbörjar verksamheten. Genom att det anges att anmälningsplikten endast omfattar sådana allmänna kommunikationsnät som vanligen tillhandahålls mot ersättning avses att undanta t.ex. fastighetsnät i flerfamiljshus som utgör fastighetstillbehör och som fastighetsägaren inte tar ut någon särskild ersättning för av en operatör. Fastighetsägaren är då inte anmälningspliktig. Däremot kan nätet utgöra en del av ett allmänt kommunikationsnät som tillhandahålls mot ersättning av den operatör som fastighetsägaren har slutit avtal med. Alternativt kan operatören tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster över nätet. Operatören är då anmälningspliktig för denna verksamhet.
>
> Att det ska vara fråga om en allmänt tillgänglig elektronisk kommunikationstjänst innebär att radio- och TV-utsändningar till allmänheten där mottagaren erhåller ett på förhand bestämt programutbud inte omfattas av anmälningsplikten. Det gäller även utsändningar i digital form. Skulle en sådan tjänst bli en allmänt tillgänglig elektronisk kommunikationstjänst genom att utbudet inte kan anses på förhand bestämt, gäller emellertid regeln i 2 § för sådana sändningar som sker i tråd.
>
> I slutna nät är de tjänster som tillhandahålls bara åtkomliga inom en begränsad grupp och det står alltså inte öppet för en vid krets av användare att ansluta sig till nätet. Slutna nät är t.ex. interna företagsnät och nät inom myndigheter och andra organisationer. Det kan röra sig om telefonnät, trådburna datanät, radiobaserade sådana nät, interna kommunika-

> tioner för videoöverföring osv. inom företag, myndigheter och andra organisationer.

Regeringen angav följande i propositionen rörande undantaget i 2 kap. 2 § LEK (prop. 2002:03/110 s. 363).

> Genom bestämmelsen undantas tillhandahållandet av kabel-TV-nät och liknande nät från anmälningsplikten enligt 1 §, om verksamheten enbart består i att överföra signaler via tråd för utsändningar till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket YGL. Detsamma gäller tillhandahållande av elektroniska kommunikationstjänster som avser sådan överföring som anges i sistnämnda lagrum. Regeln motiveras framförallt av att vissa av de krav som lagen ställer upp för den som bedriver anmälningspliktig verksamhet skulle kunna komma i konflikt med den grundlagsfästa etableringsfriheten för sådana sändningar (se 3 kap. 1 § YGL). Bedrivs även annan verksamhet i sådana nät, t.ex. bredbandsanslutning till Internet, omfattas emellertid den verksamheten inte av undantaget.

Vi bedömer att det mest lämpliga är att låta skyldigheten att lagra trafikuppgifter ansluta till anmälningsplikten i 2 kap. 1 § LEK. Därmed ska alltså leverantörer av allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning och av allmänt tillgängliga elektroniska kommunikationstjänster ha skyldighet att lagra uppgifterna. Eftersom vi föreslår att skyldigheten att lagra trafikuppgifter ska följa med anmälningsplikten blir tolkningen och tillämpningen av 2 kap. 1 § LEK avgörande för vilka som ska vara lagringsskyldiga. Det är till PTS som anmälan ska göras och det blir PTS som i första hand genom sin tillämpning av bestämmelsen får avgöra gränserna för vilka leverantörer som ska vara lagringsskyldiga. I det avseendet är det givetvis av stor vikt att hänsyn tas till den snabba teknikutvecklingen. Bestämmelserna bör inte få en för snäv tillämpning så att färre verksamheter omfattas av lagringsskyldigheten än vad som är avsikten med reglerna om anmälnings- och lagringsskyldigheterna i lagen om elektronisk kommunikation.

En del verksamheter, som i och för sig är anmälningspliktiga, är av liten omfattning samtidigt som det inte är intressant ur ett brottsbekämpande perspektiv att leverantören som bedriver verksamheten lagrar trafikuppgifter. Det behöver därför enligt vår me-

ning finnas en möjlighet till undantag från lagringsskyldigheten. I t.ex. det danska förslaget har en generell gräns för skyldigheten att lagra satts till 100 ”enheter”, dock enbart för vissa typer av föreningar (andelsforeninger, ejerforeninger, antenneforeninger og lignende foreninger eller sammenslutninger heraf). Enligt vår bedömning är det inte lämpligt att koppla skyldigheten att lagra trafikuppgifter till antalet enheter/kunder eller till en viss minsta omsättning. I takt med teknikutvecklingen kommer detta att skapa onödiga gränsdragningsproblem.

Det får i första hand vara en fråga för tillsynsmyndigheten att närmare avgöra vilka leverantörer som ska undantas från skyldigheten att lagra trafikuppgifter. Vid den bedömningen får det ske en avvägning mellan nyttan för brottsbekämpningen av att leverantören lagrar trafikuppgifterna och kostnaden för leverantören.

Frågan blir då om undantagen från skyldigheten att lagra bör ske i föreskriftsform eller genom beslut i enskilda fall.

Den anpassningsskyldighet som gäller i dag enligt 6 kap. 19 § LEK för hemlig teleavlyssning och hemlig teleövervakning innehåller en möjlighet till undantag efter beslut av PTS i enskilda fall. Även BRU:s förslag till förändring av den bestämmelsen innehåller en möjlighet till sådana undantag. BRU motiverade detta på bl.a. följande sätt (SOU 2005:38 s. 286 f.).

> Den tekniska utvecklingen går fort. De tekniska förhållandena hos varje operatör är i många avseenden unika. I dag kan det sägas finnas en än högre grad av variation hos operatörerna när det gäller verksamheternas inriktning, omfattning och tekniska lösningar jämfört med för tio år sedan då anpassningsskyldigheten infördes i telelagen. Detta ställer krav på differentierade lösningar vad gäller anpassningen i detalj. Den bedömning som regeringen gjorde tidigare har blivit bekräftad i den praktiska tillämpningen, nämligen att anpassningsskyldigheten i sig och särskilt undantag från denna inte lämpar sig att närmare beskriva i generella föreskrifter eller villkor av generell karaktär. Det kan leda till en osäkerhet såväl hos operatörerna som hos de brottsutredande myndigheterna om anpassningsskyldighetens innebörd och omfattning och därmed också till bristande effektivitet. Det ska också sägas att den grova brottsligheten enligt Rikspolisstyrelsen är uppmärksam på gränserna för de brottsutredande myndigheternas operativa möjligheter, dvs. generella föreskrifter om undantag från anpassningsskyldigheten, men även offentliga

> undantagsbeslut i enskilda fall, ger de kriminella personerna en bra uppfattning om vilka operatörer och vilka kommunikationsformer som är lämpliga att använda för deras verksamhet. Till detta kommer särskilt att operatörerna har påtalat för oss vikten av en tydlig, förutsebar reglering av anpassningsskyldigheten.

De argument som BRU angav för att enligt 6 kap. 19 § LEK ge utrymme för att i enskilda fall medge undantag från anpassningsskyldigheten har bäring även för vår bedömning av formerna för beslut om undantag. Den tekniska utvecklingen och variationen i leverantörernas verksamhet är tungt vägande skäl för att systemet bör utformas som en möjlighet för tillsynsmyndigheten (PTS, se avsnitt 10.4) att meddela undantag i enskilda fall från skyldigheten att lagra uppgifter. Undantagen bör få meddelas efter en ansökan av en leverantör och efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen (jfr 36 § förordningen om elektronisk kommunikation).

Det kan inträffa att personer som bedriver allvarlig brottslig verksamhet kommer att söka sig till de leverantörer som är undantagna från lagringsskyldigheten. Visserligen skulle det förhållandet att en leverantör får många nya kunder i och för sig vara ett skäl för att undantaget inte längre ska gälla. Detsamma gäller om de brottsbekämpande myndigheterna skulle upptäcka att kriminella personer söker sig till en viss leverantör som är undantagen från lagringsskyldigheten. Vi menar att mer exakt information om vilka leverantörer som inte är lagringsskyldiga kan skada både PTS verksamhet för prövning av frågor om undantag och brottsbekämpningen om de är offentliga. Vi föreslår därför att sekretess ska gälla hos myndigheterna för uppgifter som hänför sig till PTS verksamhet för prövning av frågor om undantag, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

Det är viktigt att påpeka att den möjlighet som PTS har enligt 7 § förordningen om elektronisk kommunikation att meddela undantag från anmälningsplikten enligt 2 kap. 1 § LEK inte är avsedd att användas i syfte att reglera lagringsskyldighetens omfattning. Vi återkommer till tillsynsmyndighetens befogenheter i avsnitt 10.5.

Ur ett brottsbekämpande perspektiv ligger det en begränsning i att direktivet om lagring av trafikuppgifter enbart omfattar leverantörer av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster. Oftast när t.ex. en e-posttjänst tillhandahålls ett ”slutet sällskap”, t.ex. de anställda i fö-

retag och myndigheter (där e-postadressen ofta slutar med företags- eller myndighetsnamnet), är företaget respektive myndigheten närmast att betrakta som tjänsteleverantör utan att samtidigt leverera en allmänt tillgänglig tjänst. Företaget/myndigheten omfattas då heller inte av skyldigheten att lagra enligt direktivet. Eftersom varje leverantör enbart ska lagra uppgifter som leverantören själv genererat eller behandlat, kommer uppgifterna i de fallen inte att lagras över huvud taget.

Utifrån de brottsbekämpande myndigheternas behov av att få tillgång till viktig information, bör vi enligt våra direktiv överväga om sådana nät- och tjänsteleverantörer som inte omnämns i direktivet och som inte heller är anmälningspliktiga enligt lagen om elektronisk kommunikation borde omfattas av en skyldighet att lagra och lämna ut trafikuppgifter.

Vi inser att det finns ett behov hos de brottsbekämpande myndigheterna av att flera leverantörer än de som följer av direktivet om lagring av trafikuppgifter får skyldighet att lagra trafikuppgifter. Samtidigt skulle ett system som innebär att andra än anmälningspliktiga leverantörer skulle omfattas av lagringsskyldigheten bli svårt att överblicka och kontrollera. Det får därför bli en fråga för framtiden om den lagringsskyldighet vi föreslår är rätt avvägd vad gäller kretsen lagringsskyldiga leverantörer.

7.3 Lagringstiden

7.3.1 Bakgrund

Artikel 6 i direktivet om lagring av trafikuppgifter anger att uppgifterna ska lagras under en period om minst sex månader och högst två år från det datum då kommunikationen ägde rum. Våra direktiv anger i den frågan att utgångspunkten ska vara att lagringstiden inte ska understiga ett år för någon typ av trafikuppgift och att andra lagringstider är möjliga om detta bedöms vara lämpligt.

BRU konstaterade tidigare (SOU 2005:38 s. 326-328) att de brottsbekämpande myndigheterna har behov av trafikuppgifter som är flera år gamla i utredningar av grova brott och att det finns flera orsaker till att leverantörerna relativt sällan i dagsläget får förfrågningar på uppgifter som är äldre än tolv månader. De främsta skälen är enligt vad BRU kom fram till att det finns en skyldighet för leverantörerna att utplåna uppgifterna och att myndigheterna, när frågan om utlämnande blir aktuell, är medvetna om att utplå-

nande måste ha skett och/eller att myndigheterna inte har möjlighet att av kostnadsskäl begära uppgifterna. Säkerhetspolisen uttryckte till BRU att en lång lagringstid, uppåt tre år, behövdes särskilt i utredningar av grov brottslighet, t.ex. grova våldsbrott, brott av organiserad karaktär och terroristbrott, där planering och förberedelser kan pågå under mycket lång tid, kanske flera år, och att det finns behov av att få uppgifter äldre än tolv månader i några hundra förundersökningar årligen. Särskilt som det rör sig om grova brott där brottsligheten även många gånger kan sägas vara organiserad, instämde BRU i Säkerhetspolisens bedömning att det är av synnerlig vikt för det brottsutredande arbetet att uppgifter finns tillgängliga under längre tid tillbaka än tolv månader.

Rikspolisstyrelsen, Säkerhetspolisen, Åklagarmyndigheten och Ekobrottsmyndigheten har uttryckt till oss att lagringstiden bör bestämmas till två år. Som skäl har myndigheterna fört fram trafikuppgifternas stora betydelse i utredningar framför allt rörande organiserad brottslighet. Myndigheterna har gett oss flera exempel på situationer där tillgången till trafikuppgifter även efter tolv månader är av synnerlig vikt för utredning av allvarlig brottslighet. Flera år gamla trafikuppgifter behövs om brottet uppdagas först efter lång tid, om brottet kräver ett långt utredningsarbete, om utredningsuppslag saknas till en början, t.ex. när vittnen framträder först sent efter brottet, och om utredningen har internationell anknytning och rättslig hjälp till eller från andra länder behövs för utredningen.

Utifrån en bedömning av hur snabbt vissa brott klaras upp, har polisen tagit fram siffror som anger exempel på hur många utredningar av grova brott som *skulle kunna* gagnas per år av en tvåårig lagringstid. Vid sidan om Säkerhetspolisens och Ekobrottsmyndighetens område rör det enligt polisen i vart fall 22 mord, 450 våldtäkter/försök till våldtäkter, 60 rån, 500 Internetrelaterade barnpornografibrott, 50 fall av människohandel och koppleri samt 480 dataintrång. Tyvärr är det i stort sett en omöjlighet att ta fram siffror på hur många av dessa utredningar som *faktiskt skulle gagnas* av en längre lagringstid en ett år.

Från åklagare har vi också fått enskilda exempel på förundersökningar där det har behövts trafikuppgifter som varit mer än ett år gamla. Det har bl.a. varit fallet i ett ärende om förberedelse till terroristbrott och förberedelse till allmänfarlig ödeläggelse där så gamla trafikuppgifter användes för att styrka vissa kontakter mellan de misstänkta och personer i ett annat land. Ett annat ärende rörde företagsspioneri där uppgifterna behövdes för att visa omfattningen

av den brottsliga verksamheten. Vid ett tillslag mot 118 personer misstänkta för Internetrelaterat barnpornografibrott hade uppkopplingarna mot den server där det barnpornografiska materialet fanns skett från hösten 2002 till mars 2003 medan ärendet initierades hos de brottsutredande myndigheterna först i februari 2004. I en utredning rörande en serie grova rån var trafikuppgifter som var mer än ett år gamla den avgörande bevisningen angående några av de äldre rånen. I ett mordfall i Stockholm återfanns en död kropp 15 månader efter dödandet. Där var gamla trafikuppgifter den avgörande bevisningen som gjorde att det över huvudtaget gick att utreda ärendet och väcka åtal. I ett ärende rörande misstankar om grovt narkotikabrott, grov narkotikasmuggling, grovt dopningsbrott samt grov smuggling (av dopningsmedel) begärdes trafikuppgifter som var äldre än ett år in rörande telefonkontakter mellan den misstänkte och personer i ett främmande land. Detta hade betydelse för att visa direktkontakter mellan köpare och säljare under hela den tid som misstankarna avsåg. Även vid begäran om rättslig hjälp från utlandet har trafikuppgifter äldre än ett år varit viktiga att få fram.

7.3.2 Våra överväganden

Förslag: Uppgifterna ska lagras i ett år från det datum kommunikationen ägde rum.

Vid lagringstidens slut ska uppgifterna utplånas, om inte de brottsbekämpande myndigheterna vid den tiden har begärt tillgång till uppgifterna men ännu inte fått ut dem eller leverantören annars har rätt att fortsätta behandla uppgifterna.

Det går inte att generellt påstå att vissa av de trafikuppgifter som ska lagras är mer eller mindre viktiga än andra för utredning av allvarlig brottslighet. Trafikuppgifternas betydelse i de enskilda brottsutredningarna varierar självfallet beroende på en rad olika omständigheter som är hänförliga till de särskilda utredningar där de kommer till användning. De brottsbekämpande myndigheterna har inte heller framfört något behov av eller några skäl för att ha skilda lagringstider för olika typer av trafikuppgifter. Vi har inte heller kunnat finna något som talar för att lagring av trafikuppgifter skulle vara mer eller mindre integritetskänslig beroende på vilken typ av trafikuppgift det är fråga om. Att skilja lagringstiderna åt är därmed varken önskvärt eller behövligt av integritetsskyddsskäl.

Givetvis går det inte heller att i förväg veta vilka trafikuppgifter som kommer att bli intressanta för de brottsbekämpande myndigheterna i utredningar av olika typer av brottslighet. Det är därför inte möjligt att bestämma lagringstiden generellt efter vad som behövs t.ex. i utredningar rörande terroristbrott eller andra brottstyper som begås inom ramen för organiserad brottslighet eller att med brottstyper som avgränsning ha ett system med skilda lagringstider beroende på svårhetsgraden av vissa brott.

Vi föreslår därför att en och samma lagringstid ska gälla för alla typer av trafikuppgifter. Det ger också den mest okomplicerade regleringen.

Frågan blir då hur lång lagringstiden ska vara. Direktivet ger möjlighet till minst sex månaders och högst två års lagring. Utgångspunkten för vårt arbete ska enligt våra direktiv vara att lagringstiden inte ska understiga ett år för någon typ av trafikuppgift men att andra lagringstider är möjliga om det bedöms vara lämpligt.

Allvarliga brott orsakar stora skador för enskilda och samhället. Varje sådant brott som klaras upp, kanske redan på planeringsstadiet, är av stort värde. Det är också avgörande för en effektiv bekämpning av allvarlig brottslighet att de brottsbekämpande myndigheterna har tillgång till trafikuppgifter. Det är den insikten som ligger bakom tillkomsten av direktivet om lagring av trafikuppgifter. Även om majoriteten av de grova brotten torde klaras upp inom ett år efter det att brottet har begåtts visar de beräkningar vi har fått om utredningar som skulle kunna gagnas av en tvåårig lagringstid att så gamla trafikuppgifter skulle användas vid ett inte obetydligt antal utredningar som alla gäller mycket grov brottslighet. Vi har också fått konkreta exempel på ett antal fall där två år gamla trafikuppgifter har varit av synnerlig vikt för utredningen och faktiskt lett till att brottet kunde klaras upp. För vissa utredningar om t.ex. terroristbrott och ekonomisk brottslighet behövs i själva verket till och med äldre trafikuppgifter än så. Vi utgår därför i våra överväganden från att upp till två år gamla trafikuppgifter behövs och är helt nödvändiga för bekämpningen av allvarlig brottslighet.

Teknikutvecklingen innebär hela tiden nya möjligheter för dem som vill begå brott och olika tekniker för kommunikation används för att planera och utföra brott och för att dölja dem. Både för medborgarna i allmänhet och brottsoffren är det angeläget att de möjligheter som den tekniska utvecklingen ger också kan användas i brottsbekämpningen så att förutsättningarna för att klara upp allvarliga brott blir så goda som möjligt.

Sett utifrån medborgarnas intressen och betydelsen för brottsoffer av att allvarliga brott utreds och gärningsmän lagförs anser vi att en lagringstid på två år väl skulle kunna motiveras.

Vårt uppdrag är dock inte att bedöma hur lång lagringstiden bör vara enbart utifrån ett brottsbekämpningsperspektiv. I vårt arbete med förslaget till genomförande av direktivet ska vi också beakta medborgarnas intresse av skydd för den personliga integriteten, att kostnaderna för genomförandet får en samhällsekonomiskt effektiv lösning samt behovet av en väl fungerande konkurrens. Vi ska alltså, efter en genomlysning av de aspekter som detta vidare perspektiv för med sig, bedöma hur lång lagringstiden bör vara.

Vi har i avsnitt 5 konstaterat att ett genomförande av direktivet kommer att föra med sig att en stor mängd trafikuppgifter kommer att lagras och att redan lagringen av trafikuppgifterna innebär ett intrång i medborgarnas integritet. Det är naturligt att medborgarnas upplevelse av intrånget har samband med lagringstidens längd. Intrånget i integriteten eller snarare medborgarnas upplevelse av att vara kontrollerade varar naturligtvis så länge lagringen pågår. Vi kommer i avsnitten 8-10 att behandla de olika överväganden vi gör i frågor om kontroll och tillsyn och våra överväganden om vilket skydd genom administrativa, straffrättsliga och civilrättsliga regler som behövs för att risken för konkreta integritetsskador ska bli så låg som möjligt. Det går dock inte att komma ifrån att ett gott skydd med olika former av tillsyn, prövning i förhand och en kontroll i efterhand ändå aldrig kan bli heltäckande och att det därmed finns en viss risk för att enskilda drabbas av konkreta integritetsskador, t.ex. genom att lagrade trafikuppgifter läcker ut och sprids. För vår bedömning av lagringstidens längd måste vi därför beakta att risken för konkreta integritetsskador genom t.ex. läckage eller annan otillåten spridning ökar med lagringstidens längd.

Också olika mer tekniska faktorer har betydelse när det gäller att bedöma hur lång lagringstiden bör vara. Lagringen av trafikuppgifterna innebär att en mängd uppgifter behöver lagras. Det kommer att ställa krav på en lagringskapacitet av stor volym och krav på en god säkerhetsnivå både avseende teknisk kapacitet och administrativa rutiner för hanteringen av lagret. Lagringsvolymen ökar självfallet ju längre lagringstiden blir och det medför ökade krav på säkerhet. För att uppgifterna enkelt ska kunna överlämnas till de brottsbekämpande myndigheterna bör de också vara sökbara på ett rationellt sätt. Sökbarheten påverkas av den samlade mängden av lagrade trafikuppgifter. Även om vi inte har låtit göra olika kostnadsberäkningar utifrån olika lagringstider måste en försiktig slut-

sats vara att kostnaderna för teknik och administrativa säkerhetsrutiner blir högre med en lagringstid på två år än med en lagringstid på ett år eller sex månader.

Inom marknaden för elektronisk kommunikation finns aktörer av vitt skilda slag. Vissa levererar en tjänst, andra levererar ett nät och ett antal levererar både tjänster och nät. Volymen på den verksamhet som leverantörerna tillhandahåller skiljer sig också väldigt mycket åt, det finns allt ifrån mycket stora leverantörer till leverantörer med relativt få kunder. Lagringstidens längd kan få olika betydelse för de olika leverantörerna och det är svårt att bedöma hur den skulle slå i konkurrenshänseende mellan leverantörer av olika storlek och mellan leverantörer av tjänster eller nät. Det vi med rimlig grad av säkerhet kan säga är dock att kraven på den kapacitet som leverantörerna måste ha för att fullgöra lagringsskyldigheten och kostnaderna för lagringen ökar med lagringstiden och att lagringstiden är en av de faktorer som kan påverka såväl etablerade som presumtiva aktörers investeringsvilja. Den tekniska utvecklingen har också lett till att kunderna inte är beroende av nationsgränser när de väljer att teckna abonnemang för fast och mobil telefoni och Internet. Den lagringstid som bestäms i Sverige blir därmed, jämförd med de lagringstider som kommer att gälla i andra medlemsstater i EU, en faktor som påverkar konkurrensen.

Även om vi ser att det från brottsbekämpningssynpunkt finns ett starkt behov av att bestämma en så lång lagringstid som möjligt bedömer vi att skyddet för den personliga integriteten och kostnads-, säkerhets- och konkurrensaspekter med sinsemellan olika styrka talar för en så kort lagringstid som möjligt. Vi behöver därför göra en avvägning som innebär att brottsbekämpningsintresset i så hög grad som möjligt blir tillgodosett samtidigt som framför allt integritetsskyddet tillgodoses och systemet blir effektivt utifrån kostnads- och konkurrenssynpunkt.

Intrånget i medborgarnas personliga integritet blir naturligtvis minst om lagringstiden blir sex månader och det är också den lagringstid som torde medföra minst kostnader. Samtidigt måste man utgå från att även en så kort lagringstid kräver stora investeringar i ny teknik och medför krav på nya säkerhetsrutiner. Det betyder att initialkostnaderna för lagring av trafikuppgifter blir stora för en lagringstid på sex månader och att de sedan ökar men inte dubbleras med t.ex. ett års lagringstid. Vi vet att utredningar om avancerad och allvarlig brottslighet måste få ta viss tid i anspråk. Brottsplanerna är ofta avancerade och det kan ta tid att kartlägga och utreda omständigheterna kring ett visst brott på ett sätt som kan leda till

att gärningsmannen eller gärningsmännen kan åtalas och dömas. Förhållandena kring brottsligheten kan också vara så komplicerade att det inte minst av rättsäkerhetsskäl krävs tid för att en mängd olika åtgärder ska kunna genomföras så att förundersökningen kan hålla den kvalitet som fordras i alla utredningar om grov brottslighet. Trafikuppgifter är en betydelsefull del av alla de utredningsåtgärder som vidtas i en komplicerad utredning om ett allvarligt brott. Vi bedömer att en så kort lagringstid som sex månader skulle innebära att de brottsbekämpande myndigheterna fick arbeta under en tidspress som skulle riskera att motverka både utredningarnas kvalitet i stort och rättsäkerhetsaspekterna i förhållande till de misstänkta. En sex månader lång lagringstid skulle dessutom innebära att vissa av de trafikuppgifter som de brottsbekämpande myndigheterna får tillgång till i dag vid hemlig teleövervakning och utlämnande enligt lagen om elektronisk kommunikation inte skulle bli tillgängliga i framtiden. Med andra ord skulle många av de brott som i dag klaras upp med hjälp av trafikuppgifterna inte ha samma förutsättningar att bli utredda i framtiden.

Om lagringstiden i stället bestäms till ett år blir integritetsintrånget för medborgarna detsamma men pågår under längre tid och risken för verkliga intrång i enskildas integritet genom t.ex. läckage ökar i viss grad. Samtidigt tillgodoses de brottsbekämpande myndigheternas behov i betydligt fler fall. En lagringstid på ett år innebär att de brottsbekämpande myndigheterna kan få tillgång till trafikuppgifter i det stora flertalet utredningar där sådana uppgifter är av synnerlig vikt för utredningen.

En ettårig lagringstid är fortfarande en begränsning i förhållande till de brottsbekämpande myndigheternas behov, eftersom trafikuppgifter inte garanterat kommer att finnas tillgängliga för de situationer där brottet upptäcks efter lång tid eller för de utredningar som på grund av utredningens komplexitet tar lång tid eller när spaningsuppslag saknas inom ett år från brottet. Detsamma gäller i de fall där svenska myndigheter behöver lämna rättslig hjälp eftersom det administrativa förfarandet kring rättslig hjälp fortfarande är tidskrävande. Tiden för lagring av trafikuppgifter kan dock inte ses för sig utan måste bedömas utifrån de andra möjligheter som de brottsbekämpande myndigheterna har att bekämpa allvarlig brottslighet. En sådan möjlighet är myndigheternas utveckling av kriminalunderrättelseverksamheten och förutsättningarna att inhämta trafikuppgifter på ett tidigt stadium vid bekämpningen av allvarlig brottslighet. Riksdagen behandlar för närvarande ett förslag om hemlig rumsavlyssning (prop. 2005/06:178) och ett förslag om åt-

gärder för att förhindra vissa särskilt allvarliga brott (prop. 2005/06:177) Om samtliga dessa verktyg kan och kommer att användas av de brottsbekämpande myndigheterna på ett ändamålsenligt sätt kommer de tillsammans med en lagringstid på ett år att innebära att förutsättningarna för bekämpning av allvarlig brottslighet förbättras.

Av intresse för bedömningen av hur lång lagringstid som bör gälla i Sverige är också hur andra länder har valt att bestämma lagringstiden. Det har betydelse för att Sverige ska kunna delta i brottsbekämpningen inom unionen på lika villkor som andra länder. Den undersökning vi har gjort (avsnitt 4) visar att flertalet av länderna i EU har valt att bestämma lagringstiden till ett år.

Enligt vår bedömning skulle en lagringstid på ett år innebära en förbättring för de brottsbekämpande myndigheterna i förhållande till i dag, när det ofta beror på slumpen huruvida trafikuppgifter över huvud taget finns sparade och kan lämnas ut för de brottsbekämpande ändamålen. Därmed skulle en stor del av brottsbekämpningsintresset tillgodoses till en rimlig kostnad samtidigt som skyddet för integriteten kan upprätthållas och risken för konkreta integritetsintrång inte blir oacceptabel. Likheten med andra länders reglering innebär också fördelar.

Frågan blir då om brottsbekämpningsintresset ändå väger tyngre så att lagringstiden bör bestämmas till t.ex. 18 månader eller två år. Vid den avvägningen bedömer vi att intresset av att skydda den personliga integriteten i nuläget väger tyngre än behovet av att ha uppgifterna lagrade under så lång tid.

Vi föreslår därför att lagringstiden ska bestämmas till ett år.

Våra förslag innebär att vissa trafikuppgifter utöver dem som följer av direktivet om lagring av trafikuppgifter ska lagras. Även om skälen för lagring av dessa trafikuppgifter inte grundar sig på direktivet utan på överväganden enligt artikel 15.1 i direktivet om integritet och elektronisk kommunikation bör lagringstiden för dessa uppgifter bestämmas utifrån samma utgångspunkter och till samma tid som de trafikuppgifter som ska lagras enligt direktivet om lagring av trafikuppgifter.

Det ska nämnas att artikel 12 i direktivet om lagring av trafikuppgifter tillåter att en medlemsstat som står inför särskilda omständigheter som föranleder en tidsbegränsad förlängning av den högsta tillåtna lagringstiden får vidta nödvändiga åtgärder för detta.

Nästa fråga blir från vilken tidpunkt lagringstiden ska beräknas. Artikel 6 i direktivet om lagring av trafikuppgifter anger att lagringstiden ska räknas från det datum kommunikationen ägde rum.

En kommunikation börjar och slutar oftast inte vid samma tidpunkt utan den har en viss varaktighet. För att syftet med lagringen av trafikuppgifter ska tillgodoses så långt som möjligt bör lagringstiden räknas från det att kommunikationen avslutades.

Artikel 7 i direktivet om lagring av trafikuppgifter föreskriver att uppgifterna ska förstöras vid slutet av lagringstiden, utom de uppgifter för vilka tillgång har medgivits och som har bevarats. Det är alltså enligt direktivet inte tillåtet att enbart avidentifiera uppgifterna som har lagrats för brottsbekämpande syften (jfr 6 kap. 5 § LEK). Den reglering vi föreslår innehåller därför ett krav på att uppgifterna ska utplånas vid lagringstidens slut, om inte de brottsbekämpande myndigheterna vid den tiden har begärt tillgång till uppgifterna men ännu inte fått ut dem eller leverantören annars har rätt att fortsätta behandla uppgifterna, t.ex. för att de krävs för abonnentfakturering. Skulle uppgifterna av sistnämnda skäl finnas kvar hos leverantören sedan den ettåriga lagringstiden gått ut, är leverantören skyldig att även efter ettårstiden lämna ut uppgifterna om förutsättningar finns enligt bestämmelserna i rättegångsbalken eller lagen om elektronisk kommunikation. Den lagringstid vi föreslår blir med andra ord inte en yttersta gräns bakåt i tiden för de brottsbekämpande myndigheternas rätt att få tillgång till trafikuppgifter som leverantörerna har.

7.4 Leverantörernas medverkan inom viss tid m.m.

Förslag: Leverantörerna ska bedriva verksamheten så att uppgifterna enkelt kan tas om hand och lämnas ut utan dröjsmål.

I avsnitt 2.5.2 redogjorde vi för den anpassningsskyldighet som finns föreskriven i 6 kap. 19 § LEK. Den innebär att en verksamhet ska bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs. Anpassningsskyldigheten innebär också att innehållet i och uppgifter om avlyssnade eller övervakade telemeddelanden ska göras tillgängliga så att informationen enkelt kan tas om hand. Anpassningsskyldigheten gäller alltså för såväl hemlig teleavlyssning som hemlig teleövervakning och avser både historiska uppgifter och realtidsuppgifter.

Av bestämmelsen framgår att anpassningsskyldigheten gäller endast för vissa verksamheter, nämligen tillhandahållande av

1. ett allmänt kommunikationsnät som inte enbart är avsett för utsändning till allmänheten av program i ljudradio eller annat som anges i 1 kap. 1 § tredje stycket yttrandefrihetsgrundlagen, eller

2. tjänster inom ett allmänt kommunikationsnät vilka består av

a) en allmänt tillgänglig telefonitjänst till fast nätanslutningspunkt som medger överföring av lokala, nationella och internationella samtal, telefax och datakommunikation med en viss angiven lägsta datahastighet, som medger funktionell tillgång till Internet, eller

b) en allmänt tillgänglig elektronisk kommunikationstjänst till mobil nätanslutningspunkt.

Skyldigheten att lagra trafikuppgifter enligt vårt förslag omfattar samtliga de leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation. Den omfattar därmed flera leverantörer än de som är anpassningsskyldiga enligt 6 kap. 19 § LEK.

För att systemet med lagring av trafikuppgifter ska bli effektivt och verkligen bidra till bekämpningen av allvarlig brottslighet bör skyldigheten att lagra trafikuppgifterna förenas med en precisering av anpassningsskyldigheten enligt 6 kap. 19 § LEK som innebär ett krav på att de lagringsskyldiga leverantörernas verksamhet ska bedrivas så att de lagrade uppgifterna enkelt kan tas om hand av de brottsbekämpande myndigheterna.

Därutöver behöver det ställas krav i fråga om hur snabbt uppgifterna ska göras tillgängliga för myndigheterna. Enligt artikel 8 i direktivet om lagring av trafikuppgifter ska det säkerställas att uppgifterna lagras på ett sådant sätt att de tillsammans med annan nödvändig information *utan dröjsmål* kan överföras till myndigheterna efter begäran.

I 27 kap. 25 § första stycket RB finns en bestämmelse om verkställighet av beslut om hemlig teleavlyssning och hemlig teleövervakning. Av paragrafen framgår att de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen får användas när rätten har lämnat tillstånd till tvångsmedlen. Med det uttrycket avses bl.a. att de tekniska hjälpmedlen får anslutas, underhållas och återtas. Av detta följer att leverantörerna har en skyldighet att biträda och lämna tillträde för brottsutredande myndigheter.

BRU konstaterade (SOU 2005:38 s. 336 ff.) att ett tvångsmedelsbeslut medför en skyldighet för leverantören att i viss mån medverka vid verkställigheten men att detta inte innebär en skyldighet att tillhandahålla utrustning eller tekniska lösningar och inte heller att biträda vid verkställigheten inom viss tid. BRU hade bl.a. identifierat att servicenivån hos många leverantörer avseende den

tid som förflyter från beställning av åtgärden till dess att tvångsmedelsbeslutet kan börja verkställas var för låg. BRU föreslog därför en bestämmelse i 27 kap. RB om att en leverantör skulle vara skyldig att *genast* på begäran av en brottsutredande myndighet medverka vid verkställighet av tvångsmedelsbesluten. Med det uttrycket avsåg BRU att arbetet skulle vara påbörjat inom en timme under kontorstid beträffande samliga leverantörer och även under annan tid beträffande de leverantörer som då har personella resurser avdelade för drift- och nätövervakning.

I skyldigheten att lagra trafikuppgifter ligger att det ska finnas teknik och resurser hos leverantörerna för att överföra nödvändig information till de brottsbekämpande myndigheterna inom en kortare tid. Det kravet kan uttryckas såsom i artikel 8 i direktivet om lagring av trafikuppgifter, nämligen att uppgifterna ska lämnas ut till myndigheterna *utan dröjsmål*. Vad som avses med detta uttryck kan skilja sig åt beroende på förhållandena hos varje enskild leverantör. Den närmare innebörden får därför avgöras mot bakgrund av resurssituationen hos respektive leverantör. Det får vara en fråga för tillsynsmyndigheten att närmare precisera kravet på medverkan inom viss tid. Vi vill dock framhålla att det är rimligt att utgå från att arbetet med att överföra informationen ska påbörjas inom någon enstaka timme räknat från när leverantören tar emot (i betydelsen blir medveten om) begäran om att trafikuppgifter ska lämnas ut. Det kan också betyda att leverantören behöver arbeta med verkställigheten utanför kontorstid. Frågor om ersättning för leverantörernas arbete behandlas i avsnitt 13.

Överföring ska ske så snart någon uppgift finns tillgänglig. Det kan innebära att det sker överföring vid flera tillfällen. Enligt de brottsbekämpande myndigheterna är det t.ex. mycket värdefullt att en leverantör snabbt börjar lämna de uppgifter som finns omedelbart tillgängliga och sedan kontinuerligt överför samtliga uppgifter allt eftersom de tas fram ur systemen.

7.5 Ändamålen med behandlingen av trafikuppgifter

Förslag: Trafikuppgifter som har lagrats för brottsbekämpande syften får behandlas av leverantörerna endast för att lämnas ut efter beslut om hemlig teleövervakning eller enligt bestämmelserna i lagen om elektronisk kommunikation, eller för att annan fullgör lagringen.

Våra förslag om lagring av trafikuppgifter innebär en avsevärd utvidgning av den mängd trafikuppgifter som kommer att lagras. Den absolut övervägande delen av trafikuppgifterna kommer aldrig att efterfrågas av de brottsbekämpande myndigheterna.

Enligt förslaget kommer trafikuppgifterna att lagras av leverantörerna. Det innebär att det blir leverantörerna som måste anses äga trafikuppgifterna och därmed i princip kunna disponera över dem. Uppgifterna kommer inte att vara omedelbart läsbara hos leverantörerna och i många fall kommer den enskilde leverantören bara att ha viss information som måste ställas samman med lagrad information hos någon annan leverantör för att en enskild persons kommunikation ska kunna utläsas. De lagrade trafikuppgifterna skulle ändå kunna ha ett värde för leverantörerna om de fick behandlas för andra ändamål än vad lagringen är tänkt för. I den allmänna debatten har det framförts farhågor för att leverantörerna ska använda uppgifterna t.ex. för sammanställningar av sociogram eller för att säljas för att behandlas vid marknadsföring. Mot bakgrund av den information om enskildas kommunikationsmönster som de lagrade trafikuppgifterna skulle kunna ge och de integritetsaspekter som gör sig gällande, måste vi överväga om det ska vara tillåtet att använda trafikuppgifterna för annat än brottsbekämpande ändamål.

Direktivet om lagring av trafikuppgifter tar inte ställning till frågan om vem som från civilrättsliga utgångspunkter har rätt till de lagrade trafikuppgifterna. Däremot har direktivet som utgångspunkt att lagringens fullgörande inte medför en oinskränkt rätt att disponera över uppgifterna. Direktivet föreskriver t.ex. en maximal tid för lagringen och att uppgifterna ska förstöras när lagringstiden gått ut. Direktivets artikel 7 synes också utgå från att trafikuppgifter som lagras med stöd av direktivet inte ska kunna behandlas för andra ändamål än de som anges i direktivet. Detta hindrar inte att leverantörer sparar trafikuppgifter för andra tillåtna ändamål enligt 6 kap. LEK, t.ex. abonnentfakturering.

Artikel 29-gruppen har uttryckt farhågor för att uppgifterna ska behandlas för andra än de brottsbekämpande syftena, som t.ex. övervakning av samtliga medborgares dagliga kommunikationsmönster. Enligt gruppen behöver det säkerställas att de uppgifter som lagras inte medför någon storskalig datautvinning avseende rese- och kommunikationsmönster för personer som de brottsbekämpande myndigheterna inte misstänker. Vidare menar gruppen att leverantörerna inte ska ha rätt att bearbeta trafikuppgifter för

andra ändamål än de som anges i direktivet, särskilt inte för egna syften.

Också Europeiska datatillsynsmannen har yttrat att det är viktigt att tillgången till och användningen av trafikuppgifterna begränsas till de syften som anges i direktivet. Enligt datatillsynsmannen måste de lagrade uppgifterna skyddas på lämpligt sätt för att motverka ett felaktigt utnyttjande av dem.

I 6 kap. 5 § LEK finns huvudregeln att trafikuppgifter ska utplånas eller avidentifieras av leverantörerna när de inte längre behövs för att överföra ett elektroniskt meddelande. Lagen tillåter dock att uppgifterna sparas för viss behandling. I avsnitt 2.2 har vi redogjort för de bestämmelserna. I korthet kan nämnas att det huvudsakligen rör abonnentfakturering, betalning av avgifter för samtrafik, marknadsföring av elektroniska kommunikationstjänster, tvistlösning samt verkställighet av beslut om hemlig teleavlyssning eller hemlig teleövervakning. Direktivet om lagring av trafikuppgifter innebär ytterligare ett undantag från grundregeln att trafikuppgifter inte får lagras utan får sparas för ett visst ändamål (artikel 3). De trafikuppgifter som omfattas av vårt förslag i avsnitt 6 ska lagras av leverantörerna under ett år för att finnas tillgängliga vid beslut om hemlig teleövervakning eller vid begäran om utlämnande enligt lagen om elektronisk kommunikation.

Den fråga som nu ska övervägas är om det bör vara tillåtet att behandla trafikuppgifterna för något ytterligare ändamål än för att lämnas ut till brottsbekämpande myndigheter. Mot bakgrund av de stora skillnader som finns mellan leverantörerna både i fråga om verksamhet och volym bedömer vi att både företagsekonomiska skäl, konkurrensskäl och säkerhetsskäl talar för att leverantörerna ska ha möjlighet att anlita annan för att fullgöra lagringen. I sådana fall kan den fysiska utrustningen vara placerad såväl hos den lagringsskyldige leverantören som hos annan. Vi vill framhålla att det inte är själva lagringsskyldigheten och de skyldigheter som följer med denna som kan uppdras åt annan. Den lagringsskyldige leverantören ska aldrig genom ett sådant avtal kunna frånhända sig någon skyldighet mot myndigheter eller enskilda.

Som framgår i avsnitt 2.3.2 regleras leverantörernas tystnadsplikt i bl.a. 6 kap. 20 § LEK. Den bestämmelsen innebär att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till uppgift om abonnemang, innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt elektroniskt meddelande inte obehörigen får föra vidare eller utnyttja

det han fått del av eller tillgång till. Den stora majoriteten av uppgifter som lagringsskyldigheten kommer att omfatta är hemliga i den betydelsen att abonnenten inte har gett sitt samtycke till att uppgifterna lämnas ut (jfr t.ex. öppna telefonnummer).

När telelagen infördes i samband med att verksamheten i Televerket överfördes till Telia AB uttalade regeringen att bestämmelserna om tystnadsplikt i den lagen (motsvarande bl.a. 6 kap. 20 § LEK) skulle utgöra en huvudsaklig motsvarighet till vad som gällde enligt sekretesslagen för Televerkets verksamhet (prop. 1992/93:200 s. 162 ff.). I sekretesslagen anges att den som på grund av anställning eller uppdrag hos myndigheten har deltagit i verksamheten och fått kännedom om uppgiften har tystnadsplikt (se 1 kap. 6 § sekretesslagen). Att tystnadsplikten enligt lagen om elektronisk kommunikation omfattar uppdragstagare i vissa fall framgår även av PTS:s ”Sammanställning av lagstiftning och praxis kring utlämnande av teleuppgifter” från 2006-11-28.

Bestämmelsen om tystnadsplikt utgör därmed inget hinder mot en ordning där leverantören avtalar med annan att fullgöra lagringen. Den som åtar sig att lagra har ett sådant uppdrag av leverantören som innebär att han eller hon kommer att omfattas av tystnadsplikten. Enligt vår bedömning kommer tystnadsplikt att gälla för den stora majoriteten av uppgifter som lagringsskyldigheten omfattar, eftersom abonnenten inte har gett sitt samtycke till att uppgifterna lämnas ut.

En möjlighet för leverantörerna att anlita annan för själva lagringen innebär fördelar för vissa leverantörer. Från rent civilrättsliga utgångspunkter finns det inte något hinder för leverantörerna att träffa sådana avtal. Ett avtal med annan att fullgöra själva lagringen påverkar inte leverantörernas skyldigheter enligt våra förslag och innebär därmed inte några negativa konsekvenser från integritetssynpunkt. Den som åtar sig lagringen blir personuppgiftsbiträde enligt 30 § första stycket PUL.

Våra förslag innebär således att leverantörerna får behandla trafikuppgifter som lagrats för brottsbekämpande syften endast för att lämna ut dem efter beslut om hemlig teleövervakning eller enligt bestämmelserna i lagen om elektronisk kommunikation, eller för att annan fullgör lagringen. Det innebär att all annan behandling av trafikuppgifter är otillåten. Uppgifterna kan således inte användas för kommersiella eller andra ändamål.

Det kan nämnas att det vid EG-domstolen för närvarande pågår ett mål som tar upp frågan huruvida det enligt gemenskapsrätten är tillåtet att lämna trafikuppgifter avseende Internetanvändare till

innehavare av immateriella rättigheter (mål nr C-275/06). Generaladvokaten menar i sitt förslag till avgörande (den 18 juli 2007) att de uppgifter som har lagrats med stöd av direktivet om lagring av trafikuppgifter enbart får lämnas ut för att utreda, avslöja och väcka åtal rörande allvarliga brott och att utlämnande därför inte får ske till innehavare av immateriella rättigheter.

8 Kvalitet och säkerhet

8.1 Sammanfattning av våra förslag och bedömningar

- I lagen om elektronisk kommunikation ska det föras in en bestämmelse som preciserar leverantörernas skyldighet att vidta särskilda tekniska och organisatoriska åtgärder för ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter.
- Tillsynsmyndigheten får efter samråd med Rikspolisstyrelsen och Datainspektionen meddela de verkställighetsföreskrifter som behövs i frågor om säkerhet för trafikuppgifterna.
- Lagring av trafikuppgifter kan ske utanför Sveriges gränser. Personuppgiftslagens bestämmelser om förbud mot överföring av personuppgifter till tredje land är tillräckliga för att upprätthålla integritetsskyddet.
- Den som övertar en lagringsskyldig leverantörs verksamhet, en konkursförvaltare eller en likvidator ska se till att lagringsskyldigheten fullgörs under den återstående lagringstiden.

8.2 Utgångspunkter

Ändamålet med lagring av trafikuppgifter är att uppgifterna ska finnas bevarade under viss tid för att de, när det finns förutsättningar för det, ska kunna användas för utredning om allvarlig brottslighet. För att lagringen ska fungera som det är tänkt samtidigt som skyddet för enskildas integritet hålls på en hög nivå, måste en rad olika frågor som gäller lagringen och skyddet av de lagrade trafikuppgifterna övervägas.

De förslag vi lägger om lagringsskyldigheten innebär att fler trafikuppgifter än i dag kommer att finnas lagrade och att lagringen ska pågå under ett år. Mot den bakgrunden ska vi överväga om det finns anledning att förändra de bestämmelser i rättegångsbalken och lagen om elektronisk kommunikation som preciserar förutsättningarna för att trafikuppgifterna ska kunna lämnas ut till de brottsbekämpande myndigheterna. Vi återkommer till dessa frågor i avsnitt 11.

Systemen för att lagra trafikuppgifter måste vara utformade så att uppgifterna snabbt och säkert kan överföras till myndigheterna. Frågan om leverantörernas skyldigheter att anpassa sina system så att beslut om hemlig teleövervakning kan verkställas m.m. regleras i 6 kap. 19 § LEK. Vi har i avsnitt 7 behandlat frågorna om vilka leverantörer som ska vara skyldiga att lagra trafikuppgifter och på vilket sätt leverantörerna ska anpassa sin verksamhet för att utan dröjsmål kunna medverka vid verkställighet.

Det som nu ska övervägas är vilka krav som bör ställas så att rätt trafikuppgifter lagras med en teknik som innebär att uppgifterna är skyddade under lagringstiden men också när de förs över till de brottsbekämpande myndigheterna. Det är således inte frågan om en anpassning av systemen som tar sikte på verkställigheten av beslut om hemlig teleövervakning utan vilka krav som bör ställas på att lagringen bl.a. sker med sådan teknisk kvalitet att de uppgifter som finns lagrade är säkrade för att kunna lämnas ut i den mån de efterfrågas av de brottsbekämpande myndigheterna.

Både skyddet för enskildas integritet och hänsynen till näringslivets affärsförhållanden kräver överväganden om hur de trafikuppgifter som lagras av leverantörerna bör vara skyddade så att de inte kan ändras eller behandlas för andra ändamål än de avsedda genom obehörig eller olaglig åtkomst. Lagrade trafikuppgifter ska således inte kunna missbrukas genom att de stjäls, lämnas ut obehörigen eller sprids av misstag t.ex. på grund av tekniskt fel eller olyckshändelse.

För att lagringen av trafikuppgifter ska ha den säkerhet som krävs för en hög tillit till systemet och lagringen utföras så att både integritetsskyddet och effektiviteten tillgodoses måste både det tekniska och organisatoriska skyddet vara tillräckligt, samtidigt som de rättsliga regler som blir tillämpliga om trafikuppgifter ändå skulle komma att spridas i strid mot lagen verkar tillräckligt avhållande och reparativa. En säker lagring av trafikuppgifter behöver

därför övervägas utifrån tekniska, administrativa, straffrättsliga, civilrättsliga och förvaltningsrättsliga utgångspunkter.

Vi kommer i det följande att analysera vilket skydd som nuvarande regler innebär för lagrade trafikuppgifter och överväga behovet av nya regler. I detta avsnitt behandlar vi frågor som gäller kvalitet hos de lagrade uppgifterna och den tekniska säkerhet som krävs för att skydda uppgifterna. Det straff- och skadeståndsrättsliga skyddet och tillsynsfrågor tas upp i avsnitt 9 och 10.

8.3 Kraven på kvalitet och säkerhet

8.3.1 Leverantörernas ansvar

Direktivet innehåller flera artiklar som syftar till en säker lagring. Det anges att lagrade trafikuppgifter ska vara av samma kvalitet och vara föremål för samma säkerhet och skydd som uppgifterna i nätverket (artikel 7 a). Dessutom ska uppgifterna omfattas av lämpliga tekniska och organisatoriska åtgärder för att skyddas mot oavsiktlig eller olaglig förstöring, oavsiktlig förlust eller oavsiktlig ändring, eller otillåten eller olaglig lagring av, behandling av, tillgång till eller avslöjande av uppgifterna (artikel 7 b). Uppgifterna ska också omfattas av lämpliga tekniska och organisatoriska åtgärder för att säkerställa att endast särskilt bemyndigad personal får tillgång till lagrade uppgifter (artikel 7 c).

En grundförutsättning för att syftet med lagring av trafikuppgifter ska uppnås är att rätt trafikuppgifter lagras med hjälp av en teknik som håller hög kvalitet och säkerhet. Det innebär att lagringen ska ske med minst samma kvalitet, säkerhet och skydd som uppgifterna i nätverket. Tekniken måste vara konstruerad så att de uppgifter som lagras inte kan ändras i systemet. Med en tillräckligt hög kvalitet i dessa avseenden tillgodoses direktivets krav på att lagrade trafikuppgifter ska vara korrekta och tillgängliga samtidigt som ett högt integritetsskydd för lagrade uppgifter uppnås.

Som vi har utformat våra förslag blir det leverantörerna som får ansvaret för att lagringen av trafikuppgifter är förenlig med de krav på kvalitet och säkerhet som direktivet ställer. Det innebär att leverantörerna måste ha en god kännedom om vilka trafikuppgifter som ska lagras, ha en tillräckligt stor lagringskapacitet, ha tekniska lösningar som innebär att lagrade trafikuppgifter har samma kvali-

tet som uppgifterna i nätverket och en driftsäkerhet som minimerar risken för att uppgifterna förstörs, förloras eller förvanskas.

För att systemet ska fungera och för att medborgarna ska kunna ha förtroende för att lagrade trafikuppgifter enbart behandlas när det är tillåtet och lämnas ut endast i de förhållandevis mindre antal fall där de används för att bekämpa allvarlig brottslighet, behövs det regler som tar sikte på risken för otillåten eller obehörig åtkomst. Det innebär att de lagrade trafikuppgifterna måste skyddas inte bara genom tekniska lösningar utan också genom organisatoriska och administrativa åtgärder som begränsar enskilda personers tillgång till uppgifterna. Primärt är skyddet således ett ansvar för leverantörerna. Ytterst blir det dock en fråga om ett straffrättsligt och skadeståndsrättsligt skydd för uppgifterna. Vi återkommer till de frågorna i avsnitt 9.

Både den tekniska utvecklingen och förändringar på marknaden för elektronisk kommunikation medför att leverantörernas åtgärder för kvalitet och säkerhet hela tiden måste följas upp och definieras med bl.a. föreskrifter av olika slag. Vi redovisar i avsnitt 10.4 våra överväganden i fråga om vilken eller vilka myndigheter som bör ha tillsyn över att regelsystemet följs och hur tillsynen bör utformas.

8.3.2 Nuvarande reglering

Enligt de regler som gäller i dag får trafikuppgifter i princip lagras endast i syfte att säkerställa att avtalsförhållandet mellan leverantör och kund fullgörs. I praktiken lagras uppgifter som behövs för att leverantören ska kunna få betalt av kunden. Det ligger därför i leverantörernas intressen att lagra just sådan information och att hålla en kvalitets- och säkerhetsnivå som svarar mot detta. Leverantörerna har också av konkurrensskäl ett starkt incitament att hålla en hög nivå på säkerhetsskyddet.

Regler om teknisk säkerhet finns i dag i 5 kap. 6 a § och 6 kap. 3 § LEK. Bestämmelsen i 5 kap. 6 a § LEK gäller driftsäkerheten i leverantörernas system. Av bestämmelsen framgår att den som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster ska se till att verksamheten uppfyller rimliga krav på god funktion och teknisk säkerhet samt har uthållighet och tillgänglighet vid extraordinära händelser i fredstid. Det innebär att systemen ska vara byggda så att störningar

i normal drift eller vid extraordinära händelser inte leder till oacceptabla avbrott eller andra problem med driften och att konsekvenserna av inträffade avbrott eller driftstörningar minimeras. PTS har utfärdat allmänna råd i fråga om kravet på driftsäkerhet (PTSFS 2007:2). Av råden framgår att leverantörerna bör bedriva ett kontinuerligt och systematiskt säkerhetsarbete i vilket delmomenten riskanalys, riskhantering, planering för avbrott och störningar samt uppföljning av inträffade avbrott och störningar bör finnas. Råden innebär att leverantörerna ska ha en säkerhetspolicy och en säkerhetsorganisation etc. som garanterar en tillräcklig säkerhetsnivå.

Bestämmelsen i 6 kap. 3 § LEK gäller inte driftsäkerhet utan avser det integritetsskydd som ska upprätthållas. I bestämmelsen anges att den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst 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. Den som tillhandahåller ett allmänt kommunikationsnät ska vidta de åtgärder som är nödvändiga för att upprätthålla samma skydd i nätet. Av förarbetena framgår inte närmare vilka åtgärder som ska vidtas (prop. 2002/03:110). I artikel 4.1 i direktivet om integritet och elektronisk kommunikation, som genomförs i 6 kap. 3 § LEK, anges att det är tekniska och organisatoriska åtgärder som avses.

Uttrycket tekniska och organisatoriska åtgärder förekommer i 31 § PUL. Enligt den bestämmelsen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

Eftersom personuppgiftslagen är subsidiär till annan lagstiftning (2 § PUL) och 6 kap. 3 § LEK tar sikte på integritetsskyddet torde 31 § PUL inte vara direkt tillämplig för leverantörerna avseende hantering av trafikuppgifter (jfr 6 kap. 2 § LEK). För vår bedömning av hur kravet på säkerhet bör bestämmas är det dock av intresse hur lagstiftaren resonerade när personuppgiftslagen infördes. I förarbetena till personuppgiftslagen anges att uppräkningen är all-

mänt hållen och kortfattad men att den på ett bra sätt beskriver de överväganden som måste göras i fråga om säkerhetsåtgärder (prop. 1997/98:44 s. 92 och SOU 1997:39 s. 409 f.). Ett exempel på de särskilda risker som finns vid behandlingen av personuppgifter anges vara antalet personer som de behandlade uppgifterna avser. Det anges att skadorna givetvis kan bli mer omfattande när det är uppgifter om många personer som behandlas på en gång och att en angripare kan vara beredd att lägga ned mer resurser på ett intrång om han på en gång kan komma åt uppgifter om många personer. Vidare anges att det väsentliga är att en lämplig säkerhetsnivå uppnås oavsett om det sker genom tekniska eller organisatoriska åtgärder, dvs. målet är det viktiga och inte vilka medel som används för att nå dit, och att det alltid måste bli fråga om en avvägning för att åstadkomma en lämplig säkerhetsnivå. Enligt förarbetena ger de allmänt hållna reglerna inte tillräcklig vägledning i det enskilda fallet utan avsikten är att Datainspektionen ska meddela de närmare föreskrifter om säkerhetsåtgärder som behövs.

Datainspektionen har utfärdat allmänna råd, Säkerhet för personuppgifter, som preciserar personuppgiftslagens krav på säkerhet vid behandling av personuppgifter. Av råden framgår bl.a. att en organisation med fungerande administrativa rutiner är väl så viktig som tekniska lösningar och att den bästa tekniken inte behöver användas för att uppnå lämplig säkerhetsnivå om det skulle kosta för mycket. Vidare framgår av råden att tillträdeskontroll, behörighetskontroll och behandlingshistorik för viss tid bör finnas för att säkerställa att endast behörig personal får tillgång till uppgifterna.

PTS har inte utfärdat några motsvarande allmänna råd för marknaden för elektronisk kommunikation.

8.3.3 Leverantörernas nuvarande säkerhetsarbete

För vår bedömning av vilka tekniska och organisatoriska åtgärder som krävs för ett fullgott skydd är det nuvarande säkerhetsarbetet hos leverantörerna en bra utgångspunkt. De leverantörer som är representerade i utredningen har redovisat viss del av säkerhetsarbetet för oss. Redovisningen har dock av både konkurrensskäl och säkerhetsskäl inte kunnat beskriva säkerhetsarbetet i detalj.

Av de uppgifter vi har fått framgår att leverantörerna anser sig ha ett i stort sett väl utbyggt och fungerande säkerhetsarbete. Detta gäller särskilt de stora leverantörerna. En starkt bidragande orsak

till detta är konkurrensskäl. Kvalitet och säkerhet utgör i högsta grad konkurrensfaktorer i leverantörernas tävlan om kunder. Leverantörerna får snabb och tydlig återkoppling från kunderna om det förekommer brister. De trafikuppgifter som leverantörerna i dag lagrar har som huvudsyfte att vara ett underlag i deras affärsverksamhet och framför allt för kunddebitering. Eftersom informationen representerar stora ekonomiska värden för leverantörerna, är de tekniska systemen byggda för mycket hög datasäkerhet och tillförlitlighet. Leverantörernas arbete med säkerheten kan i detalj vara uppbyggd på lite olika sätt, men allt syftar till att eliminera yttre och inre påverkan på de tekniska systemen och informationen. Hos de små leverantörerna kan det finns mindre brister i säkerhetsarbetet. Den största anledningen till detta uppges vara okunskap.

Som en organisatorisk åtgärd till skydd för systemen har leverantörerna tagit fram olika säkerhetsföreskrifter som bl.a. beskriver hur och vilka som ska ha tillgång till systemen, hur säkerhetskopiering ska göras samt vilket skydd utrustningen och informationen ska ha.

Det tekniska skyddet innebär att leverantörerna har ett fysiskt skydd som tar sikte på att systemen ska vara skyddade mot stöld och förstörelse. Det kan vara fråga om t.ex. låsanordningar, larm, extra strömtillförsel och på annat sätt skyddade utrymmen. Det finns också ett IT-tekniskt säkerhetsarbete som tar sikte på säkerheten för både systemen i sig och säkerheten för den information som finns i systemen. Det tekniska skyddet är uppbyggt så att inget ska kunna förstöras, förvanskas eller stjälas. Konkret innebär det att man använder olika former av behörighetskontroll, åtkomstkontroll, behandlingshistorik, loggar och kryptering av information m.m. Genom behörighetskontroller säkerställs att endast personer som behöver hantera trafikuppgifterna för tillåtna ändamål kan använda systemen. Obehörig åtkomst förhindras genom att inloggningen av behörig personal sker i olika steg. Det innebär att användaren bara tillåts ett visst antal misslyckade inloggningsförsök innan han eller hon stängs ute. Systemen är särskilt anpassade för leverantörernas behov och logiskt skilda från varandra. Systemen hanteras enligt en förvaltningsmodell och har en systemägare, en systemförvaltare och en systemadministratör. Systemägaren är kravställare och ytterst ansvarig för systemets funktion. Systemförvaltaren sköter systemet enligt systemägarens krav och systemadministratören sköter den dagliga hanteringen av systemet.

Säkerhetspolisen är en av de myndigheter som för sina utredningar begär ut uppgifter från leverantörerna. Säkerhetspolisens uppdrag är att förebygga och avslöja brott mot rikets säkerhet, bekämpa terrorism och skydda den centrala statsledningen. När Säkerhetspolisen begär ut uppgifter som från säkerhetssynpunkt har betydelse för rikets säkerhet eller för skyddet mot terrorism ställs det särskilda krav på säkerhet hos leverantörerna så att uppgifterna behandlas på ett betryggande sätt. Detta sker med stöd av säkerhetsskyddslagen (1996:627). De krav som Säkerhetspolisen kan ställa är att en säkerhetsprövning ska göras innan en person genom anställning eller på något annat sätt deltar i en viss verksamhet hos leverantören. Prövningen enligt 11 § säkerhetsskyddslagen ska klarlägga om personen kan antas vara lojal mot de intressen som skyddas och i övrigt pålitlig från säkerhetssynpunkt. Säkerhetsprövningen enligt säkerhetsskyddslagen omfattar registerkontroll och under vissa förutsättningar särskild personutredning. De säkerhetskrav som ställs på leverantörerna vid verkställighet av hemliga tvångsmedel preciseras sedan i ett avtal (säkerhetsskyddsavtal, s.k. SUA-avtal) som träffas mellan Säkerhetspolisen och leverantören.

I de fall leverantörer har slutit säkerhetsskyddsavtal med Säkerhetspolisen sker som regel hanteringen av trafikuppgifter även till andra brottsbekämpande myndigheter i enlighet med innehållet i de avtalen. Det innebär att organisationen kring all hantering och utlämnande av uppgifter följer den säkerhetsnivå som säkerhetsskyddsavtalet ställer upp.

8.4 Lagregleringen av säkerheten för lagrade trafikuppgifter m.m.

Förslag: I lagen om elektronisk kommunikation ska det föras in en bestämmelse som preciserar leverantörernas skyldighet att vidta särskilda tekniska och organisatoriska åtgärder för ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter.

Tillsynsmyndigheten får efter samråd med Rikspolisstyrelsen och Datainspektionen meddela de verkställighetsföreskrifter som behövs i frågor om säkerhet för trafikuppgifterna.

Bestämmelsen i 5 kap. 6 a § LEK och den tillsyn som PTS bedriver inom det området syftar till att allmänna kommunikationsnät och

allmänt tillgängliga elektroniska kommunikationstjänster ska uppfylla rimliga krav på god funktion och teknisk säkerhet. Bestämmelsen gäller inte enbart vid extraordinära händelser utan tillgodoser kravet på driftsäkerhet även vid andra driftavbrott. I de bedömningar vi gör nedan utgår vi från att driften är säker.

Direktivet om lagring av trafikuppgifter anger att lagrade uppgifter ska vara av samma kvalitet och vara föremål för samma säkerhet och skydd som uppgifterna i nätverket, att uppgifterna ska omfattas av lämpliga tekniska och organisatoriska åtgärder för att skyddas mot oavsiktlig eller olaglig förstöring, oavsiktlig förlust eller oavsiktlig ändring, eller otillåten eller olaglig lagring av, behandling av, tillgång till eller avslöjande av uppgifterna, och att uppgifterna ska omfattas av lämpliga tekniska och organisatoriska åtgärder för att säkerställa att endast särskilt bemyndigad personal får tillgång till lagrade uppgifter (artikel 7 a–7 c).

Den nuvarande bestämmelsen i 6 kap. 3 § LEK tar sikte på ett grundskydd för behandlingen av trafikuppgifter. Bestämmelsen reglerar kraven på säkerhet för de uppgifter som får sparas enligt nuvarande regler, dvs. i princip endast de trafikuppgifter som behövs för att säkerställa att avtalsförhållandet mellan leverantör och kund fullgörs.

Den lagringsskyldighet som vi föreslår har ett helt annat syfte och ska åstadkomma att trafikuppgifter som sammanställs av en brottsbekämpande myndighet kan ge svar på frågorna om vem som kommunicerat med vem, när det skedde, var de som kommunicerade med varandra befann sig och vilken typ av kommunikation som användes vid tillfället. Det innebär att lagringen av trafikuppgifter för brottsbekämpningssyften blir både mer omfattande och mer integritetskänslig. Det medför att kravet på säkerhet bör vara högre för de trafikuppgifter som lagras enligt våra förslag och att nivån på den säkerhet som bör gälla för uppgifterna bör preciseras i lagen om elektronisk kommunikation.

Trafikuppgifter är ofta personuppgifter. Nivån på det skydd som bör finnas för trafikuppgifterna bör därför utformas med utgångspunkt i det skydd för personuppgifter som anges i personuppgiftslagen. I den bestämmelse vi föreslår bör kravet på säkerhet för trafikuppgifterna uttryckas så att leverantörerna ska vidta de särskilda tekniska och organisatoriska åtgärder som är tillräckliga för att säkerställa att behandlade uppgifter skyddas. I detta ligger att uppgifterna ska vara tillförlitliga, ha tillräckligt hög kvalitet och ett tillräckligt skydd mot intrång och annan otillåten behandling.

I säkerheten och skyddet för personlig integritet ligger att leverantörerna ska känna till vilka trafikuppgifter som omfattas av lagringsskyldigheten och hur lagringen i övrigt ska utformas. Det ligger i tillsynsmyndighetens uppgift att informera om omfattningen av leverantörernas skyldigheter. Hur den säkerhet som uttrycks i lagen om elektronisk kommunikation mer preciserat bör uppnås beror bl.a. på den teknik de olika leverantörerna har och på teknikutvecklingen. Det bör vara en uppgift för tillsynsmyndigheten att mot bakgrund av teknikutvecklingen och leverantörernas fortlöpande säkerhetsarbete fastställa nivån på säkerheten genom föreskrifter. Föreskrifterna bör tas fram efter samråd med Rikspolisstyrelsen och Datainspektionen. Den slutliga bedömningen av om de vidtagna åtgärderna är tillräckliga kommer att ske genom tillsynsåtgärder i enskilda fall. Det är viktigt att framhålla att leverantörerna är skyldiga att lagra trafikuppgifterna med den säkerhet som förutsätts redan när lagstiftningen träder i kraft. Vi återkommer till frågan om tillsynsmyndighetens befogenheter i avsnitt 10.5.

8.5 Överföring av personuppgifter till annat land

Bedömning: Lagring av trafikuppgifter kan ske utanför Sveriges gränser. Personuppgiftslagens bestämmelser om förbud mot överföring av personuppgifter till tredje land är tillräckliga för att upprätthålla integritetsskyddet.

Inom området för elektronisk kommunikation kan en och samma leverantör verka i flera länder. Det innebär att lagringen av trafikuppgifter som har genererats i Sverige kan förläggas till ett annat land och att trafikuppgifter som har genererats i ett annat land kan lagras i Sverige. Enligt vårt förslag är en leverantör som har sådan verksamhet i Sverige som medför anmälningsskyldighet enligt 2 kap. 1 § LEK också lagringsskyldig. Även om lagringen förläggs utomlands gäller leverantörens alla skyldigheter enligt de bestämmelser som anger hur lagringsskyldigheten ska fullgöras, t.ex. skyldigheten som rör säkerheten för de lagrade trafikuppgifterna. Om en utländsk leverantör inte är anmälningspliktig för verksamhet i Sverige utan enbart förlägger sitt lager av trafikuppgifter här i landet gäller inte den svenska regleringen för lagring av trafikuppgifter. Däremot kan leverantörens hantering av uppgifterna i lagret komma att omfattas av t.ex. bestämmelserna i personuppgiftslagen

om hanteringen innebär behandling av sådana trafikuppgifter som är personuppgifter.

Även om en lagringsskyldig leverantör, som har lagret utomlands, fullgör sina skyldigheter enligt svensk lag, kan lagringslandets regler om t.ex. tvångsmedel bli tillämpliga på uppgifterna i lagret. Huruvida uppgifter som finns i ett lager i ett annat land kan få spridning utöver vad som följer av svensk rätt beror på den rättsliga regleringen i landet där lagret finns. Det finns med andra ord inte någon garanti för att uppgifter som lagras i ett annat land inte används för andra ändamål än de som den svenska lagstiftningen medger utöver den garanti som ligger i att samtliga medlemsländer i EU har rättsregler för dataskydd m.m. som bygger på EG-direktiv. Säkerhetspolisen har pekat på att detta förhållande kan innebära att information som har stor betydelse för rikets säkerhet kan bli åtkomlig i andra länder.

Vi inser att det finns avsevärda komplikationer som gäller rikets säkerhet och också skyddet för enskildas integritet om trafikuppgifter som har genererats här lagras i ett annat land. Samtidigt är ett av de grundläggande syftena bakom direktivet om lagring av trafikuppgifter att slå vakt om den fria rörligheten inom området för elektronisk kommunikation mellan EU-länderna. I de länder där direktivet redan har införts har det inte enligt vad vi har fått uppgift om införts några begränsningar som gör att trafikuppgifter inte får lagras i ett annat medlemsland. Vi bedömer att direktivet om lagring av trafikuppgifter inte ger något utrymme för att begränsa leverantörernas möjligheter att förlägga lagret av trafikuppgifter till ett annat EU-land.

Personuppgiftslagen innehåller bestämmelser som begränsar möjligheterna att förlägga lagringen av trafikuppgifter som är personuppgifter till tredje land. Enligt 33 § PUL är det förbjudet att till tredje land (dvs. ett land som varken ingår i EU eller är anslutet till EES-samarbetet) föra över personuppgifter som är under behandling eller att föra över uppgifterna för behandling i ett sådant land, om landet inte har en adekvat nivå för skyddet av personuppgifterna. Frågan om en adekvat skyddsnivå föreligger ska bedömas med hänsyn till samtliga omständigheter som har samband med överföringen. Särskild vikt ska läggas vid uppgifternas art, ändamålet med behandlingen, hur länge behandlingen ska pågå, ursprungslandet, det slutliga bestämmelselandet och de regler som finns för behandlingen i det tredje landet.

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

Regeringen eller den myndighet som regeringen bestämmer får enligt 35 § PUL meddela undantag från förbudet att föra över personuppgifter till tredje land. Enligt samma bestämmelse får regeringen meddela föreskrifter om att överföring av personuppgifter till tredje land är tillåten, om överföringen regleras av ett avtal som ger tillräckliga garantier till ett skydd för de registrerades rättigheter.

Regeringen har föreskrivit att personuppgifter får föras över till tredje land om och i den utsträckning EG-kommissionen har konstaterat att landet har en adekvat nivå för skyddet av personuppgifter. Vilka de länderna är anges i en bilaga till personuppgiftsförordningen. Vidare har regeringen bestämt att Datainspektionen får meddela beslut om undantag i enskilda fall om det finns tillträckliga garantier till skydd för de registrerades rättigheter (13 och 14 §§ personuppgiftsförordningen [1998:1191]). Information i frågan om överföring av uppgifter får ske kan lämnas av Datainspektionen.

Vi bedömer att personuppgiftslagens bestämmelser om förbud mot överföring av personuppgifter till tredje land är tillräckliga för att upprätthålla integritetsskyddet för den enskilde. Sammantaget innebär våra överväganden att vi inte ser att leverantörernas möjligheter att förlägga lagret utanför Sverige kan begränsas i förhållande till andra medlemsländer i EU eller länder ansluta till EES-avtalet och inte heller utöver vad som följer av bestämmelserna i 33 och 34 §§ PUL.

8.6 Ansvaret vid verksamhetsövergång m.m.

Bedömning: Den som övertar en lagringsskyldig leverantörs verksamhet, en konkursförvaltare eller en likvidator ska se till att lagringsskyldigheten fullgörs under den återstående lagringstiden.

En särskild fråga är vad som ska ske med de lagrade trafikuppgifterna när en leverantörs verksamhet som omfattar lagringsskyldig-

het övergår till annan eller upphör. Även då måste lagringsskyldigheten fullgöras. Det får inte bli så att de brottsbekämpande myndigheterna står utan möjlighet att komma åt uppgifterna för att de exempelvis har utplånats före lagringstidens slut. Likaså måste t.ex. kraven på kvalitet och säkerhet för de lagrade trafikuppgifterna upprätthållas. Frågan är med andra ord viktig såväl ur ett brottsbekämpnings- som ett integritetsskyddsperspektiv och blir främst aktuell om en verksamhet övergår genom försäljning eller fusion, och om leverantören försätts i konkurs eller likvidation.

De bestämmelser vi föreslår innebär bl.a. att den lagringsskyldige ska se till att trafikuppgifter lagras under ett år, att uppgifterna utplånas efter den tiden och att åtgärder vidtas för att säkerställa att de behandlade uppgifterna skyddas. Det följer av de regler vi föreslår att skyldigheterna rörande exempelvis lagringstid, utplånande och skyddsåtgärder övergår till den som övertar verksamheten om verksamheten även fortsättningsvis träffas av lagringsskyldigheten, dvs. om leverantören är anmälningspliktig enligt 2 kap. 1 § LEK. En konkurs eller likvidation innebär inte i sig att lagringsskyldigheten upphör. Den som under ett sådant förfarande företräder den lagringsskyldige, i första hand konkursförvaltaren respektive likvidatorn, har att se till att skyldigheterna fullgörs under den återstående lagringstiden, bl.a. att uppgifterna lagras under ett år och utplånas därefter. Både när verksamheten övergår och upphör kan lagringen fullgöras genom att någon anlitas för det ändamålet (se avsnitt 7.5). De nu angivna förhållandena följer av de regler som redan gäller och behöver inte regleras särskilt i lagen om elektronisk kommunikation.

9 Det straff- och skadeståndsrättsliga skyddet

9.1 Vår sammanfattande bedömning

- Lagringen av trafikuppgifter ger inte anledning att förändra några straff- eller skadeståndsrättsliga bestämmelser.
- Det kan övervägas om det behövs en bestämmelse om grovt dataintrång med en strängare straffskala.

9.2 Direktivet om lagring av trafikuppgifter

I avsnitt 7.5 har vi föreslagit att leverantörerna ska få behandla de trafikuppgifter som lagras enligt vårt förslag endast för vissa klart angivna ändamål. Dit hör att uppgifterna får behandlas för att lämnas ut efter beslut om hemlig teleövervakning eller enligt bestämmelserna i lagen om elektronisk kommunikation, eller för att annan fullgör lagringen. Vi har i avsnitt 8 redovisat våra överväganden i fråga om den säkerhetsnivå som bör gälla för leverantörernas behandling av trafikuppgifterna och deras ansvar för att vidta särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter.

För att skyddet mot integritetsintrång för enskilda ska vara tillräckligt starkt måste också de straff- och skadeståndsrättsliga reglerna verka avhållande samtidigt som de, om skador ändå inträffar, innebär en tillräcklig straffrättslig reaktion och ett skadeståndsrättsligt skydd för den som drabbas.

Direktivet om lagring av trafikuppgifter anger i artikel 13 att medlemsstaterna ska säkerställa att rättslig prövning, ansvar och sanktioner finns till skydd för uppgifterna. Medlemsstaterna ska särskilt vidta nödvändiga åtgärder för att säkerställa att förbjuden tillgång till eller överföring av lagrade uppgifter beläggs med sank-

tioner, inbegripet administrativa eller straffrättsliga sanktioner, som är effektiva, proportionerliga och avskräckande.

Straffbestämmelser som skyddar enskildas integritet finns i ett flertal författningar. Vad som främst är aktuellt att behandla i detta sammanhang är vissa regler i 4 och 20 kap. brottsbalken, i personuppgiftslagen och i lagen (1990:409) om skydd för företagshemligheter.

Straffansvaret är personligt och innebär att endast fysiska personer som begått en straffbar handling kan dömas. Den lagringsskyldighet vi föreslår ska fullgöras av den som är anmälningspliktig enligt lagen om elektronisk kommunikation. Det innebär att trafikuppgifter alltid kommer att lagras inom ramen för en näringsverksamhet. En otillåten behandling av trafikuppgifter kan därmed också bli att bedöma utifrån de sanktioner som kan åläggas näringsidkaren enligt reglerna om företagsbot och förverkande i 36 kap. brottsbalken.

De skadeståndsbestämmelser som kan bli aktuella vid lagring av trafikuppgifter finns i lagen om elektronisk kommunikation, personuppgiftslagen, lagen om skydd för företagshemligheter och skadeståndslagen (1972:207).

9.3 Skyddet i de straff- och skadeståndsrättsliga bestämmelserna

9.3.1 Straffrätten

Dataintrång m.m.

I 4 kap. brottsbalken finns bestämmelser om brott mot frihet och frid. Enligt 4 kap. 8 § brottsbalken är det straffbart som brytande av telehemlighet att olovligen bereda sig tillgång till ett telemeddelande. Paragrafen skyddar med andra ord innehållet i ett telemeddelande och inte trafikuppgifterna i sig. Den bestämmelsen blir alltså inte aktuell i detta sammanhang. Även 4 kap. 9 § brottbalken om intrång i förvar skyddar innehållet i ett meddelande från att någon olovligen tar del av det. Även om också annat än meddelanden skyddas bedömer vi att paragrafen inte blir aktuell i fråga om skyddet av de lagrade trafikuppgifterna. Detsamma gäller olovlig avlyssning enligt 4 kap. 9 a § brottsbalken.

Ett förfarande som innebär att någon olovligen bereder sig tillgång till trafikuppgifter blir närmast att bedöma enligt 4 kap. 9 c § brottsbalken om dataintrång. Bestämmelsen lyder på följande sätt.

> Den som i annat fall än som sägs i 8 och 9 §§ 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 döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift.

Alla uppgifter (fakta, information eller begrepp) som uttrycks i en för en dator anpassad och läsbar form omfattas av bestämmelsen, således även trafikuppgifter och oavsett om dessa innehåller personuppgifter eller inte. Det har ingen betydelse var uppgifterna finns i systemet eller på vilket datamedium de finns. Även om själva tillgången till uppgiften är lovlig, är det straffbart att olovligen ändra, utplåna eller blockera eller i register föra in uppgift som är avsedd för automatiserad behandling. Att blockera en uppgift innebär att uppgiften görs oåtkomlig eller att den hindras från att flöda. Exempel på det är inmatning eller spridning av olika typer av sabotageprogram (datavirus, trojaner eller logiska bomber). Med register avses information som på något sätt har systematiserats, som t.ex. tabeller, kataloger och filer. Däremot avses inte löpande text. Skyddet gäller oavsett om effekten av den olovliga förändringen är tillfällig eller bestående. Som framgår av bestämmelsens andra mening finns ett straffansvar även för den som olovligen genom liknande åtgärd som i första meningen allvarligt stör eller hindrar användningen av en uppgift som är avsedd för automatiserad behandling. Det gäller exempelvis s.k. tillgänglighetsattacker eller överbelastningsattacker.

Bestämmelsen om dataintrång blir således tillämplig om någon utomstående olovligen vidtar åtgärder som innebär att han eller hon bereder sig tillgång till de lagrade trafikuppgifterna, ändrar i uppgifterna, förstör uppgifter eller för in uppgifter i leverantörens lager. Här bortser vi från de övriga brott som kan begås i sådana sammanhang, t.ex. skadegörelse enligt 12 kap. 1 § brottsbalken.

Vi har föreslagit att leverantörerna ska få behandla de lagrade trafikuppgifterna endast för att lämna ut dem enligt ett beslut om hemlig teleövervakning eller enligt lagen om elektronisk kommu-

nikation eller när annan anlitas för lagringen (se avsnitt 7.5). Det innebär att annan behandling är förbjuden. Av det följer att den hos leverantören som behandlar uppgifterna för andra ändamål olovligen bereder sig tillgång till uppgifterna. Förfarandet kan därmed bli att bedöma enligt bestämmelsen om dataintrång. Skulle det vara fråga om att någon hos leverantören ändrar i uppgifterna, förstör eller utplånar uppgifter eller för in uppgifter som inte ska finnas i lagret blir även detta förfarande att bedöma enligt bestämmelsen om dataintrång. Förfarandet kan också bli att bedöma enligt andra bestämmelser i brottsbalken, t.ex. bestämmelserna om egenmäktigt förfarande och skadegörelse i 8 kap. 8 § respektive 12 kap. 1 § brottsbalken.

Brott mot tystnadsplikten

Den personliga integriteten skyddas bl.a. genom regler om tystnadsplikt. Som framgår på flera ställen i betänkandet regleras tystnadsplikten i det allmännas verksamhet i sekretesslagen. När det gäller tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst regleras tystnadsplikten i 6 kap. 20 § LEK. Den bestämmelsen innebär att leverantörerna har tystnadsplikt i fråga om de trafikuppgifter som ska lagras enligt våra förslag. Bestämmelsen anger att den som i samband med tillhandahållande av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst har fått del av eller tillgång till uppgift om abonnemang eller annan uppgift som angår ett särskilt elektroniskt meddelande inte obehörigen får föra vidare eller utnyttja det han har fått del av eller tillgång till. Straffskalan sträcker sig från böter till fängelse i ett år. Enligt 6 kap. 21 § LEK finns tystnadsplikt även för uppgift som hänför sig till användning av bl.a. hemlig teleövervakning.

Bestämmelserna om tystnadsplikt är straffsanktionerade enligt bestämmelsen i 20 kap. 3 § brottsbalken om brott mot tystnadsplikten. Enligt den bestämmelsen kan den som röjer uppgift som han är skyldig att hålla hemlig enligt lag eller annan författning eller enligt förordnande eller förbehåll som har meddelats med stöd av lag eller annan författning, eller olovligen utnyttjar en sådan hemlighet, dömas för brott mot tystnadsplikten. Straffskalan för brott mot tystnadsplikten är böter eller fängelse i högst ett år. Om brot-

tet begås av oaktsamhet döms till böter. I ringa fall ska dock inte dömas till ansvar.

Skulle någon anställd hos de brottsbekämpande myndigheterna eller hos leverantören uppsåtligen eller av oaktsamhet bryta mot tystnadsplikten och föra vidare eller utnyttja trafikuppgifterna finns alltså ett skydd i bestämmelserna om tystnadsplikt. Tystnadsplikten träffar också andra aktörer, t.ex. den som på uppdrag av leverantören utför delar av tillhandahållandet av nätet eller tjänsten och den som leverantören har anlitat för att lagra uppgifterna (se avsnitt 2.3.2 och 7.5).

I sammanhanget bör också nämnas något om den meddelarfrihet som normalt gäller och som innebär att var och en har rätt att lämna även sekretessbelagd information för offentliggörande i bl.a. tryckt skrift. Meddelarfriheten är i vissa fall begränsad såvitt avser trafikuppgifter (se 1 kap. 1 § tredje stycket tryckfrihetsförordningen och 1 kap. 2 § yttrandefrihetsgrundlagen). Av 16 kap. sekretesslagen framgår att meddelarfriheten inte innebär en rätt att lämna information som omfattas av 5 kap. 1 § sekretesslagen och som avser uppgift om hemlig teleövervakning. Det framgår också att den som har tystnadsplikt enligt 6 kap. 20 och 21 §§ LEK inte har meddelarfrihet såvitt avser uppgift om innehållet i ett elektroniskt meddelande eller annan uppgift som angår ett särskilt sådant meddelande samt om hemlig teleövervakning.

Brott mot personuppgiftslagen

Många av de trafikuppgifter som vårt förslag omfattar är samtidigt personuppgifter, dvs. de kan direkt eller indirekt hänföras till en fysisk person som är i livet (3 §).

Straffbestämmelsen i personuppgiftslagen finns i 49 §. Enligt den bestämmelsen är det straffbart att uppsåtligen eller av oaktsamhet bl.a. lämna osann uppgift i information till den som registrerats och i anmälan eller information till tillsynsmyndigheten, att behandla integritetskänsliga personuppgifter i strid med personuppgiftslagens bestämmelser och att lämna ut personuppgifter och integritetskänsliga uppgifter till tredje land i strid med lagen. Straffskalan för brott mot personuppgiftslagen är böter eller fängelse i högst sex månader, eller om brottet är grovt, fängelse i högst två år. I ringa fall döms inte till ansvar.

Det är med andra ord straffbart att behandla trafikuppgifter som är integritetskänsliga personuppgifter i strid med personuppgiftslagen och att föra över trafikuppgifter som är personuppgifter till tredje land om landet inte har en adekvat skyddsnivå för behandling av uppgifterna (se även avsnitt 8.5).

Lagen om skydd för företagshemligheter

Lagen om skydd för företagshemligheter innehåller bestämmelser om straff för den som olovligen bereder sig tillgång till en företagshemlighet eller som på annat sätt tar olovlig befattning med en företagshemlighet. Med företagshemlighet förstås enligt lagen sådan information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för honom i konkurrenshänseende (1 §). Med vissa affärs- eller driftförhållanden avses information om affärshändelser, både enskilda och av allmänt slag. Även information som kan hänföras till pågående drift eller produktion skyddas av lagen liksom information som rör konstruktions- och utvecklingsarbete (prop. 1987/88:155 s. 35).

Information om lagrade trafikuppgifter kan enligt vår bedömning i vissa fall vara sådana företagshemligheter som skyddas av lagen. Den som i sådana fall uppsåtligen bereder sig olovlig tillgång till trafikuppgifterna kan dömas för företagsspionerі och den som anskaffar en företagshemlighet för olovlig befattning med företagshemlighet (4 §).

Företagsbot och förverkande

Företagsbot är en ekonomisk sanktion som under vissa förutsättningar kan åläggas näringsidkare. Förverkande innebär att vinster eller ekonomiska fördelar som har uppkommit hos en näringsidkare eller en enskild till följd av brott kan bli föremål för förverkande till staten enligt allmänna eller särskilda förverkanderegler.

Företagsbot och förverkande kan bli aktuellt t.ex. om leverantören inte har vidtagit särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter (se avsnitt 8.4). Enligt 36 kap. 7 § brottsbalken kan en näringsidkare åläggas företagsbot om brott har begåtts i utöv-

ningen av näringsverksamheten, om det för brottet är föreskrivet strängare straff än penningböter. Det krävs att näringsidkaren inte har gjort vad som skäligen kunnat krävas för att förebygga brottsligheten, eller att brottet har begåtts av antingen en person i ledande ställning eller en person som annars haft ett särskilt ansvar för tillsyn eller kontroll i verksamheten. Enligt 36 kap. 8 § brottsbalken ska företagsboten fastställas till lägst fem tusen kronor och högst tio miljoner kronor.

Om en enskild person gör sig skyldig till brott kan förverkande av vinster ske enligt 36 kap. 1 § brottsbalken. Det är framför allt det fall av förverkande som anges i 36 kap. 4 § brottsbalken som är intressant att beröra här. Har det till följd av ett brott som är begånget i utövning av näringsverksamhet uppkommit ekonomiska fördelar för näringsidkaren, ska värdet av fördelarna förklaras förverkade om det inte är oskäligt.

Bestämmelserna om företagsbot och förverkande blir tillämpliga om trafikuppgifter behandlas på ett otillåtet sätt inom ramen för leverantörens verksamhet. Det innebär att den leverantör som driver näringsverksamhet kan åläggas företagsbot och drabbas av förverkande om någon anställd hos företaget behandlar lagrade trafikuppgifter på ett otillåtet sätt. Om det är leverantören själv som har gjort sig skyldig till brott kan den samlade reaktionen på brottet bli ett personligt straffansvar, företagsbot och förverkande.

9.3.2 Skadeståndsrätten

Lagen om elektronisk kommunikation och personuppgiftslagen

Som framgått tidigare är många av de trafikuppgifter som vårt förslag omfattar samtidigt personuppgifter, dvs. de kan direkt eller indirekt hänföras till en fysisk person som är i livet (3 § PUL).

Lagen om elektronisk kommunikation är främst en näringsrättslig reglering som bl.a. syftar till att enskilda och myndigheter ska få tillgång till säkra och effektiva elektroniska kommunikationer. Lagen innehåller bestämmelser om integritetsskydd (6 kap. LEK) men ingen bestämmelse om skadestånd. Enligt 6 kap. 2 § andra stycket LEK gäller i stället personuppgiftslagens regler om skadestånd vid behandling av personuppgifter enligt lagen om elektronisk kommunikation. Det innebär att skadeståndsbestämmelsen i personuppgiftslagen ska tillämpas när trafikuppgifter som är per-

sonuppgifter behandlas i strid med bestämmelserna i lagen om elektronisk kommunikation. Vid felaktig behandling av trafikuppgifter som inte är personuppgifter blir i stället skadeståndsreglerna i lagen om skydd för företagshemligheter och skadeståndslagen tillämpliga.

Enligt skadeståndsregeln i 48 § PUL ska den registrerade få ersättning för sådan skada eller kränkning av den personliga integriteten som en behandling av personuppgifter i strid med personuppgiftslagen har orsakat. Därutöver ska eventuell personskada, sakskada och ren förmögenhetsskada (ekonomisk skada utan samband med person- eller sakskada) ersättas. Skadeståndsansvaret är i princip strikt. Om den personuppgiftsansvarige visar att felet inte berodde på honom eller henne kan ersättningsskyldigheten dock jämkas till ett skäligt belopp. Bestämmelserna om skadestånd i personuppgiftslagen har karaktären av specialbestämmelse som tar över de allmänna skadeståndsreglerna i skadeståndslagen.

Otillåten eller felaktig behandling av trafikuppgifter som är personuppgifter kan grunda skadeståndsskyldighet för leverantören enligt personuppgiftslagen, om förfarandet strider mot de grundläggande kraven för behandling av personuppgifter enligt 9 § PUL. Enligt den bestämmelsen får personuppgifter samlas in bara för särskilda, uttryckligen angivna och berättigade ändamål och de får inte behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in. Leverantören kan bli skadeståndsskyldig för lagring eller annan behandling som strider mot personuppgiftslagen. Av 9 § PUL följer att leverantörens skyldighet att se till att de personuppgifter som behandlas är riktiga, och att uppgifterna inte lagras under längre tid än vad som är tillåtet, är skadeståndssanktionerad. När det gäller bevarande av uppgifter innehåller lagen om elektronisk kommunikation sedan tidigare särskilda bestämmelser om bl.a. utplåning och avidentifiering. Att behandla uppgifter i strid med dessa regler eller i strid med de bestämmelser om lagring av trafikuppgifter som vi nu föreslår kan därmed grunda skadeståndsskyldighet enligt personuppgiftslagen. För att kunna undvika skadeståndsskyldighet måste leverantören således ha en hög kvalitet i sin lagring och utplåna uppgifterna i enlighet med vårt förslag, dvs. omedelbart vid lagringstidens slut.

Lagen om skydd för företagshemligheter

Lagen om skydd för företagshemligheter innehåller ett flertal bestämmelser om skadestånd. Bl.a. ska den som gör sig skyldig till företagsspionerі eller olovlig befattning med företagshemlighet ersätta den skada som uppkommer genom brottet eller genom att företagshemligheten obehörigen utnyttjas eller röjs (5 §). Skadestånd kan också dömas ut om någon uppsåtligen eller av oaktsamhet utnyttjar eller röjer en företagshemlighet som han i förtroende fått del av i samband med en affärsförbindelse (6 §). Detsamma gäller en anställd som i vissa fall utnyttjar eller röjer en företagshemlighet hos arbetsgivaren som den anställde fått del av i sin anställning (7 §). Den som uppsåtligen eller av oaktsamhet utnyttjar eller röjer en företagshemlighet som angripits kan bli skadeståndsskyldig om han insett eller bort inse detta (8 §).

Skadeståndslagen

De allmänna reglerna i skadeståndslagen blir tillämpliga i den utsträckning det saknas andra regler. Skadeståndslagen är i första hand avsedd för s.k. utomobligatoriska förhållanden, således när det saknas avtal mellan skadevållaren och den skadelidande. För det fall t.ex. personuppgiftslagens bestämmelser eller skadeståndsreglerna i lagen om företagshemligheter inte ger rätt till ersättning kan alltså skadeståndslagen träda in.

I 2 kap. regleras skadeståndsansvaret för olika typer av skador. Har någon av uppsåt eller oaktsamhet orsakat en person- eller sakskada ska den ersättas. En ren förmögenhetsskada ska ersättas om den orsakas genom brott (2 kap. 1 och 2 §§). Likaså ska den som allvarligt kränker någon genom brott som innefattar ett angrepp mot person, frihet eller frid ersätta den skada som kränkningen innebär (2 kap. 3 §). Ersättning för kränkning kan som framgår inte utgå vid alla brott utan är begränsad till brott som utgör ett angrepp på den skadelidandes personliga integritet.

Kränkningsersättning enligt skadeståndslagen kan bli aktuell vid dataintrång om inte skadestånd utgår enligt bestämmelser i annan lag. Även brott mot tystnadsplikten kan ge rätt till kränkningsersättning enligt skadeståndslagen.

Skadeståndslagen innehåller även regler om fördelning av skadeståndsansvar mellan arbetsgivare och arbetstagare, grunderna för

beräkningen av skadeståndet, jämkning och ansvaret vid flera skadevållare.

9.4 Vår bedömning

Bedömning: Lagringen av trafikuppgifter ger inte anledning att förändra några straff- eller skadeståndsrättsliga bestämmelser.

Det kan övervägas om det behövs en bestämmelse om grovt dataintrång med en strängare straffskala.

De straff- och skadeståndsrättsliga regler som vi har beskrivit innebär sammantaget ett skydd både för själva trafikuppgifterna och för enskilda som skadas om uppgifterna hanteras på ett otillåtet sätt.

Även om den nuvarande lagringen av trafikuppgifter främst sker för faktureringsändamål är uppgifterna i flera fall desamma och i många fall lika integritetskänsliga som de trafikuppgifter som kommer att lagras enligt vårt förslag. Skillnaden blir främst att mängden lagrade trafikuppgifter kommer att öka och att många fler typer av uppgifter kommer att lagras. Dessutom kommer lagringen generellt sett att pågå under längre tid än tidigare. Det är mot bakgrund av den skillnaden som vi ska överväga om riskerna för integritetsskador ökar så att det finns ett behov av att göra förändringar i de straff- och skadeståndsrättsliga regler som gäller i dag.

Enligt vår bedömning ligger den främsta risken för integritetsförluster liksom i dag i att trafikuppgifterna på ett otillåtet sätt, genom uppsåtliga handlingar eller på grund av oaktsamhet, skulle spridas, förstöras eller förändras.

De straffrättsliga regler som redan gäller täcker en rad olika situationer där integritetskänsliga uppgifter behandlas i offentlig och privat verksamhet. Enligt vår bedömning täcker bestämmelserna också de olika situationer där trafikuppgifter kan kommas åt på ett otillåtet sätt och missbrukas medvetet eller av oaktsamhet. Vi bedömer att det inte finns något behov av någon ytterligare straffrättslig reglering som tar sikte på att skydda just lagrade trafikuppgifter.

En fråga som dock kan övervägas är om straffskalan i bestämmelsen om dataintrång är tillräcklig. Mot bakgrund av den mängd integritetskänsliga uppgifter som kommer att lagras hos leverantörerna kan ett dataintrång få vittgående följder för både enskilda, företag och viktiga samhällsintressen. Det kan därför diskuteras om

straffskalan är tillräckligt sträng för att en adekvat påföljd ska kunna dömas ut vid grövre brott. Det innebär att en bestämmelse om grovt dataintrång med en strängare straffskala skulle behöva övervägas. Ett sådant övervägande bör dock inte göras enbart utifrån behovet av ett tillräckligt straffrättsligt skydd för lagrade trafikuppgifter utan frågan om bestämmelsen om dataintrång bör ändras bör göras i ett sammanhang där också andra behov och skäl för en lagändring som kan finnas kan övervägas. Vi föreslår därför inte någon ändring av den bestämmelsen.

Den straffrättsliga regleringen innebär också att företagsbot kan bli aktuellt t.ex. om leverantören inte har vidtagit tillräckliga åtgärder för att förebygga brott genom att exempelvis vidta särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter. Om ett brott har inneburit ekonomiska fördelar för leverantören kan värdet eller del av värdet förverkas.

En enskild som skadas på grund av brott kan få skadestånd. Förutom att den enskilde kan få ersättning för person-, sak- eller ren förmögenhetsskada kan ersättning för kränkning dömas ut om skadan orsakas genom dataintrång eller brott mot tystnadsplikten. Om skada orsakas genom brott mot lagen om skydd för företagshemligheter kan den leverantör som skadas få ersättning genom bestämmelser i den lagen.

Skadestånd enligt skadeståndslagen kan också dömas ut på grund av att trafikuppgifter har hanterats oaktsamt eller felaktigt utan att det har varit fråga om ett brott. Skadeståndslagen ger rätt till ersättning om skada har vållats genom oaktsamhet. I dessa fall blir det fråga om ersättning för person-, sak- eller ren förmögenhetsskada. Personuppgiftslagen ger ett betydligt starkare skydd och ger rätt till skadestånd både för kränkning och person-, sak- och förmögenhetsskada om inte den personuppgiftsansvarige visar att felet inte berodde på honom eller henne.

Det straff- och skadeståndsrättsliga systemet kompletteras genom vissa bestämmelser som innebär att en enskild som har anspråk på skadestånd kan få biträde. Om skadeståndsanspråket grundar sig på ett brott kan den skadelidande få sitt skadeståndsanspråk prövat i samband med åtalet och sin skadeståndstalan utförd av åklagare enligt bestämmelserna i 22 och 45 kap. RB. Enligt lagen (1988:609) om målsägandebiträde kan den som är målsägande avseende ett brott enligt 4 kap. brottsbalken under vissa förutsättningar få bistånd av ett målsägandebiträde. Målsägandebiträdet ska ta till-

vara målsägandens intressen och bistå med talan om enskilt anspråk om det inte utförs av åklagaren. I en civilrättslig skadeståndstvist om kränkning kan den enskilde också beviljas rättshjälp enligt bestämmelserna i rättshjälpslagen (1996:1619).

Det straff- och skadeståndsrättsliga systemet kompletteras också av tillsynsverksamheten. Tillsynen bör verka förebyggande så att förhållanden som gör brott möjliga eller medför risker för integriteten på grund av oaktsamhet motverkas. Om olagligheter eller oaktsamheter ändå inträffat kan tillsynsmyndigheten i efterhand vidta åtgärder. Tillsynsmyndigheten har redan i dag flera befogenheter i sin verksamhet, t.ex. kan myndigheten meddela föreläggande och förbud vid vite och ytterst besluta att leverantören ska upphöra med verksamheten. Vi återkommer till tillsynsfrågorna i avsnitt 10.

Vi bedömer att de nuvarande straff- och skadeståndsrättsliga bestämmelserna, som kompletteras av regler som ger enskilde rätt till biträde av åklagare eller annan juridisk hjälp och av tillsynsregleringen, inte behöver förändras i anledning av lagringen av trafikuppgifter. De gällande reglerna ger således enligt vår mening ett skydd mot kränkningar av den personliga integriteten vid otillåten och oaktsam behandling av trafikuppgifter som svarar väl mot direktivets krav på sanktioner, inbegripet administrativa eller straffrättsliga sanktioner, som är effektiva, proportionerliga och avskräckande.

10 Tillsyn

10.1 Sammanfattning av våra förslag och bedömningar

- Post- och telestyrelsen ska ha tillsyn över leverantörernas lagring av trafikuppgifter.
- Datainspektionens tillsyn enligt personuppgiftslagens bestämmelser förändras inte på grund av våra förslag.
- Post- och telestyrelsens nuvarande tillsynsbefogenheter är ändamålsenliga och tillräckliga.

10.2 Direktivet om lagring av trafikuppgifter

Våra förslag innebär att leverantörerna får ansvaret för att de trafikuppgifter som lagras är korrekta och att de är skyddade mot otillåten eller oaktsam behandling och spridning. Det innebär att de som har skyldigheten att lagra också har ett särskilt ansvar för systemets effektivitet, kvalitet och säkerhet. Leverantörernas ansvar för lagringen av trafikuppgifter behöver, inte minst mot bakgrund av den snabba teknikutvecklingen, preciseras och definieras. Det är också viktigt utifrån medborgarnas krav på skydd för den enskildes integritet och deras förväntningar på effektivitet i brottsbekämpningen att systemet följs upp genom en fortlöpande kontroll och tillsyn. Detta fordrar en aktiv tillsynsverksamhet med en tillsynsmyndighet som har god kännedom om regleringen av marknaden för elektronisk kommunikation och samtidigt insikter om hur trafikuppgifter får användas i brottsbekämpningen.

Enligt direktivet om lagring av trafikuppgifter ska medlemsstaterna utse en eller flera behöriga tillsynsmyndigheter som ska övervaka att bestämmelserna om säkerhet för lagrade trafikuppgifter

efterlevs. Den eller de myndigheter som svarar för tillsynen ska vara helt oberoende (artikel 9).

I det följande redogör vi för hur gällande tillsynsreglering ser ut när det gäller trafikuppgifter och personuppgifter och för de överväganden vi gör beträffande vilken eller vilka myndigheter som bör ha tillsyn över lagringen av trafikuppgifter samt vilka befogenheter tillsynsmyndigheten bör ha för att tillsynen ska leda till att trafikuppgifterna lagras med hög kvalitet och säkerhet.

10.3 Gällande tillsynsreglering

10.3.1 Post- och telestyrelsen

PTS utövar tillsyn över verksamhet som bedrivs med stöd av lagen om elektronisk kommunikation. PTS har ett samlat ansvar inom området för elektronisk kommunikation och ska genom sin tillsyn främja tillgången till säkra och effektiva elektroniska kommunikationer enligt de mål som anges i lagen. Vidare ska PTS bl.a. främja en sund konkurrens, övervaka pris- och tjänsteutvecklingen samt följa utvecklingen inom området för elektronisk kommunikation, särskilt vad gäller säkerhet vid elektronisk informationshantering och uppkomsten av eventuella miljö- och hälsorisker. PTS ska pröva frågor om tillstånd och skyldigheter, fastställa och analysera marknader samt pröva tvister enligt lagen om elektronisk kommunikation. PTS ska också vara delaktig i EU-arbetet och annan internationell verksamhet (1, 3, 4 och 9 §§ förordningen [1997:401] med instruktion för Post- och telestyrelsen). Myndighetens tillsynsområde är således relativt stort.

För att utöva tillsyn har PTS rätt att få tillträde till områden, lokaler och andra utrymmen där verksamhet som omfattas av lagen bedrivs. PTS kan efter yttrande från leverantören meddela föreläggande och förbud som får förenas med vite. Sker inte rättelse kan PTS besluta om återkallelse av tillstånd, ändring i tillståndsvillkor eller att en leverantörs verksamhet helt eller delvis ska upphöra. Om en överträdelse utgör ett allvarligt hot mot allmän ordning, allmän säkerhet eller folkhälsan eller kan befaras orsaka allvarliga ekonomiska eller operativa problem för tillhandahållare eller användare av elektroniska kommunikationsnät eller elektroniska kommunikationstjänster får myndigheten, i avvaktan på att ärendet avgörs slutligt, omedelbart meddela förelägganden, återkalla till-

stånd eller ändra tillståndsvillkoren samt besluta att en verksamhet helt eller delvis ska upphöra (7 kap. 1-9 §§ LEK).

PTS får också meddela de verkställighetsföreskrifter som behövs för frågor om anmälan, ansökan, tillstånd, tillsyn och prövning av tvister enligt lagen om elektronisk kommunikation (4 § förordningen om elektronisk kommunikation). Myndigheten har inte använt sig av möjligheten att meddela verkställighetsföreskrifter på nätsäkerhetsområdet.

Beslut som PTS fattar enligt lagen om elektronisk kommunikation eller enligt föreskrifter som meddelas med stöd av lagen får överklagas hos allmän förvaltningsdomstol (8 kap. 19 § LEK). Vid överklagande till kammarrätten krävs prövningstillstånd.

PTS har hittills inte haft något tillsynsärende avseende leverantörernas lagring av trafikuppgifter. Redan år 2004 påbörjades arbetet med direktivet om lagring av trafikuppgifter inom EU, varför PTS bedömde det som olämpligt att i det läget påbörja en sådan tillsyn. PTS saknar därför t.ex. specifik kännedom om hur länge trafikuppgifterna i dagsläget lagras. Myndigheten har inte heller närmare kännedom om vilka uppgifter som leverantörerna lagrar.

PTS har inte sett något behov av att genom föreskrifter reglera vad som ska anses vara en trafikuppgift. Den bedömningen har gjorts mot bakgrund av de många förslag som finns på förändring av lagstiftningen inom området. PTS har inte heller tagit fram några allmänna råd avseende säkerhetsbestämmelser till skydd för integritetsintrång (6 kap. 3 § LEK).

PTS har också tillsyn när det gäller leverantörernas anpassning av systemen så att hemlig teleavlyssning och hemlig teleövervakning kan verkställas (6 kap. 19 § LEK). Eftersom myndigheten inte fått några indikationer på att det skulle finnas några brister har ingen tillsyn, vare sig egeninitierad eller annan, vidtagits på senare tid.

10.3.2 Datainspektionen

Datainspektionen svarar för tillsynen enligt personuppgiftslagen och personuppgiftsförordningen. Inspektionen har till uppgift att bl.a. verka för att människor skyddas mot att den personliga integriteten kränks genom behandling av personuppgifter. Datainspektionen ska följa och beskriva utvecklingen på IT-området när det gäller frågor som rör integritet och ny teknik. Inspektionen har också tillsyn över t.ex. de brottsbekämpande myndigheternas verksamhet när det gäller behandling av personuppgifter.

Datainspektionen har i sin tillsynsverksamhet rätt att på begäran få tillgång till de personuppgifter som behandlas, upplysningar om och dokumentation av behandlingen av personuppgifter och om säkerheten vid behandlingen samt tillträde till sådana lokaler som har anknytning till behandlingen av personuppgifter. Om inspektionen efter en sådan begäran inte kan få tillräckligt underlag för att konstatera att behandlingen av personuppgifter är laglig, får myndigheten vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem. Inspektionen ska också, om den konstaterar att personuppgifter behandlas eller kan komma att behandlas på ett olagligt sätt, genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse. Inspektionen ska i första hand försöka åstadkomma rättelse genom att samtala med berörd organisation och den personuppgiftsansvarige. Går det inte att få rättelse på sådant sätt eller är saken brådskande, får myndigheten vid vite förbjuda den personuppgiftsansvarige att fortsätta att behandla personuppgifterna på annat sätt än genom att lagra dem (43-46 §§ PUL).

Datainspektionens beslut i tillsynsfrågor får överklagas till allmän förvaltningsdomstol. Vid överklagande till kammarrätten krävs prövningstillstånd.

Datainspektionens tillsyn av vilka tekniska och organisatoriska säkerhetsåtgärder som den personuppgiftsansvarige vidtar för att skydda personuppgifter sker utifrån den avvägning som ska göras mellan de tekniska möjligheter som finns, kostnaderna för att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga uppgifterna är. Det medför att utrymmet för generella föreskrifter om vilka säkerhetsåtgärder som bör vidtas är mindre och att tillsynen i stället innebär att Datainspektionen i enskilda fall avgör om vidtagna åtgärder är tillräckliga med beaktande av den lämplighetsavvägning som ska göras. Om Datainspektionen konstaterar att det föreligger brister brukar det räcka med att bristerna påtalas med en uppmaning till den personuppgiftsansvarige att vidta rättelse. Ett föreläggande kan avse vilka konkreta åtgärder som ska vidtas. Det är dock ovanligt att inspektionen utnyttjar sin formella möjlighet att besluta om vilka tekniska och organisatoriska säkerhetsåtgärder som den personuppgiftsansvarige ska vidta.

Behandling av personuppgifter som innebär särskilda risker för otillbörligt intrång i den personliga integriteten ska anmälas för förhandskontroll till Datainspektionen (41 § PUL). I dessa fall har

myndigheten emellanåt använt sig av möjligheten att i förväg fatta beslut om vilka säkerhetsåtgärder som ska vidtas.

Om personuppgifter behandlas på ett olagligt sätt kan Datainspektionen begära att länsrätten förordnar om att personuppgifterna utplånas (47 § PUL).

Datainspektionen har hittills inte behövt använda sig av möjligheten att förena ett föreläggande om rättelse med vite för att åstadkomma rättelse. Inte heller har det förekommit något fall där inspektionen behövt vända sig till länsrätt med en begäran om att uppgifter ska förstöras. Inspektionen har polisanmält olaglig behandling av personuppgifter men det förekommer inte ofta. I de fall inspektionen har gjort en polisanmälan har det vanligtvis handlat om grova integritetskränkningar på Internet som omfattat också andra brott än brott enligt personuppgiftslagen.

10.4 Tillsynsmyndighet för lagringen

Förslag: Post- och telestyrelsen ska ha tillsyn över leverantörernas lagring av trafikuppgifter.

Datainspektionens tillsyn enligt personuppgiftslagens bestämmelser förändras inte på grund av våra förslag.

Enligt direktivet om lagring av trafikuppgifter ska en eller flera offentliga myndigheter utses för att ansvara för att inom landets territorium övervaka att de bestämmelser som genomför direktivet i fråga om uppgiftsskydd och datasäkerhet efterlevs.

Det är PTS som utövar tillsyn över verksamhet enligt lagen om elektronisk kommunikation och som således har tillsyn över leverantörernas verksamhet i dag, bl.a. i fråga om hur trafikuppgifter behandlas.

Datainspektionen har tillsyn över personuppgiftslagens tillämpning. Det innebär att Datainspektionen har tillsyn över både myndigheter och näringsverksamheter när det gäller behandling av personuppgifter.

En viktig utgångspunkt vid bedömningen av vilken eller vilka myndigheter som bör ha tillsynen över lagringen av trafikuppgifter är givetvis den ordning för tillsynen som gäller i dag. Under vårt arbete har det inte framkommit något behov av ett särskilt tillsynsorgan som specifikt skulle utöva tillsyn i fråga om lagring av trafikuppgifter.

Vi föreslår att regleringen avseende lagring av trafikuppgifter ska tas in i lagen om elektronisk kommunikation. Frågan blir då om PTS ska ha tillsynsuppgiften även rörande den lagringsskyldighet vi föreslår. För att tillsynen ska bli effektiv kräver det att tillsynsmyndigheten har kunskap om vilka leverantörer som omfattas av skyldigheten att lagra trafikuppgifter och den verksamhet de annars bedriver. PTS är den myndighet som bäst besitter den kunskapen. PTS har också tillsynsansvar enligt säkerhetsskyddslagen. Det innebär att PTS är den myndighet som ska kontrollera säkerhetsskyddet hos de leverantörer som ingått säkerhetsskyddsavtal (SUA-avtal) med Säkerhetspolisen.

Mot bakgrund av att lagrade trafikuppgifter i många fall är just personuppgifter, skulle det i och för sig kunna övervägas om Datainspektionen ska ha tillsynsansvaret för lagringen. En del av de lagrade uppgifterna kommer dock inte att vara personuppgifter och således en ”främmande” tillsynsuppgift för Datainspektionen. Det framstår inte heller som särskilt effektivt att Datainspektionen som har en generell tillsynsuppgift på personuppgiftsområdet skulle ha tillsyn över ett visst område som gäller marknaden för elektronisk kommunikation när det finns en annan myndighet, PTS, som har tillsynsansvaret i övrigt på detta område.

Vi bedömer att den mest lämpliga ordningen blir att PTS, i enlighet med det tillsynsuppdrag myndigheten redan har, utövar tillsynen över den lagring av trafikuppgifter som följer av våra förslag. Det betyder inte att Datainspektionens uppgift att utöva tillsyn över personuppgiftslagens tillämpning skulle förändras i förhållande till vad som gäller i dag. Det innebär att de båda myndigheternas tillsynsverksamheter delvis kan komma att överlappa varandra. Hur tillsynen i praktiken ska utövas i dessa fall bör, liksom hittills, lösas genom samråd mellan Datainspektionen och PTS.

10.5 Tillsynsmyndighetens befogenheter

Bedömning: Post- och telestyrelsens nuvarande tillsynsbefogenheter är ändamålsenliga och tillräckliga.

Liksom när det gäller den tillsyn som PTS i dag bedriver är det en grundläggande förutsättning för en fungerande tillsyn att initiativ och beslut är väl underbyggda. Därför är det av vikt att tillsynsmyndigheten kan begära in de upplysningar och handlingar som är av intresse för tillsynen. Tillsynsmyndigheten ska ha möjlighet att

förelägga de leverantörer som är lagringsskyldiga att tillhandahålla sådan information. Myndigheten ska vid behov kunna förena förelägganden med vite (7 kap. 3 § LEK).

Myndigheten kan också behöva besluta om tillträde till områden, lokaler och andra utrymmen där verksamhet som omfattas av lagringsskyldigheten bedrivs. Myndigheten ska också ha rätt att begära verkställighet hos kronofogdemyndigheten av beslut (7 kap. 2 § LEK).

Utgångspunkten i PTS nuvarande tillsyn är att det ska vara en god kommunikation mellan tillsynsmyndigheten och leverantören så att myndighetens påpekanden om behov av ändringar efterföljs utan att de påtryckningsmedel som myndigheten har till sitt förfogande behöver användas. Därför ska även fortsättningsvis PTS, när myndigheten misstänker att en leverantör inte efterlever sina skyldigheter, ha möjlighet att underrätta leverantören om detta och ge denne möjlighet att yttra sig. Först därefter bör PTS meddela de förelägganden eller förbud som behövs för att en rättelse ska ske (7 kap. 4 och 5 §§ LEK). Förelägganden och förbud kan förenas med vite. PTS kan också behöva besluta att en verksamhet ska upphöra (7 kap. 5 § LEK). Det är också väsentligt att PTS kan meddela omedelbara provisoriska åtgärder (7 kap. 8 § LEK). Beslut som fattas enligt lagen om elektronisk kommunikation gäller omedelbart, om inte annat har bestämts (8 kap. 22 § LEK). Domstolen har möjlighet att i stället inhibera beslut.

Enligt vår bedömning är de tillsynsbestämmelser som redan finns i lagen om elektronisk kommunikation ändamålsenligt utformade och tillräckliga även för lagringen av trafikuppgifter.

Avslutningsvis ska nämnas att vi i avsnitt 8.4, 13.8.4 och 7.2.3 föreslår att PTS ska få meddela föreskrifter rörande säkerhet och ersättning och medge undantag från lagringsskyldigheten.

11 Myndigheternas tillgång till trafikuppgifter

11.1 Vår sammanfattande bedömning

Bedömning: Lagringen av trafikuppgifter ger inte anledning att förändra bestämmelserna om hemlig teleövervakning respektive utlämnande enligt lagen om elektronisk kommunikation.

11.2 Vårt uppdrag

Enligt våra direktiv är utgångspunkten för vårt arbete att de förutsättningar som gäller i dag för de brottsbekämpande myndigheternas tillgång till trafikuppgifter ska gälla även för de ytterligare trafikuppgifter som kommer att lagras till följd av direktivet.

Syftet med lagringen av trafikuppgifter är enligt direktivet att uppgifterna ska finnas tillgängliga för att kunna lämnas ut och användas vid misstanke om allvarlig brottslighet. Direktivet reglerar vilka uppgifter som ska lagras, hur länge lagringen ska pågå samt frågor om skydd för uppgifterna och tillsyn. Direktivet reglerar däremot inte under vilka förutsättningar som trafikuppgifterna ska kunna lämnas ut till de brottsbekämpande myndigheterna. Förutsättningarna för utlämnande är i stället en fråga för nationell rätt.

I skäl 25 i ingressen i direktivet erinras om att frågor om tillgång till de uppgifter som lagras av nationella myndigheter faller utanför tillämpningsområdet för de europeiska gemenskapernas lagstiftning och om att de nationella reglerna ska respektera de grundläggande rättigheterna i Europakonventionen. Vidare anges bl.a. följande i fråga om de bestämmelser som ger de brottsbekämpande myndigheterna tillgång till trafikuppgifter: ”Enligt den tolkning Europeiska domstolen för de mänskliga rättigheterna gjort av artikel 8 i Europeiska konventionen om skydd för de mänskliga rättig-

heterna och de grundläggande friheterna måste offentliga myndigheters intrång i rätten till privatliv stå i förhållande till vad som är nödvändigt och proportionerligt och därför tjäna närmare angivna, tydliga och legitima syften samt utövas på ett sätt som är rimligt och relevant och som inte är överdrivet i förhållande till syftet med intrånget.”

Vi ska enligt våra direktiv analysera om hänvisningen i direktivet om lagring av trafikuppgifter till Europakonventionen bör medföra ändringar i de förutsättningar som gäller för de brottsbekämpande myndigheternas tillgång till trafikuppgifter i ett enskilt ärende. Enligt ett uttalande från rådet till artikel 1 ska medlemsstaterna ta ”vederbörlig hänsyn” till de brott som förtecknas i den lista som finns i artikel 2 i rambeslutet om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (2002/584/RIF). Vi ska pröva om det mot bakgrund av den utvidgade lagring som blir följden av våra förslag finns anledning att ändra bestämmelserna i rättegångsbalken och i lagen om elektronisk kommunikation om utlämnande av trafikuppgifter. Skulle vi finna att direktivets fokus på allvarlig brottslighet och den koppling som görs till den lista över brott som finns i det nämnda rambeslutet motiverar lagändringar i detta avseende, får vi enligt direktiven föreslå nödvändiga förändringar.

11.3 Förutsättningarna för tillgång till trafikuppgifter

Direktivet om lagring av trafikuppgifter innebär inte att de brottsbekämpande myndigheterna ska få fri tillgång till de uppgifter som lagras. Direktivet reglerar inte alls i vilka fall som myndigheterna ska ha möjlighet att få del av trafikuppgifterna. Direktivets syfte är i stället att se till att, när förutsättningarna finns enligt nationell lagstiftning att lämna ut uppgifter, uppgifterna är ”säkrade” för de brottsbekämpande ändamålen. Syftet med direktivet är alltså att det i fortsättningen inte ska vara en slump beroende på t.ex. den enskilde leverantörens faktureringsrutiner om trafikuppgifterna finns tillgängliga och kan lämnas ut vid utredningar av grövre brott.

Våra förslag om lagringsskyldigheten påverkar inte förutsättningarna för de brottsbekämpande myndigheterna att få trafikuppgifter från leverantörerna med stöd av rättegångsbalken och lagen om elektronisk kommunikation såsom de bestämmelserna är utformade i dagsläget.

Förutsättningarna för *hemlig teleövervakning* enligt 27 kap. 19-21 §§ RB är följande.
1. Det ska finnas en skäligen misstänkt person.
2. Misstanken ska röra
a) brott för vilket inte är föreskrivet lindrigare straff än fängelse i sex månader (även anstiftan och medhjälp),
b) dataintrång, barnpornografibrott som inte är ringa, narkotikabrott eller narkotikasmuggling, eller
c) försök, förberedelse eller stämpling till brott under a) och b).
3. Åtgärden ska vara av synnerlig vikt för utredningen.
4. Åtgärden får avse uppgifter om telemeddelanden som befordras eller har befordrats till eller från teleadresser med viss anknytning till den misstänkte.
5. Åtgärden ska beslutas av domstol.

Förutsättningarna för att få ut trafikuppgifter enligt *6 kap. 22 § första stycket 3 LEK* är följande (i jämförelse med rättegångsbalken).
1. Det behöver inte finnas en skäligen misstänkt person.
2. Det ska vara fråga om brott för vilket inte är föreskrivet lindrigare straff än två års fängelse (även anstiftan och medhjälp).
3. Åtgärden behöver inte vara av synnerlig vikt för utredningen.
4. Åtgärden är inte begränsad till vissa teleadresser men uppgiften ska angå ett särskilt elektroniskt meddelande.
5. Åtgärden beslutas av den brottsbekämpande myndigheten.

Det ska också nämnas att förutsättningarna för att få ut trafikuppgifter i form av uppgift om abonnemang (”kataloguppgifter”) enligt *6 kap. 22 § första stycket 2 LEK* är att fängelse är föreskrivet för brottet och det kan föranleda annan påföljd än böter i det enskilda fallet, dvs. brottet ska vara så allvarligt att det ligger på fängelsenivå.

11.4 Trafikuppgifter lämnas ut för allvarliga brott

För att hemlig teleövervakning ska få användas måste alltså det brott förundersökningen avser ha ett minimistraff på sex månaders fängelse i straffskalan. Det kan vara av värde att ge några exempel på vilka brottstyper som faller under den kategorin. Det rör sig om mord, dråp, grov misshandel, vållande till annans död (enbart grovt brott), människorov, människohandel, olaga frihetsberövande (som inte är mindre grovt), olaga tvång (enbart grovt brott), grov fridskränkning/kvinnofridskränkning, olaga hot (enbart grovt

brott), våldtäkt (som inte är mindre grov), grovt sexuellt tvång, grovt sexuellt utnyttjande av person i beroendeställning, våldtäkt mot barn, grovt sexuellt övergrepp mot barn, grovt koppleri, grov stöld, rån, tillgrepp av fortskaffningsmedel (enbart grovt brott), grovt bedrägeri, utpressning (enbart grovt brott), ocker (enbart grovt brott), häleri (enbart grovt brott), penninghäleri (enbart grovt brott), svindleri (enbart grovt brott), grov förskingring, trolöshet mot huvudman (enbart grovt brott), olovligt brukande (enbart grovt brott), grov oredlighet mot borgenärer, grovt bokföringsbrott, mordbrand, allmänfarlig ödeläggelse, grovt sabotage, sjö- eller luftfartssabotage (enbart grovt brott), grov urkundsförfalskning, penningförfalskning (enbart grovt brott), grovt barnpornografibrott, övergrepp i rättssak (enbart grovt brott), grovt tjänstefel, bestickning/mutbrott (enbart grova brott), grovt narkotikabrott, grovt skattebrott, grovt dopningsbrott, brott mot alkohollagen (enbart grovt brott), grovt vapenbrott, grovt miljöbrott, grovt artskyddsbrott, grov smuggling, grov narkotikasmuggling, grovt tullbrott, terroristbrott, grovt insiderbrott och grov människosmuggling. Hemlig teleövervakning får också användas vid dataintrång, barnpornografibrott, som inte är att anses som ringa, narkotikabrott och narkotikasmuggling.

För att de brottsbekämpande myndigheterna ska få tillgång till annat än rena ”kataloguppgifter” enligt lagen om elektronisk kommunikation krävs, som framgick tidigare, att uppgiften gäller misstankar om brott med minst två års fängelse i straffskalan. Exempel på sådana brott är mord, dråp, människorov, människohandel, våldtäkt, våldtäkt mot barn, grovt koppleri, grovt rån, mordbrand, allmänfarlig ödeläggelse, grovt sabotage, sjö- och luftfartssabotage (enbart grovt brott), övergrepp i rättssak (enbart grovt brott), grovt narkotikabrott, grov narkotikasmuggling och terroristbrott.

Varje år lämnar regeringen en redovisning till riksdagen över tillämpningen av hemlig teleavlyssning och hemlig teleövervakning. Regeringen får uppgifterna från Åklagarmyndigheten och Rikspolisstyrelsen. Den senaste redovisningen, som avser år 2005, gjordes i regeringens skrivelse 2006/07:28. Där framkommer bl.a. följande. Under år 2005 lämnades tillstånd till hemlig teleövervakning i 1 027 fall. I samtliga fall där hemlig teleavlyssning beviljades under året (833 fall) hade domstolen samtidigt gett tillstånd till hemlig teleövervakning. I 194 fall hade tillstånd meddelats till enbart hemlig teleövervakning. I skrivelsen ger regeringen exempel på vid vilka brott hemlig teleövervakning användes. De brott som nämns är mord, dråp, grov misshandel, människorov, människohandel, olaga

hot (grovt brott), grov våldtäkt, grovt koppleri, grov stöld, grovt rån, tillgrepp av fortskaffningsmedel (grovt brott), grovt bedrägeri, utpressning (grovt brott), häleri (grovt brott), grovt bokföringsbrott, grov mordbrand, allmänfarlig ödeläggelse, övergrepp i rättssak (grovt brott), grovt narkotikabrott, grovt skattebrott, grovt vapenbrott, grova smugglingsbrott och grovt insiderbrott.

Även om inte regeringens skrivelse till riksdagen över tillämpningen av tvångsmedlen under år 2006 ännu har lämnats, har Åklagarmyndigheten och Rikspolisstyrelsen redovisat uppgifterna till regeringen. Av dessa framgår bl.a. följande. Under år 2006 lämnades tillstånd till hemlig teleövervakning i 1 119 fall. I samtliga fall där hemlig teleavlyssning beviljades under året (893 fall) hade domstolen samtidigt gett tillstånd till hemlig teleövervakning. I 226 fall hade tillstånd meddelats till enbart hemlig teleövervakning. I redovisningen ger myndigheterna exempel på vid vilka brott hemlig teleövervakning användes. Förutom de brott som nämns i föregående stycke anges även exempelvis olaga frihetsberövande, dataintrång, grovt tjänstefel och grovt dopningsbrott.

Det saknas statistik över de fall där de brottsbekämpande myndigheterna begär ut uppgifter (”annan uppgift som angår ett särskilt elektroniskt meddelande”) med stöd av lagen om elektronisk kommunikation. Polisen uppskattar antalet till ca 8 000 under år 2006. Mot bakgrund av kravet i den lagen på att det ska vara fråga om utredning om brott med ett straffminimum på två års fängelse, kan man förutsätta att dessa fall gäller utredningar om mycket allvarlig brottslighet.

I artikel 1 i direktivet om lagring av trafikuppgifter anges att syftet med direktivet är att säkerställa att de uppgifter som ska lagras finns tillgängliga vid bekämpningen av allvarliga brott, såsom de definieras i varje lands lagstiftning. Vår uppgift är således att analysera om de brott som preciseras genom de straffskalor och brott som anges i rättegångsbalkens regler om hemlig teleövervakning och i reglerna om utlämnande i lagen om elektronisk kommunikation är tillräckligt allvarliga. Vår bedömning ska ske mot bakgrund av syftet med lagringen och de överväganden om proportionalitet som krävs enligt Europakonventionen. I frågan om det behöver ske några förändringar rörande vilka brott som ska få föranleda utlämnande till de brottsbekämpande myndigheterna i framtiden, ska det tas ”vederbörlig hänsyn” till den lista med brott som numera finns som bilaga till lagen om överlämnande från Sverige enligt en europeisk arresteringsorder (se avsnitt 2.4).

Vissa brottsbeteckningar i listan motsvarar på ett tydligt sätt brott enligt svensk lagstiftning. Vid misstanke om de brotten är det också möjligt för de brottsbekämpande myndigheterna att få tillgång till trafikuppgifter. Det rör sig om mord, grov misshandel, människorov, människohandel, olaga frihetsberövande (som inte är mindre grovt), våldtäkt (som inte är mindre grov), grov stöld, rån, grovt bedrägeri, utpressning (grovt brott), svindleri (grovt brott), mordbrand, grovt sabotage, sjö- eller luftfartssabotage (grovt brott), penningförfalskning (grovt brott), grovt barnpornografibrott, grovt miljöbrott, grovt artskyddsbrott och terroristbrott.

Andra beteckningar i listan kan någorlunda lätt sägas motsvara brott där hemlig teleövervakning eller utlämnande enligt lagen om elektronisk kommunikation kan användas, som dataintrång, häleri (grovt brott), penninghäleri (grovt brott), grov urkundsförfalskning, Internetrelaterade barnpornografibrott, bestickning/mutbrott (grova brott), grovt narkotikabrott, grovt dopningsbrott, grovt vapenbrott, grov smuggling och grov människosmuggling.

I vissa fall är listan mer svårbedömd, exempelvis begreppet ”förfalskning och piratkopiering”, som kan motsvara brott mot lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, och begreppet ”olaglig handel med mänskliga organ och vävnader”, som kan motsvara brott mot lagen (1976:351) om genetisk integritet m.m. Inte i något av dessa fall kan hemlig teleövervakning eller utlämnande enligt lagen om elektronisk kommunikation användas.

För andra brott på listan är det svårt att peka ut en exakt motsvarighet i svensk lag. Det rör t.ex. ”deltagande i kriminell organisation” och ”rasism och främlingsfientlighet”. Det kan vara fråga om gärningar som enligt svensk rätt anses vara medhjälp till annans brott eller förhållande som mer motsvarar en försvårande omständighet vid bedömning av straffvärdet (t.ex. 30 kap. 2 § 7 brottsbalken).

11.5 Behöver bestämmelserna om tillgång till trafikuppgifter förändras?

Bedömning: Lagringen av trafikuppgifter ger inte anledning att förändra bestämmelserna om hemlig teleövervakning respektive utlämnande enligt lagen om elektronisk kommunikation.

Enligt direktivet om lagring av trafikuppgifter har den lagringsskyldighet som bestämts övervägts mot bakgrund av artikel 8 i Europakonventionen och begränsningen till allvarlig brottslighet har ansetts legitimera det intrång i rätten till respekt för privatlivet som lagringsskyldigheten innebär. Själva lagringen av trafikuppgifter kan som vi har beskrivit inte delas in efter brottstyper. För att det intrång i integritetsskyddet som lagringen innebär ska vara motiverat förutsätts det därför att uppgifterna inte kan lämnas ut annat än för utredning och lagföring av allvarliga brott. Avvägningen av vad som är allvarlig brottslighet ska göras i nationell rätt så att det uppnås proportionalitet i förhållande till intrånget i enskildas privatliv.

Genom kravet på brott av viss svårhetsgrad har lagstiftaren enligt de regler som nu gäller förbehållit hemlig teleövervakning och utlämnande enligt 6 kap. 22 § första stycket 3 LEK för de mer allvarliga typerna av brott och dessutom i många fall för den svåraste graden av brotten. För utredning om sådana brott är också tillgången till trafikuppgifter av avgörande betydelse för arbetet och uppgifterna är ofta helt nödvändiga för att utredningarna ska kunna föras framåt (se avsnitt 6.5). De brott som finns i bilagan till lagen om överlämnande från Sverige enligt en europeisk arresteringsorder överensstämmer mycket väl beträffande svårhetsgrad med de brott vid vilka hemlig teleövervakning och utlämnande enligt lagen om elektronisk kommunikation får användas. Det är t.o.m. så att listan tar upp vissa gärningar som inte utgör brott i Sverige. Vissa brott i listan är inte så allvarliga att metoderna får användas här.

Samtidigt som vi bl.a. i avsnitt 6.5 har konstaterat det mycket stora behov som finns i den brottsbekämpande verksamheten av trafikuppgifter, har vi på flera ställen i betänkandet utvecklat våra bedömningar i frågor som rör integritetsskyddet, t.ex. riskerna för integritetsskyddet, och vi har utformat våra förslag så att riskerna för integritetsförluster ska motverkas. Vi har redovisat de bedömningar och förslag till författningsändringar och åtgärder i övrigt som vi anser krävs för att lagringen av trafikuppgifter ska bli så säker som möjligt och omfattas av ett tillfredsställande integritets-

skydd. Det är mot den bakgrunden vi överväger behovet av ändringar i de bestämmelser som reglerar myndigheternas möjligheter att få tillgång till trafikuppgifter.

De regler som BRU har föreslagit om att reglerna i lagen om elektronisk kommunikation bör föras in i rättegångsbalken innebär att samtliga utlämnanden av trafikuppgifter utom utlämnande av uppgifter om abonnemang (”kataloguppgifter”) enligt 6 kap. 22 § första stycket 2 skulle prövas i domstol. Som vi ser det vore det en klar fördel för integritetsskyddet om de överväganden om proportionalitet som ska göras när trafikuppgifter lämnas ut alltid gjordes av en domstol.

Den analys vi ska göra gäller dock inte i första hand förfarandet vid utlämnande av trafikuppgifter utan i stället om de brott som i dag kan utredas med tillgång till trafikuppgifter är allvarlig brottslighet i den mening som avses i direktivet.

När bestämmelserna om hemlig teleövervakning och utlämnande enligt lagen om elektronisk kommunikation har utformats, har lagstiftaren utgått från att de brottsbekämpande myndigheterna alltid får tillgång till samtliga de uppgifter som metoderna omfattar. Det förhållandet att leverantörerna nu får en skyldighet att lagra trafikuppgifter och att myndigheterna därför i praktiken inte bara behöver hoppas på, utan t.o.m. kan lita på, att de historiska uppgifterna finns kvar under lagringstiden, är inte en omständighet som innebär att bestämmelserna behöver förändras. Avvägningen av vad som är allvarlig brottslighet påverkas således i princip inte av leverantörernas förmåga att ”leverera” utifrån en begäran om utlämnande av trafikuppgifter och inte heller av att de brottsbekämpande myndigheterna kan förväntas att i något ökad utsträckning än i dag begära och därmed få ut trafikuppgifter som man även tidigare haft rätt att få ut men som varit utplånade.

De nuvarande reglerna innebär att trafikuppgifter endast kan lämnas ut för brott som är minst lika allvarliga som de brott som anges när utlämnande enligt en europeisk arresteringsorder kan ske. Det innebär att trafikuppgifter lämnas ut till de brottsbekämpande myndigheterna endast om det brott som ska utredas med tillgång till uppgifterna är lika allvarligt som de brott som kan föranleda att svenska medborgare lämnas ut enligt arresteringsordern. Om förutsättningarna för myndigheternas tillgång till trafikuppgifterna gjordes snävare skulle det innebära att trafikuppgifter inte skulle kunna användas i brottsbekämpningen i samma utsträckning som i dag och i många fall till oacceptabla konsekvenser för möjligheterna att bekämpa allvarliga brott. Det skulle på sikt kunna med-

föra att själva syftet med lagringen av trafikuppgifter inte uppnåddes. Det förhållandet att lagringen ger en mer förutsebar tillgång till trafikuppgifter ändrar inte heller innebörden i den avvägning mellan brottsbekämpningsintresset och integritetsskyddet som ligger bakom de nuvarande reglerna. Vi bedömer därför att det inte finns något behov av att förändra de bestämmelser som gäller i dag för att de brottsbekämpande myndigheterna ska få begära ut trafikuppgifter. Inte heller finns det skäl att i anledning av lagringen av trafikuppgifter göra någon förändring av de övriga grundläggande förutsättningarna för metoderna.

Uppgifter om abonnemang (”kataloguppgifter”) ska enligt 6 kap. 22 § första stycket 2 LEK lämnas ut till brottsbekämpande myndigheter om fängelse är föreskrivet för brottet och det kan föranleda annan påföljd än böter i det enskilda fallet. Det är uppgifter som leverantörerna i stor omfattning lagrar redan i dag och som ofta är nödvändiga för att identifiera abonnenten eller den registrerade användaren. Dessa uppgifter kan alltså lämnas ut vid misstanke om mindre allvarliga brott än vad som nyss nämndes. Uppgifterna ska lagras enligt direktivet om lagring av trafikuppgifter.

Om det skulle införas ett krav på att denna typ av uppgifter endast skulle få lämnas ut till de brottsbekämpande myndigheterna vid allvarligare brottslighet, skulle det medföra en avsevärd försämring från brottsbekämpningssynpunkt. Många av de brott som i dag klaras upp med hjälp av uppgifterna skulle inte ha samma förutsättningar att bli utredda i framtiden. Liksom när det gäller utlämnande av övriga uppgifter till de brottsbekämpande myndigheterna, har den reglering av förutsättningarna för utlämnande som gäller i dag lagts fast efter en bedömning av proportionalitetskravet enligt regeringsformen, Europakonventionen och direktivet om integritet och elektronisk kommunikation. Denna bedömning ändras enligt vår mening inte av det förhållandet att lagringen av uppgifterna blir en skyldighet i framtiden. Vi anser därför att ett genomförande av direktivet, som överlåter åt medlemsstaterna att avgöra för vilka brott de lagrade uppgifterna ska få användas, inte motiverar en ändring av bestämmelsen om utlämnande av sådana uppgifter enligt lagen om elektronisk kommunikation.

11.6 Ska det finnas undantag för utlämnande av uppgifter i vissa fall?

I 36 kap. 5 § RB finns bestämmelser om vad som brukar kallas frågeförbud, alltså det förhållandet att personer med s.k. särställning inte får höras som vittnen i vissa fall. Det rör exempelvis advokater, läkare, tandläkare, präster och journalister. En särskild fråga är om lagringen av trafikuppgifter bör föra med sig några begränsningar i möjligheten för de brottsbekämpande myndigheterna att få tillgång till trafikuppgifter som har anknytning till sådana yrkesutövare.

Det är tekniskt omöjligt och dessutom olämpligt av integritetsskäl att införa ett system där det vore förbjudet för leverantörerna att lagra trafikuppgifter som kan knytas till personer som omfattas av bestämmelsen. I stället blir frågan om det ska finnas begränsningar för de brottsbekämpande myndigheterna i möjligheten att få ut sådana uppgifter.

I dag finns inga begränsningar när det gäller att knyta ett beslut om hemlig teleövervakning till en person som i vissa fall omfattas av 36 kap. 5 § RB. Personen kan vara skäligen misstänkt själv, eller så kan det finnas synnerlig anledning att anta att en misstänkt har ringt till eller på annat sätt kontaktat denne (se 27 kap. 20 § RB). Inte heller finns det något krav på att uppgifter ska förstöras av de brottsbekämpande myndigheterna om det t.ex. visar sig att en misstänkts teleadress har kontaktat en advokats teleadress (utan att teleövervakningen samtidigt var knuten till advokatens teleadress). I detta avseende finns det med andra ord inget skydd för den s.k. klientsekretessen i dag, dvs. det förhållandet att någon har haft kontakt med en advokat.

Det kan i övrigt nämnas att det inte finns några begränsningar när det gäller att verkställa hemlig teleavlyssning rörande dessa personer, med undantag för telemeddelanden mellan en skäligen misstänkt och dennes försvarare. Enligt 27 kap. 22 § RB ska avlyssningen avbrytas om det framkommer att det är fråga om ett sådant meddelande. De upptagningar och uppteckningar som finns ska då förstöras i de delarna.

Som framgått finns inte heller några begränsningar i detta avseende i fråga om utlämnande enligt lagen om elektronisk kommunikation.

Redan i samband med att hemlig teleövervakning infördes diskuterades vilket skydd som skulle finnas för bl.a. de yrkeskategorier som omfattas av 36 kap. 5 § RB. Regeringen ansåg att det inte behövdes något undantag för verkställighet av tvångsmedlet utan

menade att en uttryckligt reglerad proportionalitetsprincip var tillräcklig (prop. 1988/89:124 s. 26 ff.). Det anges numera i 27 kap. 1 § tredje stycket RB att bl.a. hemlig teleövervakning får beslutas endast om skälen för åtgärden uppväger det intrång eller men i övrigt som åtgärden innebär för den misstänkte eller för något annat motstående intresse. I den bedömningen måste givetvis ingå sådana faktorer som vilka typer av uppgifter och hur stor uppgiftsmängd som begärs ut liksom en persons särställning enligt 36 kap. 5 § RB. Utrymmet för domstolen att knyta ett beslut om hemlig teleövervakning till personer med sådan ställning är alltså redan i dag mycket begränsat (jfr prop. 1988/89:124 s. 28). Till det kommer att det är möjligt för domstolen att, för det fall tillstånd ges, föreskriva villkor för verkställigheten för att begränsa integritetsintrånget.

Vid begäran om utlämnande enligt lagen om elektronisk kommunikation gäller inte 27 kap. 1 § RB. För polisens del finns behovs- och proportionalitetsprinciperna reglerade i 8 § polislagen (1984:387). För tullens del finns kravet på proportionalitet reglerat i exempelvis 6 kap. 1 § tullagen (2000:1281). Principerna anses också gälla generellt utan uttryckligt lagstöd vid ingripande åtgärder från myndigheternas sida mot enskilda.

Vår bedömning är att de bestämmelser om lagring av trafikuppgifter som vi föreslår inte bör föranleda några begränsningar av möjligheten för de brottsbekämpande myndigheterna att använda hemlig teleövervakning respektive utlämnande enligt lagen om elektronisk kommunikation med anknytning till personer som avses i 36 kap. 5 § RB. Det skulle bli en märklig ordning om sådana begränsningar infördes samtidigt som det klart mer ingripande tvångsmedlet hemlig teleavlyssning får verkställas i de fallen.

12 Balansen mellan brottsbekämpning och integritetsskydd

12.1 Vår sammanfattande bedömning

Bedömning: Såsom förslagen om lagring av trafikuppgifter har utformats bedömer vi att det har uppnåtts en god balans mellan brottsbekämpningens intressen och integritetsskyddet.

12.2 Balansen i våra förslag

Bestämmelser om lagring av trafikuppgifter håller på att genomföras i alla länder i EU. Det följer av Sveriges medlemskap i unionen att direktivet om lagring av trafikuppgifter ska genomföras i svensk rätt. Vid våra överväganden om hur det ska ske ska vi utforma förslag som skapar en balans mellan medborgarnas integritetsskydd och deras intresse av en effektiv brottsbekämpning. Direktivet innehåller inte bara en uppräkning av vilka trafikuppgifter som ska lagras utan också flera artiklar som ska garantera en rimlig proportionalitet mellan brottsbekämpningens intressen och integritetsskyddet. Det gäller t.ex. den längsta acceptabla lagringstiden, att uppgifterna ska utplånas vid slutet av den tiden och att uppgifterna ska skyddas mot olika åtgärder som är skadliga för integriteten.

I vårt uppdrag ingår att belysa de integritetsaspekter som aktualiseras vid lagringen av trafikuppgifter. Det ska ske med utgångspunkt i 2 kap. regeringsformen och artikel 8 i Europakonventionen så att det nationella genomförandet av direktivet om lagring av trafikuppgifter är förenligt med dessa stadganden. Vi ska föreslå regler som syftar till att stärka skyddet för integriteten och motverka missbruk av uppgifterna. Våra förslag ska vara förenliga med dataskyddsdirektivet och direktivet om integritet och elektronisk kommunikation.

Regeringsformen innehåller i 2 kap. 12 § en uttrycklig proportionalitetsprincip av innebörd att rättighetsinskränkande lagstift-

ning aldrig får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den. Motsvarande princip finns i artikel 8 i Europakonventionen och formuleras där som att vars och ens rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens inte får inskränkas annat än om det i ett demokratiskt samhälle är nödvändigt med hänsyn till vissa angivna intressen. Inskränkningar i integritetsskyddet får göras endast om det motstående intresse som ska tillgodoses är så starkt och integritetsskyddsintresset så förhållandevis svagt att inskränkningen framstår som proportionerlig. Nyttan av lagringen ska stå i rimlig proportion till den integritetsskada som lagringen kan orsaka (jfr SOU 2007:22 s. 449 ff.). Det ska med andra ord finnas en balans mellan brottsbekämpningens intressen av att trafikuppgifter lagras i angiven omfattning och integritetsskyddet.

I det följande gör vi vår bedömning om våra förslag motsvarar en sådan balans.

Direktivet om lagring av trafikuppgifter har tagits fram inom EU mot bakgrund av de fördelar från brottsbekämpningssynpunkt som har kunnat konstateras i flera medlemsländer. I skäl 9 i ingressen i direktivet om lagring av trafikuppgifter: ”Eftersom lagring av uppgifter har visat sig vara ett så nödvändigt och effektivt redskap för de brottsbekämpande myndigheternas utredningar i många medlemsstater och framför allt i allvarliga fall som organiserad brottslighet och terrorism är det därför nödvändigt att se till att brottsbekämpande myndigheter får tillgång till lagrade uppgifter under en viss tid i enlighet med de villkor som föreskrivs i detta direktiv. Antagandet av ett instrument om lagring av uppgifter i enlighet med kraven i artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna är därför en nödvändig åtgärd.”

Behovet av trafikuppgifter bör diskuteras utifrån den precisering och beskrivning av nyttan som de brottsbekämpande myndigheterna kan göra. Den självklara utgångspunkten måste vara att det är medborgarna i allmänhet och brottsoffren som för sin trygghet och upprättelse har behov av en effektiv bekämpning av särskilt den allvarliga brottsligheten.

Vi har kommit fram till att tillgången till de trafikuppgifter som enligt våra förslag ska omfattas av lagringsskyldigheten är av avgörande betydelse för brottsbekämpningen och att de ofta är helt nödvändiga för att utredningarna över huvud taget ska kunna föras framåt. Bakgrunden till vår bedömning framgår i avsnitt 6.5.

Samtidigt medför lagring av trafikuppgifter ett påtagligt intrång i integritetsskyddet. Vi konstaterade i avsnitt 5.2 att integritetsintrånget vid lagring av trafikuppgifter sker redan genom att det allmänna säkrar tillgången till trafikuppgifterna, dvs. när lagringen sker av respektive uppgift. Det har framhållits att den psykologiska effekt det innebär att människor vet om att uppgifter lagras om deras kommunikation är den stora integritetsskadan i sammanhanget och inte att de brottsbekämpande myndigheterna får ut en mycket liten del av de lagrade trafikuppgifterna i ett begränsat antal ärenden årligen. Det innebär att det är viktigt för tilliten till systemet för lagring och förtroendet för brottsbekämpningen att regleringen är klar och tydlig så att medborgarna känner till både vad som ska lagras och att lagringen av trafikuppgifter inte innebär att myndigheterna har någon slags fri tillgång till uppgifterna utan att det bl.a. krävs misstankar om allvarliga brott för att uppgifterna ska få lämnas ut av leverantörerna. Det krävs också att det finns flera integritetsskyddande bestämmelser kring lagringen av trafikuppgifter.

Vi ser att den främsta risken för integritetsförluster för den enskilde ligger i att trafikuppgifterna på ett felaktigt sätt, genom uppsåtliga handlanden eller av oaktsamhet, sprids från leverantörerna till obehöriga och i att leverantörerna använder trafikuppgifterna för andra ändamål än de tillåtna. Det är svårt att bedöma hur stora riskerna är, men våra förslag syftar i flera avseenden till att minska riskerna för att enskilda drabbas av integritetsintrång och orsakas skador till följd av detta.

Vi har föreslagit att lagringen ska ske på flera håll så att uppgifter om varje persons kommunikation inte finns samlad på ett och samma ställe i ett centrallager utan är spridd hos leverantörerna. Lagringstiden ska, främst av integritetsskäl, vara begränsad till ett år, vilket enligt vår mening är den kortaste tid som kan accepteras för att lagringstiden inte ska bli så kort att det leder till begränsningar i det brottsbekämpande arbetet. Efter lagringstidens slut ska trafikuppgifterna utplånas. Vid sidan om de i övrigt tillåtna ändamålen enligt 6 kap. LEK ska leverantörerna få behandla uppgifterna endast för att lämna ut dem efter beslut om hemlig teleövervakning eller enligt bestämmelserna i lagen om elektronisk kommunikation eller för att lämna över dem till annan som fullgör lagringen. Det innebär att ändamålet för behandling av de lagrade trafikuppgifterna är starkt begränsat och inte kan ändras utan ett uttryckligt stöd i lag. Vidare ska leverantörerna vidta särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behand-

lingen av lagrade trafikuppgifter. Det ska med andra ord ställas höga krav på kvalitet och säkerhet för lagringen. Dessutom förutsätts att endast särskilt behörig personal hos leverantörerna har tillgång till uppgifterna. Om trafikuppgifterna är personuppgifter får de inte föras över till annat land som inte har en adekvat nivå för skyddet av uppgifterna. Som ett skydd mot missbruk av de lagrade trafikuppgifterna finns straff- och skadeståndsrättsliga bestämmelser, som i olika avseenden verkar preventivt och reparativt. Reglerna stadgar straff för t.ex. dataintrång och brott mot tystnadsplikten och ger rätt till skadestånd vid otillåtna kränkningar av den personliga integriteten och rätt till ersättning för personskada, sakskada och ren förmögenhetsskada. Till skyddet hör också den verksamhet som ska bedrivas av tillsynsmyndigheten och som ska gå ut på att kontrollera att leverantörernas verksamhet avseende lagring av trafikuppgifter följer gällande regelverk. Ytterst kan tillsynsmyndigheten besluta att en leverantörs verksamhet ska upphöra.

En del i integritetsskyddet är också att det blir ett tydligt regelsystem så att var och en kan bedöma vilket integritetsintrång man kan drabbas av. Enligt vår bedömning innefattar författningsförslagen så tydliga och väl avgränsade regler som är rimliga att ha när bestämmelserna samtidigt måste utformas så att de så långt som möjligt blir oberoende av den tekniska utvecklingen. Författningsförslagen och de motiv för dem som vi har anfört tydliggör vilka trafikuppgifter som ska lagras, vem som ska lagra och hur lång lagringstiden är men också vilka säkerhetsåtgärder till skydd för integriteten som lagringen ska omges av. Integritetsskyddet kommer också att preciseras i tillsynsmyndighetens föreskrifter. Till det kommer att den enskilde har möjlighet att enligt 26 § PUL en gång per år få besked av leverantören bl.a. om vilka personuppgifter om den sökande som behandlas (jfr skäl 15 i ingressen i direktivet om lagring av trafikuppgifter). Även de förutsättningar som gäller enligt rättegångsbalken och lagen om elektronisk kommunikation för att de brottsbekämpande myndigheterna ska få tillgång till de lagrade trafikuppgifterna är tydliga, även om det för vissa uppgifter kan vara något oklart om de ska anses vara uppgifter om abonnemang eller andra uppgifter (se 6 kap. 20 § första stycket 1 och 3 LEK samt avsnitt 2.3.2).

Vi bedömer att vi genom förslagen om hur direktivet om lagring av trafikuppgifter ska genomföras har preciserat den balans mellan intresset av en effektiv bekämpning av allvarlig brottslighet och intresset av skydd för enskildas integritet som direktivet bygger på. Vi menar också att förslagen uppfyller de krav som artikel 29-

gruppen och Europeiska datatillsynsmannen har ställt för skyddet av den personliga integriteten. Vid vår bedömning beaktar vi också att tillämpningen av bestämmelserna om hemlig teleövervakning och utlämnande enligt lagen om elektronisk kommunikation förutsätter att hänsyn tas till integritetsskyddet genom den proportionalitetsprövning som ska ske i varje enskilt ärende.

När balansen mellan brottsbekämpningens intressen och integritetsskyddet bedöms har också möjligheterna till kontroll av leverantörerna och myndigheterna som hanterar trafikuppgifter betydelse. För leverantörernas del avses den kontroll som kommer att utövas av tillsynsmyndigheten och som ytterst ska säkerställa att leverantörerna följer gällande regelsystem så att trafikuppgifterna kan komma brottsbekämpningen till del och så att lagringen sker i avsedd omfattning och med fullgott integritetsskydd.

Vid bedömningen om balansen blir god är också kontrollen av de myndigheter som utnyttjar trafikuppgifter i sin brottsbekämpande verksamhet viktig. Vi bortser här från att de tjänstemän som deltar i verksamheten givetvis är underkastade ett straffrättsligt ansvar för bl.a. dataintrång, tjänstefel och brott mot tystnadsplikten. Enskilda som blir föremål för användning av hemliga tvångsmedel har begränsade möjligheter att påkalla en rättslig prövning genom överklagande av tillstånd till tvångsmedelsanvändningen. Utöver den kontroll i förhand som kravet på tillstånd av domstol för användning av hemlig teleövervakning innebär finns det olika slag av tillsyn och kontroll som utövas i efterhand. Justitieombudsmannen och Justitiekanslern utövar tillsyn över bl.a. den brottsbekämpande verksamheten. Registernämnden och Datainspektionen utövar tillsyn över Säkerhetspolisens personuppgiftsbehandling. Datainspektionens tillsyn omfattar även den öppna polisens och Tullverkets personuppgiftsbehandling.

I propositionen Ytterligare rättssäkerhetsgarantier vid användandet av hemliga tvångsmedel, m.m. (prop. 2006/07:133) föreslås att personer som har utsatts för hemliga tvångsmedel, t.ex. hemlig teleövervakning, ska underrättas om det. En underrättelse ska dock skjutas upp och får även underlåtas om en uppgift i underrättelsen omfattas av sekretess. Underrättelseskyldigheten ska inte omfatta utredningar om sabotagebrott, brott mot rikets säkerhet och terroristbrott, dvs. brott som knyter an till Säkerhetspolisens verksamhetsområde. Vidare föreslås att det under regeringen inrättas en fristående och självständig myndighet, Säkerhets- och integritetsskyddsnämnden, som ska utöva tillsyn över brottsbekämpande myndigheters användning av hemliga tvångsmedel och därmed

sammanhängande verksamhet. Nämnden ska på begäran av en enskild vara skyldig att kontrollera om han eller hon har utsatts för hemliga tvångsmedel och om det har skett i enlighet med lag eller annan författning. Nämnden ska underrätta den enskilde om att kontrollen har utförts. Det ska erinras om att ett utlämnande av trafikuppgifter enligt lagen om elektronisk kommunikation inte är ett hemligt tvångsmedel.

BRU har föreslagit att bestämmelserna om hemlig teleövervakning i rättegångsbalken och utlämnanden av trafikuppgifter enligt lagen om elektronisk kommunikation ska föras samman (SOU 2005:38 s. 182 ff.). Förslaget innebär i praktiken att möjligheten att få trafikuppgifter enligt bestämmelsen i lagen om elektronisk kommunikation upphör. Ett viktigt skäl är enligt BRU att integritetsskyddet än mer skulle förstärkas genom att det som huvudregel skulle krävas tillstånd hos domstol till hemlig teleövervakning för att få ut uppgifterna. Vi instämmer i de bedömningar som låg bakom förslaget. Förslaget bereds för närvarande i Justitiedepartementet. Om förslaget genomförs innebär det att samtliga trafikuppgifter som lämnas ut till brottsbekämpande myndigheterna kommer att falla inom ramen för den tillsyn som Säkerhets- och integritetsskyddsnämnden kommer att utföra.

Det är vår bedömning att den sammantagna innebörden i våra förslag innebär att det har uppnåtts inte bara en rimlig utan en god balans mellan brottsbekämpningens intressen av att trafikuppgifter lagras i angiven omfattning och skyddet för den personliga integriteten.

13 Fördelning av kostnaderna

13.1 Sammanfattning av våra förslag och bedömningar

- Lagringsskyldigheten medför kostnader för att identifiera, spara, lagra och lämna ut trafikuppgifter.
- Kostnaden för att genomföra lagringsskyldigheten och anpassningsskyldigheten kan beräknas till omkring 200 miljoner kronor. Kostnaden för att lämna ut uppgifterna kan beräknas till omkring 20 miljoner kronor.
- Leverantörerna ska stå kostnaderna för lagring, säkerhet och anpassning av systemen. Det allmänna ska ersätta leverantörerna när uppgifter lämnas ut i enskilda ärenden.
- Post- och telestyrelsen får efter samråd med Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen och Tullverket meddela föreskrifter om ersättningen.

13.2 Inledning

Våra förslag innebär en lagringsskyldighet och en anpassningsskyldighet för leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation. Till skillnad mot nuvarande reglering som ger möjlighet till lagring av vissa trafikuppgifter endast för särskilt specificerade ändamål innebär vårt förslag en mer generell lagringsplikt för leverantörerna. Lagringsskyldigheten innebär att fler typer av trafikuppgifter än tidigare ska lagras och att lagringen ska ske under ett år. Antalet trafikuppgifter som ska lagras kommer således att öka och i många fall innebär det att trafikuppgifterna kommer att lagras under längre tid än i dag. Sammantaget innebär detta att den volym trafikuppgifter som ska finnas lagrad blir betydligt större än i dag.

Våra förslag innebär också att leverantörerna måste införa olika typer av säkerhetsåtgärder och säkerhetsrutiner som tar sikte på att lagrade uppgifter ska ha hög kvalitet och på att skyddet för enskildas integritet ska vara högt.

Det krävs ny teknik och nya administrativa system för att leverantörerna ska kunna identifiera, spara och sedan lagra trafikuppgifterna under ett år med den säkerhet som krävs. Det behövs också väl fungerande tekniska och administrativa system så att leverantörerna kan lämna ut uppgifterna till de brottsbekämpande myndigheterna utan dröjsmål och så att uppgifterna enkelt kan tas om hand. Sammantaget uppkommer kostnader för investeringar i nya tekniska system eller för anpassning av befintliga system, för underhåll av tekniska system och för administration.

I vårt uppdrag ingår att beräkna de angivna kostnaderna och belysa olika modeller för en fördelning av kostnaderna mellan det allmänna och leverantörerna samt de för- respektive nackdelar de olika alternativen för med sig. En betydelsefull omständighet som vi ska beakta vid valet mellan olika lösningar är vilken lösning som blir samhällsekonomiskt mest kostnadseffektiv.

För att få en mer specifik uppfattning om vilka nya tekniska lösningar och vilka anpassningar av befintliga system som krävs och en grund för vår bedömning av hur stora kostnaderna blir har vi bett de leverantörer som är representerade i utredningen att komma in med vissa uppgifter. Vi har frågat om kostnader för grundinstallationer, underhåll av systemen och kostnader för utlämnande av trafikuppgifter i enskilda ärenden. Vi har också tillfrågat branschorganisationen IT & Telekomföretagen, PTS och Svenskt Näringsliv. Vi har även skaffat oss ett underlag genom att låta en expert inom området för elektronisk kommunikation göra en analys av de kostnader som våra förslag innebär. Vi har därutöver fått information om beräkningar av kostnader som har utförts i Norge, Danmark och Storbritannien och hur fördelningen av kostnader ser ut i några länder.

13.3 Kostnader

13.3.1 Uppgifter från vissa leverantörer m.fl.

De leverantörer som har kommit in med uppgifter har i huvudsak valt att basera sina svar på den lagringsskyldighet som följer direkt av direktivet om lagring av trafikuppgifter. Det innebär att de bedömningar som leverantörerna har gjort avser en mindre omfattande lagringsskyldighet än den vi föreslår. Endast en av leverantörerna har kommit med en bedömning av kostnader för trafikuppgifterna avseende misslyckad uppringning (se avsnitt 6.13).

Samtliga leverantörer som har inkommit med uppgifter har framhållit svårigheterna att ange mer preciserade kostnadsberäkningar. De har anfört att det finns många osäkerhetsfaktorer. Enligt leverantörerna är det svårt att bedöma vilka de slutliga kraven blir för anpassning av systemen och beräkningen av kostnaden blir osäker på grund av den stora variationen i pris mellan olika systemleverantörer.

Den stora delen av kostnaderna för att genomföra lagringsskyldigheten avser nödvändiga tekniska system för att identifiera, spara, lagra och lämna ut uppgifterna. Kostnader uppkommer antingen för helt nya system eller för att anpassa befintliga system. Det är enligt leverantörerna till övervägande delen helt nya kostnader. I de fall leverantörerna lagrar uppgifterna redan i dag för faktureringsändamål behövs i och för sig inte nya tekniska system eller anpassningar av befintliga system. Men utvecklingen går mot att leverantörerna tillhandahåller kommunikationslösningar mot s.k. flat rate, dvs. kunden betalar en fast summa oavsett hur mycket man sedan kommunicerar. Det minskar leverantörernas behov av att lagra trafikuppgifter för fakturering. Enligt leverantörerna måste därför kostnadsbedömningen utgå från ett snabbt minskande behov av att lagra trafikuppgifter för faktureringsändamål.

Leverantörerna har också redovisat att kostnaderna för att genomföra lagringsskyldigheten kommer att variera mycket mellan olika leverantörer beroende på vilka tekniska system som de har i dag och i vad mån systemen kan anpassas för att fullgöra lagringsskyldigheten. Ofta kan standardlösningar inte appliceras. Anpassningen kan därför till viss del bli unik för varje leverantör. Alternativt kan nya tekniska system behöva införskaffas, antingen nu eller i ett senare skede beroende på hur de nuvarande tekniska systemen hos enskilda leverantörer kan användas initialt. Enligt leverantörer-

na påverkas också kostnaderna om kraven på leverantörerna förändras över tid. Leverantörerna bedömer att det är mest troligt att effekterna av förslagen kommer att vara mindre för de stora leverantörerna än för de små. För de stora leverantörerna som verkar i flera länder finns också möjligheten till samordningsvinster, bl.a. genom att samma typ av teknik kan användas i alla länder. Samtidigt kan det motsatta bli fallet med en fördyring om olika länder inför olika system för lagringen.

Leverantörerna har mycket grovt uppskattat kostnaderna för att *identifiera, spara och lagra* uppgifterna under första året till allt ifrån 10 till 20–40 miljoner kronor för några av de stora leverantörerna upp till 400 miljoner kronor för en av de största leverantörerna. Efter det första året minskar troligen kostnaderna. Generellt anger leverantörerna att kostnaderna för lagring av trafikuppgifter avseende fast och mobil telefoni per kund är betydligt lägre än kostnaderna avseende bredband/Internet. Kostnaderna för att lagra misslyckad uppringning uppges vara stora. En av leverantörerna har i relativa tal angett de totala kostnaderna för genomförandet av lagringsskyldigheten och utlämnande av trafikuppgifter. Enligt denna leverantör utgör kostnaderna för att identifiera och spara de uppgifter som ska lagras ca 15 procent av totalkostnaden, kostnaderna för lagring av uppgifterna ca 50 procent, kostnaderna för att lagra misslyckad uppringning med mobil telefoni ca 25 procent och kostnaderna för att lämna ut uppgifter ca 10 procent av totalkostnaden. I de angivna kostnaderna ingår kostnader för personal och säkerhetsåtgärder. En leverantör har angett kostnaderna för drift och underhåll av IT-system till 10-15 procent av investeringskostnaderna, en annan har angett samma kostnader till 5 procent av investeringskostnaderna. Det skulle innebära kostnader mellan 2 och 20 miljoner kronor. Vi har inte fått några uppgifter om de små leverantörernas kostnader.

Kostnaderna för att *lämna ut uppgifter* i enskilda ärenden uppges av leverantörerna uppgå till 1 500–2 000 kronor per ärende, om hanteringen sker med låg automatiseringsgrad. Kostnadsnivån per ärende kan enligt leverantörerna sänkas med väl utbyggda stödsystem och beställnings- och leveransrutiner. De stora leverantörerna har redan etablerade system och rutiner för att lämna ut trafikuppgifter, medan de små kan behöva vidta åtgärder som medför så stora kostnader att deras existens kan hotas. Utlämnande till en rimlig kostnad ställer krav på att de brottsbekämpande myndigheterna har en väl anpassad administration och teknik som följer med i utveck-

lingen. Leverantörerna har också uppgett att totalkostnaderna beror på i hur många fall myndigheterna begär att trafikuppgifter ska lämnas ut. Med en ökad efterfrågan från de brottsbekämpande myndigheterna kommer sannolikt totalkostnaden för att lämna ut uppgifter att bli högre.

13.3.2 Nuvarande ersättningar i samband med verkställande av hemlig teleavlyssning och hemlig teleövervakning

Inom polisen, inklusive Ekobrottsmyndigheten, har Säkerhetspolisen ansvaret för tekniska och administrativa frågor som rör hemlig teleavlyssning och hemlig teleövervakning. I dag gäller att de brottsbekämpande myndigheterna ersätter leverantörerna för kostnader som uppstår i anslutning till verkställighet i det enskilda fallet. Säkerhetspolisen har slutit avtal som reglerar verkställighetskostnaderna med de största leverantörerna. Avtalens innehåll är sekretessbelagt och vi kan därför inte redovisa ersättningsnivåerna. Vad som däremot kan sägas är att avtalen med respektive leverantör inte har helt likalydande innehåll, att ersättningen för hemlig teleavlyssning generellt är högre än för hemlig teleövervakning och att ersättningen beror på vilken tid på dygnet som verkställigheten sker.

Det har inte varit möjligt att få fram uppgifter från de brottsbekämpande myndigheterna om hur mycket de betalar årligen för trafikuppgifter som lämnas ut enligt rättegångsbalken. Det beror på att myndigheterna inte kostnadsför dessa uppgifter på ett samlat sätt utan kostnaderna anges som förundersökningskostnader i varje enskilt ärende.

13.3.3 Nuvarande ersättningar i samband med utlämnande av trafikuppgifter enligt lagen om elektronisk kommunikation

Även när det gäller ersättningar i samband med utlämnande av trafikuppgifter enligt lagen om elektronisk kommunikation har Säkerhetspolisen slutit avtal med de största leverantörerna om ersättningar i standardärenden. Ett standardärende är t.ex. när polisen frågar efter vilka samtal som har ägt rum under en viss period och från ett visst telefonnummer. Den ersättning som de brottsbekäm-

pande myndigheterna får betala till leverantören när det inte gäller standardärenden bestäms normalt i samband med varje enskilt ärende och beror av vilka trafikuppgifter som begärs, hur lätt tillgängliga trafikuppgifterna är hos leverantören och tidsramen för leverantörens hantering. Den ersättning som i dessa fall begärs av leverantörerna varierar stort. Flera små leverantörer som lämnar ut uppgifter någon eller några gånger om året avstår ibland från att ta betalt medan andra begär hög ersättning.

Av de skäl som anfördes i föregående avsnitt finns det inte heller någon samlad uppgift om de totala årliga kostnaderna för de brottsbekämpande myndigheterna för utlämnande av trafikuppgifter enligt lagen om elektronisk kommunikation.

13.4 Kostnadsbedömningar och kostnadsfördelningar i andra länder

13.4.1 Danmark

I Danmark har leverantörerna angett att deras totala kostnad beräknas till 100–200 miljoner DKK (ca 123–246 miljoner SEK) för en lagringstid på ett år. Till detta kommer sedan kostnader för verkställighet, vilka leverantörerna inte har beräknat. I Danmark har man i några avseenden gått utöver direktivet om lagring av trafikuppgifter och infört en längre gående lagringsskyldighet. Utvidgningen innebär bl.a. att uppgifter om en ”Internetsessions initierande och avslutande paket” och om lokalisering vid ett mobilsamtals slut ska lagras. Den angivna kostnaden täcker även kostnaderna för den utvidgningen. Utan utvidgningen har leverantörerna beräknat kostnaderna till 50–100 miljoner DKK (ca 61–123 miljoner SEK).

Det är leverantörerna som står för kostnaderna för att anpassa systemen. De brottsbekämpande myndigheterna betalar ersättning till leverantören när uppgifter lämnas ut. Storleken på ersättningarna diskuteras i ett samarbetsforum inom Telekommunikationsindustrin, som är leverantörernas branschorganisation. Mot bakgrund av dessa diskussioner, som sker mellan leverantörerna och polisen, utarbetas sedan en priskatalog över de uppgifter som leverantörerna lämnar ut till de brottsbekämpande myndigheterna.

De leverantörer som inte är med i branschorganisationen bestämmer själva sina priser i förhållande till de brottsbekämpande

myndigheterna. Dessa priser följer dock till övervägande delen priserna i branschorganisationens priskatalog.

För uppgifterna i priskatalogen råder sekretess. Vi har dock fått del av några uppgifter, av vilka framgår att utlämnande av historiska uppgifter från faktureringssystem eller liknande kostar 1 750 DKK (ca 2 170 SEK) för en månads uppgifter. Förhandlingar om fastställande av priser för utlämnande av lagrade trafikuppgifter inleddes under oktober 2007.

13.4.2 Finland

Vi har inte några uppgifter om hur kostnaderna för genomförandet av direktivet har beräknats i Finland.

Enligt den finländska kommunikationsmarknadslagen ska teleföretagen avgiftsfritt lämna ut uppgifter till en myndighet som behöver uppgifterna för att kunna utföra sitt uppdrag. Myndigheten ska på egen bekostnad ordna ett system med hjälp av vilket den kan ta emot och behandla sådana uppgifter. Myndigheten svarar även för kostnader för anslutning av systemet till ett kommunikationsnät.

När teleföretagen lämnar ut uppgifter har de rätt att av statens medel få ersättning för omedelbara kostnader för investeringar i system, användning och underhåll av system samt utrustning och programvara som anskaffats enbart för de behov som myndigheten uppgett. Teleföretagen har rätt att av statens medel få ersättning även för omedelbara kostnader som orsakas av en åtgärd som myndigheten förordnat. Detta innebär att teleföretagen och staten kommer överens om vilka investeringar som är nödvändiga att göra och vad som är en rimlig kostnad för detta. Kan teleföretagen och staten inte komma överens är det ytterst Kommunikationsverket som bestämmer vilka åtgärder som ska vidtas och ersättningen till leverantören. Teleföretagen får inte för sin kommersiella verksamhet använda system, utrustning eller programvara som bekostats av myndigheten.

Enligt uppgift avser man att tillämpa detta system även beträffande kostnaderna för lagring av trafikuppgifter enligt direktivet. Leverantörerna och de brottsbekämpande myndigheterna ska komma överens om vilka typer av åtgärder som leverantörerna måste vidta, dvs. hur lagringen rent tekniskt ska gå till, och hur mycket myndigheterna ska betala. Liksom nu ska ytterst Kommu-

nikationsverket avgöra vilka kostnader som leverantörerna ska få ersättning för.

13.4.3 Norge

Det norska företaget Teleplan har genomfört en analys av de ekonomiska konsekvenserna av ett genomförande av direktivet om lagring av trafikuppgifter för fast och mobil telefoni samt vissa aspekter av Internetaccess. Analysen behandlar alltså inte ett genomförande fullt ut av direktivet avseende Internet. Analysen bygger på material som har samlats in från små, mellanstora och stora leverantörer av telefoni- och Internettjänster (tolv leverantörer av fast telefoni, åtta leverantörer av mobil telefoni och 39 bredbandsleverantörer) och från leverantörer av tekniska lösningar för lagring och sökning.

Teleplan har utrett de ekonomiska konsekvenserna för leverantörer och brottsbekämpande myndigheter i fyra olika modeller; obligatorisk lagring i central lagringsbas, frivillig lagring i central lagringsbas, lokal lagring hos leverantörerna eller lagring genom outsourcing och utifrån en lagringstid om 6 månader, ett år eller två år. Outsourcing enligt den norska regleringen kan inte helt jämföras med förslaget i avsnitt 7.5 att den lagringsskyldige ska ha möjlighet att avtala med annan att fullgöra lagringen. Vi redovisar därför inte de siffrorna.

Analysen visar att de sammanlagda kostnaderna hos leverantörerna varierar mellan 90 och 200 miljoner NOK (ca 104 och 231 miljoner SEK) beroende på lagringstid, uppskattad lagringsvolym, utvecklingsbehov hos leverantörerna (dvs. behov av tekniska investeringar för att genomföra lagringsskyldigheten) och val av lagringsmodell.

Med en lagringstid om 12 månader, lokal lagring hos leverantörerna och hög lagringsvolym har den sammanlagda kostnaden för leverantörerna beräknats till 95 miljoner NOK (ca 108 miljoner SEK) vid ett lågt utvecklingsbehov. Med ett mellanstort utvecklingsbehov uppgår kostnaden till 111 miljoner NOK (ca 126 miljoner SEK) och vid ett stort behov till 144 miljoner NOK (ca 163 miljoner SEK). Är lagringsvolymen i stället låg uppgår kostnaden vid ett lågt utvecklingsbehov till 89 miljoner NOK (ca 100 miljoner SEK), vid mellanstort behov till 106 miljoner NOK (ca 120 miljo-

ner SEK) och vid ett stort behov till 139 miljoner NOK (ca 157 miljoner SEK).

I kostnadsberäkningarna har man utgått från att leverantörerna ska ha tekniska system som är separerade från de system som leverantörerna i dag använder när de lagrar trafikuppgifter för egna ändamål. Vidare har man inte tagit hänsyn till att en del leverantörer redan lagrar trafikuppgifter som omfattas av lagringsskyldigheten.

När det gäller kostnaden för att lämna ut uppgifter i enskilda ärenden vid lokal lagring hos leverantörerna anges i analysen att det är svårt att fastställa den kostnaden. Man har antagit att leverantörerna behöver 45 minuter för att besvara en begäran från myndigheterna och att kostnaden per timme är 600 NOK (ca 700 SEK).

I analysen har också beräknats att investeringskostnaderna för en liten leverantör, vid lokal lagring hos leverantörer och sex månaders lagringstid med låg lagringsvolym och ett högt utvecklingsbehov, uppgår till mellan 85 000 och 575 000 NOK (ca 96 000 och 651 000 SEK). Man har inte beräknat motsvarande kostnader för en längre lagringstid eller med en högre lagringsvolym.

För myndigheterna uppgår kostnaderna för att begära ut uppgifter till 13 miljoner NOK (ca 14,7 miljoner SEK), vid lokal lagring och med 12 månaders lagringstid.

Enligt analysen är en viktig slutsats att lagringstid och lagringsvolym påverkar kostnaderna i relativt liten omfattning. Den största kostnaden är i stället knuten till själva etableringen av lagringssystemet. Det är således utvecklingsbehovet av de tekniska systemen som i största grad påverkar kostnaderna, dvs. vilka system de enskilda leverantörerna har i dag och vilka förändringar som de behöver för att kunna genomföra lagringsskyldigheten. Kostnader för informationssäkerhet påverkar till en viss grad kostnaderna men är inte kostnadsdrivande.

Arbetet med ett förslag till genomförande av direktivet har ännu inte kommit så långt att man har tagit ställning till frågan om fördelning av kostnaderna.

13.4.4 Storbritannien

I Storbritannien har kostnadsbedömningar gjorts utifrån tre olika alternativ. Det första alternativet innebär att direktivet om lagring av trafikuppgifter inte genomförs, ”do nothing”-alternativet. Enligt det alternativet fortsätter man med det system med frivillig lagring

av trafikuppgifter som redan finns i dag och som innebär att endast de största leverantörerna lagrar uppgifter. Det andra alternativet som beräknats är att alla tjänsteleverantörer ska lagra trafikuppgifter och det tredje alternativet är att alla tjänsteleverantörer ska lagra uppgifter men att det i möjligaste mån ska undvikas att uppgifter lagras hos fler än en leverantör. Kostnadsberäkningarna har gjorts utifrån en tänkt lagringstid på ett år.

Kostnaden för ”do nothing”-alternativet uppgår till 17,4 miljoner GBP (ca 235,6 miljoner SEK). I bedömningen har inte tagits med kostnader för eventuella överträdelser genom att direktivet inte genomförs. Alternativet innebär att endast vissa trafikuppgifter från särskilt utsedda leverantörer kommer att finnas tillgängliga för de brottsbekämpande myndigheterna. Det andra alternativet beräknas uppgå till 30,03 miljoner GBP (ca 406,6 miljoner SEK). Med denna lagring kommer alla nödvändiga uppgifter att finnas lagrade för de brottsbekämpande myndigheterna och man undviker kostnader för att inte följa direktivet. Det tredje alternativet har samma fördelar och innebär att uppgifterna i möjligaste mån bara lagras hos en leverantör. Kostnaden för det tredje alternativet blir lägre och uppgår till 21,13 miljoner GBP (ca 286 miljoner SEK).

Kostnaden för att lagra och lämna ut trafikuppgifter, med en lagringstid på 12 månader, har för en större leverantör av mobil telefoni uppskattats till 875 000 GBP (ca 11,7 miljoner SEK). De uppgifter som då lagras är i huvudsak de som ska lagras enligt direktivet (jfr Teleplans analys).

Den nuvarande frivilliga lagringen av trafikuppgifter i Storbritannien innebär att staten ersätter de kostnader som uppkommer för de leverantörer som staten har slutit avtal med för lagringen av trafikuppgifter. I avtalet med respektive leverantör har staten preciserat bl.a. vilka uppgifter som ska lagras, hur lagringen ska gå till och hur uppgifterna ska lämnas ut till de brottsbekämpande myndigheterna. Leverantören redovisar sedan vilka åtgärder som vidtagits för att tillgodose statens krav, bl.a. avseende tekniska investeringar, och vilka kostnaderna är. Därefter bedömer en oberoende expert om leverantörens åtgärder tillgodoser myndighetens krav och om den angivna kostnaden är rimlig. Bedöms kostnaden vara rimlig betalar staten det som leverantören har begärt. Anses kostnaden däremot inte vara rimlig får leverantören komma in med ett nytt förslag.

Mot bakgrund av att flera medlemsstater har andra regler för kostnadsfördelning har man i Storbritannien övervägt att införa ett

system som innebär att statens ersättningar till leverantörerna begränsas. På grund av den hårda konkurrensen på marknaden och svårigheterna att skilja ut olika kostnader för t.ex. insamling av uppgifter och lagring av dem, har man dock stannat för att behålla det system man tillämpar nu.

13.4.5 Tyskland

Vi har inte några uppgifter om hur kostnaderna för genomförandet av direktivet har beräknats i Tyskland.

De kostnader som uppkommer ska fördelas mellan det allmänna och leverantörerna så att leverantörerna ska stå för kostnaden för anpassning av systemen och vad som i övrigt följer med lagringsskyldigheten. Det allmänna kommer att betala ersättning till leverantörerna när trafikuppgifter lämnas ut i enskilda ärenden. Kostnadsersättningen uppgår f.n. till maximalt 17 euro per timme (ca 160 SEK) och betalas av den brottsbekämpande myndighet som begärt uppgiften. För närvarande diskuteras om detta system ska förändras och i fortsättningen baseras på en schablonersättning per utlämning.

13.5 Nuvarande kostnadsfördelning avseende hemlig teleavlyssning och hemlig teleövervakning

Enligt 6 kap. 19 § LEK har i dag vissa leverantörer skyldighet att anpassa sin verksamhet så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas.

När anpassningsskyldigheten infördes i telelagen år 1996 begränsades den till att endast omfatta tillståndspliktiga leverantörer. Dessa skulle också svara för de kostnader som hänförde sig till anpassningen och för drift och underhåll av systemen men skulle ha rätt till ersättning för de kostnader som uppkom vid varje enskild verkställighet.

Anpassningsskyldighetens omfattning fastslogs av PTS i beslut om tillståndsvillkor för respektive leverantör. I förarbetena (prop. 1995/96:180 s. 28 ff.) påpekades särskilt att anpassningsskyldigheten inte innebar att polisen fritt fick bestämma vilka anpassningar som skulle göras i telesystemen. Tillståndsmyndigheten skulle vid sin prövning beakta nyttan av en anpassning mot kostnaden för

denna, samt även beakta om anpassningen gjordes i ett befintligt telesystem eller om det var krav som ställdes i samband med byte till ny teknik.

BRU har därefter föreslagit en utvidgad anpassningsskyldighet för leverantörerna (SOU 2005:38 s. 278 ff.). BRU behandlade i det sammanhanget även frågan om hur kostnaderna för anpassningen skulle fördelas och föreslog att leverantörerna även i fortsättningen skulle stå för kostnaderna. BRU:s skäl var huvudsakligen desamma som de regeringen anförde när anpassningsskyldigheten infördes (se nedan avsnitt 13.8.3). Förslaget bereds för närvarande inom Justitiedepartementet.

13.6 Vilka kostnader uppstår?

Bedömning: Lagringsskyldigheten medför kostnader för att identifiera, spara, lagra och lämna ut trafikuppgifter.

13.6.1 Kostnader för att identifiera och spara de uppgifter som ska lagras

Vårt förslag innebär i förhållande till vad som gäller nu att vissa av de trafikuppgifter som leverantörerna sparar enligt nuvarande bestämmelser kommer att lagras också för brottsbekämpningsändamål och att nya typer av trafikuppgifter ska lagras. Det innebär att leverantörerna måste införa tekniska lösningar som medger att just de trafikuppgifter som ska lagras för att kunna lämnas ut i brottsutredningar kan identifieras och sparas i leverantörernas system. I den mån de system som leverantörerna har i dag inte kan anpassas kommer det att innebära att leverantörerna måste investera i nya tekniska system. Kostnaderna kan således avse helt nya tekniska system eller kostnader för anpassning av befintliga system.

Till detta kommer sedan löpande kostnader för drift och underhåll av systemen och för säkerhetsåtgärder. Leverantörerna har också vissa administrativa kostnader.

13.6.2 Kostnader för att lagra uppgifter

Enligt vårt förslag ska fler typer av trafikuppgifter än tidigare lagras. Det medför att antalet trafikuppgifter som ska lagras ökar väsentligt. Att lagringstiden föreslås bli ett år medför i många fall en längre lagringstid än i dag. Följden blir att volymen lagrade trafikuppgifter kommer att bli större. Leverantörerna måste ha kapacitet för att lagra dessa uppgifter. Det medför kostnader för nyanskaffningar eller kostnader för anpassning av befintliga lagringssystem (t.ex. servrar, diskar och licenser). Till det kommer vissa kostnader för drift och underhåll av systemen.

Vårt förslag innebär också att leverantörerna ska vidta tekniska och organisatoriska säkerhetsåtgärder som skyddar de lagrade trafikuppgifterna. Lagrade trafikuppgifter bör bl.a. hållas logiskt skilda från leverantörernas övriga verksamhet. Det medför kostnader för investeringar i tekniska system och administrativa kostnader.

När lagringstiden är slut ska uppgifterna utplånas. Det medför kostnader för både tekniska system och administrativa rutiner. De uppgifter som ska utplånas måste identifieras och sedan förstöras eller tas bort ur lagret. Leverantörerna får också administrativa kostnader för t.ex. utbildning och kompetensutveckling.

13.6.3 Kostnader för att lämna ut uppgifter

När trafikuppgifter ska lämnas ut till en myndighet behöver leverantörerna använda sökverktyg som identifierar de uppgifter som ska lämnas ut i det enskilda ärendet. Detta innebär att kostnader uppstår för nya tekniska system eller för att anpassa befintliga system. Till detta kommer kostnader för drift och underhåll av systemen.

För att kravet på säkerhet i lagringen ska uppfyllas kan endast särskilt behörig personal ha tillgång till och hantera trafikuppgifterna vid ett utlämnande. Detta medför administrativa kostnader.

Leverantörerna har också kostnader i samband med själva överlämnandet av uppgifterna till de brottsbekämpande myndigheterna. Kostnaderna består bl.a. i att hitta ett gemensamt gränssnitt mellan leverantören och de brottsbekämpande myndigheterna så att uppgifterna enkelt kan lämnas ut.

13.7 Hur stora blir kostnaderna?

Bedömning: Kostnaden för att genomföra lagringsskyldigheten och anpassningsskyldigheten kan beräknas till omkring 200 miljoner kronor. Kostnaden för att lämna ut uppgifterna kan beräknas till omkring 20 miljoner kronor.

13.7.1 Leverantörernas uppgifter

Med utgångspunkt enbart i de uppgifter som leverantörerna har lämnat till oss och marknadsbeskrivningen i avsnitt 14.4 skulle de totala kostnaderna för samtliga leverantörer mycket grovt kunna uppskattas till 600–700 miljoner kronor.

Leverantörerna har bedömt att kostnaderna för att lämna ut uppgifter i ett enskilt ärende uppgår till 1 500–2 000 kronor med de beställnings- och leveransrutiner som finns i dag och under kontorstid. Den kostnaden avser i huvudsak de stora leverantörerna som har utvecklade beställnings- och leveransrutiner. För de små leverantörerna som inte har samma rutiner och inte heller kan antas lämna ut uppgifter i samma utsträckning som de stora kan kostnaderna antas bli högre. Kostnaden kan sänkas med en högre automatiseringsgrad och effektivare beställnings- och leveransrutiner.

13.7.2 Beräkningar av kostnader för genomförande av direktivet

För att få ytterligare underlag för våra bedömningar av kostnaderna har vi anlitat en expert inom området för elektronisk kommunikation som på grundval av våra förslag och leverantörernas beräkningar har lämnat en rapport med beräkningar av kostnaderna för genomförandet av direktivet.

Rapporten har tagits fram under relativt kort tid och bygger på PTS rapport Svensk telemarknad 2006, intervjuer med såväl stora som små leverantörer på marknaden (fem stycken), intervjuer med leverantörer av tekniska system (två stycken) samt med PTS och Säkerhetspolisen. Utifrån dessa uppgifter och våra förslag avseende vilka leverantörer som ska vara lagringsskyldiga och vilka krav som ställs på de lagringsskyldiga, har kostnaderna för genomförandet av direktivet uppskattats.

I rapporten finns en uppskattning av antalet noder, dvs. de växlar för fast telefoni och mobil telefoni samt servrar för Internet, som de lagringsskyldiga leverantörerna har med en bedömning av om utrustningen är modern eller äldre. I rapporten anges att det finns ungefär 200 växlar (system) för fast telefoni, varav hälften är äldre. En av de största leverantörerna uppges ha ungefär 75 procent av dessa växlar, varav de flesta är äldre. Vidare uppges det finnas ca 100 växlar för mobil telefoni, där en av de största leverantörerna har ungefär hälften. En tredjedel av samtliga mobila växlar uppges vara äldre. Slutligen uppges det finnas ca 1 000 servrar av olika typer, varav en av de största leverantörerna har ungefär 15 procent.

I det följande redovisas i sammandrag de resonemang som förs i rapporten.

När det gäller kostnader för att *identifiera och spara uppgifter* konstateras att lagring av lokaliseringsinformation vid kommunikationens slut för mobil telefoni och av uppgifter rörande misslyckad uppringning kräver anpassning av systemen. I dag identifieras i och för sig dessa uppgifter och sparas för en kort stund, men de lagras inte eftersom de inte behövs för abonnentfakturering. Systemen behöver därför anpassas så att uppgifterna efter identifiering också lagras. Anpassningskostnaderna för lokaliseringsinformation vid kommunikationens slut för mobil telefoni uppskattas till ca 100 000 kronor per växel. Anpassningskostnaderna avseende fast telefoni för misslyckad uppringning uppgår till ca 500 000 kronor för en modern växel och till ca 5 miljoner kronor för en äldre växel. För mobil telefoni är kostnaderna ca 500 000 kronor för en modern växel och ca 2 miljoner kronor för en äldre växel. För Internettjänster framgår av rapporten att de uppgifter som ska lagras oftast redan finns. Det är i stället själva lagringen som kräver anpassningar eller nya system.

De totala kostnaderna för att identifiera och spara uppgifterna uppskattas till 665 miljoner kronor om äldre system också ska anpassas och till 102 miljoner kronor om systemen är modernare. Det är företrädesvis de leverantörer som har varit verksamma på marknaden sedan tidigt på 1990-talet som har äldre växlar. Det stora flertalet av leverantörerna har moderna växlar, där anpassningskostnaden är väsentligen lägre. I rapporten anges att utbyte av de äldre systemen under åren 2008-2009 redan planeras, av andra skäl än att lagringsskyldigheten tillkommer, och att de nya system som anskaffas torde vara utrustade med de funktioner som lagrings-

skyldigheten kräver. I så fall tillkommer inte några anpassningskostnader för dessa system.

När det gäller kostnaderna för att *lagra uppgifter* anges i rapporten att lagringskostnaden blir ca 50 000 kronor per tekniskt system avseende fast och mobil telefoni med ett fyrfaldigande av dagens datamängd och med lagringstid på ett år. Volymökningen beror till stora delar på att misslyckad uppringning ofta inte lagras i dag och att de uppgifterna är en stor andel av alla samtal. Avseende t.ex. fast telefoni utgör de misslyckade uppringningarna tre fjärdedelar av alla samtal. Dessutom kan en kostnad för logisk separation och system för behörighetshantering om ca 30 000 kronor för varje system tillkomma. Vidare behöver varje leverantör avseende Internettjänster åtminstone en server, oavsett hur stor del av den servern som behöver utnyttjas. En server kostar 10 000 kronor.

De totala lagringskostnaderna uppskattas i rapporten till maximalt 104 miljoner kronor per år. Kostnaden baseras på att samtliga uppgifter i en nod också lagras i den noden. Enligt rapporten är det troligt att varje leverantör kommer att centralisera lagringen inom den egna verksamheten, vilket i så fall sänker kostnaden. Om lagringskostnaden uppskattas per abonnent och år uppgår den, vid ett effektivt utnyttjande av lagringskapaciteten, för fast och mobil telefoni samt Internet till ungefär 3,5 öre. Även om lagringsvolymerna blir mycket större kommer den absoluta kostnadsökningen enligt rapporten fortfarande att hamna på en rimlig nivå med tanke på den förhållandevis låga lagringskostnaden.

Om leverantören *avtalar med annan* om att denne ska lagra trafikuppgifterna uppstår kostnader om drygt 18 miljoner kronor för de tekniska system som krävs för att föra över uppgifterna till den lagringsansvarige. De årliga kostnaderna för att lagra och lämna ut uppgifterna innefattar en engångsavgift på 5 000 kronor och uppåt samt 3 kronor per abonnent och år. De årliga kostnaderna uppgår sammanlagt till drygt 58 miljoner kronor. De totala kostnaderna för att annan ska lagra och lämna ut trafikuppgifterna uppgår till knappt 77 miljoner kronor. Kostnaden kan enligt rapporten sänkas om det uppstår konkurrens mellan dessa aktörer.

När det gäller kostnader för att *lämna ut uppgifter*, har leverantörerna beroende på deras storlek olika stora behov av personal. Personalen behöver också ha utbildning och behörighet. Om det antas att det tar ca 2 timmar att lämna ut en uppgift, blir personalkostnaden ca 500 kronor. Kostnaden för säkerhetsåtgärder och utbildning har uppskattats till ca 34 000 kronor. De totala kostnader-

na för att lämna ut uppgifter har uppskattats till ca 21 miljoner kronor per år.

I rapporten har också beräknats vad kostnaden skulle bli för att identifiera, spara, lagra och lämna ut uppgifterna utslaget på antal abonnenter. Med endast äldre system blir kostnaden för att identifiera, spara och lagra uppgifterna 41 kronor per abonnent medan den blir 11 kronor om systemen är modernare. Den årliga kostnaden för att lämna ut uppgifterna om leverantörerna gör det själva blir 1,50 kronor per abonnent. Första året tillkommer kostnaden för teknik (5,30 kronor per abonnent). Om alla leverantörer avtalar med annan att lagra och lämna ut uppgifterna blir kostnaden 3 kronor per abonnent och år. Första året tillkommer kostnaden för teknik (1 krona per abonnent).

13.7.3 Vår bedömning av kostnaderna

Kostnaderna för att *identifiera och spara* de uppgifter som ska lagras kan variera relativt mycket mellan leverantörerna. Kostnaderna blir olika stora beroende på den typ av tjänst som trafikuppgifterna är kopplade till, hur anpassade de tekniska system som de olika leverantörerna har i dag är i förhållande till de nya kraven och storleken på leverantörens verksamhet.

Enligt den analys av kostnaderna som vi har låtit utföra beror kostnaderna för att identifiera och spara uppgifterna mycket på om leverantörerna väljer att införa ny teknik eller om de i stället anpassar de äldre systemen. Införandet av ny teknik synes vara det mest kostnadseffektiva sättet, särskilt som de leverantörer som har äldre system redan av andra skäl har planerat att byta till nya system. Mot bakgrund av de beräkningar som görs i rapporten bedömer vi att kostnaderna för att identifiera och spara uppgifterna kan beräknas till omkring 100 miljoner kronor.

När det gäller kostnaderna för att *lagra* trafikuppgifterna bör det beaktas att den tekniska utvecklingen av system som kan lagra elektroniska uppgifter har varit mycket snabb under de senaste åren och att utvecklingen pågår hela tiden. Utvecklingen går mot att allt större mängder uppgifter kommer att kunna lagras med allt mindre utrymme. Kostnaderna påverkas också av våra krav på tillräckliga tekniska och organisatoriska säkerhetsåtgärder. Våra förslag innebär att högre krav ställs på leverantörerna än vad som nu är fallet enligt 6 kap. 3 § LEK. För de leverantörer som i dag har ett väl ut-

byggt och fungerande säkerhetssystem kommer kostnaderna troligen inte att bli särskilt betungande medan andra leverantörer kan behöva införa nya rutiner och system som medför kostnader.

Enligt rapporten blir kostnaden för att lagra trafikuppgifterna med de krav på säkerhet som vi föreslår olika hög beroende på hur lagringen genomförs. Den sammanlagda kostnaden uppskattats till 104 miljoner kronor om varje leverantör lagrar i egna system. Den kostnaden bygger på att varje leverantör lagrar uppgifterna i den växel eller server där uppgiften uppkommer och inte centraliserar lagringen inom den egna verksamheten. Om alla leverantörer i stället skulle ha ett gemensamt system för lagringen beräknas den totala kostnaden enligt rapporten till 77 miljoner kronor. Den kostnaden inkluderar kostnader för att lämna ut uppgifter. Enligt rapporten kan denna kostnad sänkas på sikt genom att det blir konkurrens mellan de aktörer som åtar sig lagringsuppdrag.

Våra förslag bygger på att varje enskild leverantör har det ansvar för lagringen som följer av lagringsskyldigheten. Förslagen utgår från att lagring ska ske hos varje leverantör men öppnar en möjlighet för den enskilde leverantören att anlita någon annan att lagra uppgifterna. Det är i dagsläget svårt att bedöma om leverantörerna kommer att bygga upp ett samarbete kring lagringen av uppgifterna. Det går därför inte att nu beräkna kostnaderna som om lagringen redan från början skulle genomföras på det totalt sett mest kostnadseffektiva sättet. De beräkningar som har gjorts i rapporten och en jämförelse med de kostnadsberäkningar som har gjorts i andra länder tyder dock på att kostnaderna för lagringen inte är så höga som leverantörernas beräkningar visar och att lagringen kan utföras rationellt inom varje leverantörs verksamhet. Vi bedömer att kostnaderna för lagringen med en kostnadseffektiv lagring hos varje leverantör kan beräknas uppgå till omkring 100 miljoner kronor.

Kostnaderna för att *lämna ut* trafikuppgifter beror i stor utsträckning på verksamhetens omfattning, dvs. antalet kunder och antalet förfrågningar från brottsbekämpande myndigheter. I och med att fler uppgifter kommer att finnas lagrade skulle det kunna antas att de brottsbekämpande myndigheterna i större utsträckning än i dag kommer att begära ut uppgifter. Enligt vår bedömning torde ökningen dock inte bli så stor eftersom vi inte föreslår några ändringar i de bestämmelser som reglerar när trafikuppgifter ska lämnas ut. Vi bedömer att leverantörer med ett stort antal kunder kommer att behöva verkställa ett större antal beslut om tillgång till

trafikuppgifter än leverantörer med få kunder. Det är dock inte säkert att det alltid blir så. I vissa fall kan en leverantör med få kunder också behöva verkställa ett relativt sett stort antal beslut.

Vid beräkningen av kostnaderna för utlämnande av uppgifterna måste det också beaktas att våra förslag inte innebär något krav på en ”jourverksamhet” dygnet runt för leverantörerna. Vårt förslag innebär alltså inte att t.ex. små leverantörer alltid måste ha en beredskap för att snabbt kunna lämna ut uppgifter. De större leverantörerna torde redan i dag ha kapacitet för att lämna ut uppgifterna även efter kontorstid. Under förutsättning att själva utlämnandet sker på samma sätt som i dag räknar vi med att det inte uppstår några ytterligare kostnader i förhållande till de kostnader som leverantörerna har i dag även om små leverantörer som i dag inte har några rutiner för överlämnande kan få vissa nya kostnader.

Den kostnadsanalys som finns i rapporten anger att kostnaderna för att lämna ut trafikuppgifter innefattar personalkostnader och kostnader för utbildning och säkerhetsåtgärder. I rapporten uppskattas dessa kostnader till ca 21 miljoner kronor per år. Vi har räknat med en viss ökning av antalet fall där trafikuppgifter kommer att begäras ut och bedömer att antalet fall kommer att stiga från ca 9 000 per år till ca 10 000 per år. I dag beräknar leverantörerna och de brottsbekämpande myndigheterna att kostnaden för utlämnande i ett normalt ärende uppgår till ca 1 500–2 000 kronor per ärende. Med dessa beräkningar som grund bedömer vi att kostnaderna för utlämnande av trafikuppgifter kommer att uppgå till omkring 20 miljoner kronor per år.

En sammanfattande bedömning innebär att kostnaderna för att genomföra våra förslag kan beräknas uppgå till omkring 220 miljoner kronor, varav ca 200 miljoner kronor avser kostnader för att identifiera, spara och lagra trafikuppgifter och 20 miljoner kronor avser kostnader för att lämna ut uppgifterna. Denna kostnadsbedömning kan jämföras med de bedömningarna av kostnader som har gjorts i Norge (ca 100–160 miljoner kronor) och i Danmark (ca 123–246 miljoner kronor). Kostnaden kan också jämföras med den totala omsättningen i Sverige på marknaden för elektronisk kommunikation som uppgick till knappt 49 miljarder kronor år 2006.

13.8 Kostnadsfördelningen

Förslag: Leverantörerna ska stå kostnaderna för lagring, säkerhet och anpassning av systemen. Det allmänna ska ersätta leverantörerna när uppgifter lämnas ut i enskilda ärenden.

Post- och telestyrelsen får efter samråd med Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen och Tullverket meddela föreskrifter om ersättningen.

13.8.1 Våra utgångspunkter

Utifrån de kostnadsberäkningar vi gjort ska vi enligt våra direktiv ta fram olika alternativ för fördelningen av kostnaderna och redovisa de för- och nackdelar de olika alternativen medför. Vid valet mellan olika fördelningsmodeller ska vi särskilt beakta vilken lösning som blir samhällsekonomiskt mest kostnadseffektiv. I våra resonemang ska vi beakta behovet av en väl fungerande konkurrens på marknaden.

Vid de diskussioner vi har fört med leverantörerna och de brottsbekämpande myndigheterna har deras utgångspunkter i frågan om kostnadernas fördelning varit olika. Leverantörerna ser lagringen av trafikuppgifter som en ”verksamhetsfrämmande” uppgift som de inte har någon nytta av och i princip inte bör betala för, medan de brottsbekämpande myndigheterna befarar att brottsbekämpningens effektivitet sätts i fara om statens kostnader blir för höga.

En samhällsekonomisk utgångspunkt för våra överväganden om kostnadernas fördelning bör vara att ansvaret för kostnaderna ska förläggas så att det ger ett incitament att hålla kostnaderna nere. För att syftet med lagringen av trafikuppgifter ska uppnås måste fördelningen av kostnaderna också göras så att kostnaderna i sig inte blir ett hinder som leder till att trafikuppgifterna inte används i de fall det är befogat. Ansvaret för kostnaderna bör således fördelas så att de lagrade trafikuppgifterna utnyttjas effektivt och fullt ut inom de ramar som rättegångsbalken och lagen om elektronisk kommunikation medger. Med andra ord bör kostnaderna för lagring och utlämnande av trafikuppgifter i möjligaste mån fördelas så att den som kan påverka kostnaden har ansvaret för den. Vi bör också söka efter en lösning som innebär så låga administrativa

kostnader som möjligt både för staten och för leverantörerna på marknaden för elektronisk kommunikation.

Erfarenheterna från andra länder visar att det i princip finns tre olika system som tillämpas för fördelning av kostnaderna. Systemen innebär antingen att staten betalar samtliga kostnader, att leverantörerna betalar samtliga kostnader eller att kostnaderna fördelas mellan staten och leverantörerna. I det följande presenteras tre modeller för hur kostnaderna skulle kunna fördelas med redovisning av de för- och nackdelar som varje modell medför. Därefter redovisar vi den modell som vi förordar för kostnadsfördelningen.

13.8.2 Olika modeller för kostnadsfördelning

Det allmänna står för alla kostnader

Genomförandet av direktivet om lagring av trafikuppgifter innebär att uppgifterna lagras enbart för att användas vid bekämpning av allvarliga brott. Det är medborgarna som har ett intresse av att allvarliga brott kan utredas och lagföras. Det är således det allmänna, genom medborgarna, men också företag och organisationer, som utifrån ett sådant resonemang måste sägas ha nytta av att trafikuppgifterna lagras. Lagringsskyldigheten kan med dessa utgångspunkter anses som en statlig angelägenhet som bör bekostas av det allmänna.

Eftersom det blir leverantörerna som faktiskt genomför lagringen av trafikuppgifterna, anpassar sina system och lämnar ut uppgifterna måste en ordning där staten skulle stå för alla kostnader innebära att leverantörerna får ersättning av staten för de kostnader de haft och framdeles har för lagring, anpassning och utlämnande av trafikuppgifter.

En fördel med att det allmänna står för samtliga kostnader är att kostnaderna för brottsbekämpningen blir tydligt avgränsade. Därmed skulle det också kunna bli möjligt att bedöma systemets kostnadseffektivitet utifrån användningen av de lagrade uppgifterna i brottsbekämpningen. En annan fördel med att staten skulle stå för kostnaderna är att inte en särskild sektor inom näringslivet skulle få bära en del av kostnaderna för brottsbekämpningen. En ytterligare fördel med att det allmänna skulle stå för alla kostnader skulle kunna vara att det skulle bli ett konkurrensneutralt system. Det förutsätter dock att staten kan fastställa exakt vad varje leverantör

ska utföra och också ersätter alla leverantörer på exakt samma sätt. En modell som har framförts som tänkbar är att staten skulle bestämma vilka nödvändiga standardinvesteringar som leverantörerna behöver vidta för att lagra de olika trafikuppgifterna och därefter ge ersättning till leverantörerna fördelat per kund och år. Det argument som har framförts för den modellen är att leverantörerna skulle ha incitament att lagra och lämna ut uppgifter till lägsta möjliga kostnad.

En modell som innebär att det allmänna står för samliga kostnader är också förenad med flera nackdelar. Om staten skulle betala alla kostnader skulle det med nödvändighet föra med sig att staten eller i praktiken de brottsbekämpande myndigheterna mer specifikt skulle behöva avgöra vilken teknik och vilka säkerhetsåtgärder som är nödvändiga för att genomföra lagringen. Det skulle i sin tur kräva att det allmänna byggde upp en enorm kompetens om den tekniska utvecklingen och detaljer rörande flera hundra leverantörers system och deras organisation med bl.a. säkerhetssystem. Alternativet skulle vara att det allmänna, utan att ha möjlighet att ifrågasätta kostnaderna eller påverka dem, betalade vad leverantören begärde eller att staten angav en fix summa och ”beställde en lösning” av varje leverantör. Ett ersättningssystem enligt någon av de skisserade modellerna skulle också medföra administrativa kostnader för både staten och leverantörerna. De administrativa kostnaderna skulle röra sig om upphandling, hur ersättningen skulle fördelas mellan olika leverantörer, vilka kostnader som skulle ersättas och andra liknande frågor. Ett system som innebär att det allmänna står för samtliga kostnader skulle ändå inte innebära någon garanti för att leverantörerna skulle anse sig rent faktiskt få ersättning för alla kostnader eller att den ersättning en leverantör skulle få blev rättvis i förhållande till andra leverantörer.

Oavsett vilken av de skisserade metoderna man väljer är det alltmänt sett förenat med en risk för att det inte i slutänden blir en samhällsekonomiskt effektiv kostnadsfördelning om den som ska betala kostnaderna inte har tillräcklig kunskap samtidigt som den som ska utföra uppdraget inte har något egentligt incitament att hålla kostnaderna nere.

Mot bakgrund av den mycket stora variationen mellan de leverantörer som är anmälningspliktiga och därmed lagringsskyldiga både avseende innehållet i deras verksamhet och storleken på verksamheten kan vi konstatera att det skulle vara mycket komplicerat

att hitta ett system där staten kan ersätta leverantörer för kostnader på ett sätt som blir både kostnadseffektivt och konkurrensneutralt.

Leverantörerna står för alla kostnader

Om leverantörerna skulle stå för kostnaderna skulle intresset av kostnadseffektiva lösningar för tekniska system, drift, administration och underhåll bli tydligt. Leverantörernas kunskap om sina respektive tekniska system och behov av nyanskaffningar och anpassningar, deras kunskap om systemens behov i drift och av underhåll samt om vilka säkerhetssystem som finns och vilka system som behöver utvecklas skulle därmed utnyttjas fullt ut och säkert leda till att kostnaderna kunde hållas nere.

Samtidigt finns det flera omständigheter som talar emot att leverantörerna skulle stå för samtliga kostnader. En sådan lösning av kostnadsfrågan skulle kunna kritiseras utifrån att det kan anses tveksamt om en viss sektor i näringslivet ska stå för kostnaderna för ett system som alla medborgare, företag och organisationer har nytta av. En annan sak som talar emot att enbart leverantörerna skulle stå för kostnaderna är att de i huvudsak inte har nytta av de uppgifter som lagringsskyldigheten omfattar, även om de redan i dag lagrar en del av de uppgifter som ska lagras enligt vårt förslag. Leverantörerna skulle därmed få en kostnad som antingen leder till minskad vinst eller till att kostnaderna måste tas ut av kunderna. Det skulle kunna få en hämmande effekt på leverantörernas vilja att genomföra lagringen på bästa sätt och samtidigt bli en risk för försämrad konkurrens på marknaden för elektronisk kommunikation. Om leverantörerna skulle stå för samtliga kostnader skulle det också kunna uppstå en viss osäkerhet kring frågan om lagringen utnyttjas effektivt av de brottsbekämpande myndigheterna. I effektivitetskravet ligger att lagrade trafikuppgifter ska utnyttjas så långt reglerna i rättegångsbalken och lagen om elektronisk kommunikation medger. Både ett överutnyttjande och ett underutnyttjande skulle innebära negativa konsekvenser för tilltron till systemet.

Vi kan således konstatera att en modell som innebär att leverantörerna står för samtliga kostnader också är förenad med flera komplicerade överväganden och att frågor om konkurrens och tilltron till systemet skulle behöva övervägas noggrant innan modellen kan utvecklas till att bli en kostnadseffektiv och konkurrensneutral lösning.

Kostnaderna fördelas mellan det allmänna och leverantörerna

En fördel med att fördela kostnaderna mellan det allmänna och leverantörerna är att det blir möjligt att dra nytta av det bästa med de två andra modellerna och förena de positiva faktorerna i en lösning. Ett delat kostnadsansvar leder till att leverantörernas tekniska och administrativa kapacitet på området för elektronisk kommunikation och deras incitament att hålla kostnaderna nere länkas till de brottsbekämpande myndigheternas incitament att använda trafikuppgifterna precist och på ett sätt som är effektivt för brottsbekämpningen. Det är också den lösning som leder till minst administrativa kostnader.

En modell som innebär att kostnaderna fördelas mellan det allmänna och leverantörerna kräver dock noggranna överväganden om hur fördelningen bör ske. Utgångspunkten för dessa överväganden bör vara att kostnadsansvaret ska ligga där det finns möjligheter att påverka kostnaderna. En fördelning som innebär så lite administration som möjligt och som minskar behovet av kostnadsfördelningsresonemang bör också eftersträvas.

Den nuvarande anpassningsskyldigheten i 6 kap. 19 § LEK bygger på en kostnadsfördelning mellan det allmänna och leverantörerna som innebär att leverantörerna står för kostnaderna för anpassning, drift och underhåll och de brottsbekämpande myndigheterna betalar en ersättning till leverantörerna vid varje utlämnande av uppgifter. Grunden för den kostnadsfördelningen är principiella överväganden om fördelningen av anpassningskostnader mellan det allmänna och leverantörerna när det gäller tillgång till viss del av leverantörernas verksamhet i brottsbekämpningen. Dessa överväganden har giltighet även för bedömningen av hur kostnaderna för genomförandet av våra förslag bör fördelas. Vi ser det som en fördel om samma principer för kostnadsfördelningen som har använts tidigare kan användas för kostnaderna för lagringsskyldigheten.

Vi bedömer att fördelarna med en modell där kostnaderna fördelas mellan det allmänna och leverantörerna är stora jämfört med de andra alternativ vi har prövat och vi bedömer att en sådan modell inte är förenad med några avgörande nackdelar. Det är därför den modell vi förordar. I följande avsnitt redovisar vi närmare våra överväganden om hur en sådan modell bör utformas.

13.8.3 Vårt förslag på hur kostnaderna ska fördelas

Vi förordar en modell som innebär en fördelning av kostnaderna för lagringen av trafikuppgifter.

Som vi nämnt bygger den nuvarande anpassningsskyldigheten i 6 kap. 19 § LEK på en kostnadsfördelning mellan det allmänna och leverantörerna, där leverantörerna står för kostnaderna för anpassning, drift och underhåll av systemen och de brottsbekämpande myndigheterna betalar en ersättning till leverantörerna vid varje utlämnande av uppgifter. När den kostnadsfördelningen infördes anförde regeringen att det finns en rad verksamhetsområden där samhället som förutsättning för att få idka näring kräver att vissa samhälleliga intressen beaktas (prop. 1995/96:180 s. 31 ff.). Som exempel angavs arbetsgivares skyldighet att uppbära, redovisa och inbetala preliminär skatt för anställda och miljöfarlig verksamhet där företagen måste investera stora summor för att minimera de skador som kan följa med verksamheten. Regeringen menade att det inte fanns någon avgörande principiell skillnad mellan dessa förpliktelser och en förpliktelse att på egen bekostnad anpassa telesystemen så att möjligheterna till hemlig teleavlyssning och hemlig teleövervakning bibehålls. Regeringen anförde vidare att hemlig teleavlyssning och hemlig teleövervakning inte kunde sägas inta någon särställning i detta hänseende endast på den grunden att det rör sig om brottsbekämpande verksamhet. Regeringen uttryckte att det redan fanns lagstadgade skyldigheter för företag att vidta vissa åtgärder för att underlätta den brottsbekämpande verksamheten. Som exempel nämndes bankernas uppgiftsskyldighet enligt lagen (1993:768) om åtgärder mot penningtvätt. En anpassning av de tekniska systemen hos leverantörerna skulle betraktas som helt skild från den brottsbekämpande verksamheten i form av de enskilda förundersökningar där tvångsmedel aktualiseras.

Regeringen anförde att leverantörerna skulle stå för anpassningskostnaderna, men underströk samtidigt att denna princip inte innebar att polisen fritt fick bestämma vilka anpassningar som skulle göras. Vilka anpassningar som ålåg respektive leverantör skulle fastslås av PTS i beslut om tillståndsvillkor. Tillståndsmyndigheten skulle vid sin prövning beakta nyttan av en anpassning mot kostnaden för denna, samt även beakta om anpassningen gjordes i ett befintligt telesystem eller om det var krav som ställdes i samband med byte till ny teknik.

Vidare fann regeringen att när det gällde kostnaderna för ett utlämnande av uppgifter i det enskilda fallet borde polisen för varje enskild verkställighetsåtgärd betala en ersättning till leverantörerna. Regeringen menade att de brottsbekämpande myndigheterna också i fortsättningen borde få väga kostnaderna och fördelarna med dessa tvångsmedel mot kostnaderna och fördelarna med andra åtgärder som kan komma i fråga. Regeringen fann inte skäl att reglera vilken ersättning som skulle utgå. Tvärtom utgick regeringen från att leverantörerna och polisen själva skulle lösa detta (prop. 1995/96:180 s. 29 f.).

Den lagringsskyldighet och anpassningsskyldighet som vi föreslår blir endast en del av det regelsystem som redan gäller enligt rättegångsbalken och lagen om elektronisk kommunikation. Med denna utgångspunkt måste starka skäl anses tala för att kostnaderna ska fördelas på samma sätt som enligt det redan nu gällande systemet. Vi förordar därför en modell som innebär att leverantörerna ska stå för kostnaderna för lagring, säkerhet och anpassning av systemen och att det allmänna ska betala ersättning till leverantörerna när uppgifter lämnas ut.

Med en sådan fördelning uppnår man fördelen att leverantörerna genom sin kunskap och kompetens om de egna systemen och om den tekniska anpassning som behöver göras kan hålla kostnaderna nere. Samtidigt får de brottsbekämpande myndigheterna betala för utlämnandet av just de trafikuppgifter som har en direkt koppling till uppgiften att utreda och lagföra allvarlig brottslighet. Därmed skapas ett incitament för myndigheterna att förena de rättssäkerhetsöverväganden som görs vid användning av hemliga tvångsmedel och inhämtande av uppgifter enligt lagen om elektronisk kommunikation med överväganden som innebär att lagrade trafikuppgifter används på ett kostnadseffektivt sätt.

Den modell vi förordar innebär också att vi kommer att ha en fördelning av kostnaderna som liknar den modell som flertalet av de länder vi har kunskap om har valt.

13.8.4 Ersättning för utlämnande av trafikuppgifter

Den modell för fördelningen av kostnaderna som vi förordar innebär att ansvaret för kostnaderna och möjligheterna att påverka kostnaderna hänger ihop. När principerna för den ersättning som myndigheterna ska betala för utlämnande av trafikuppgifter ska

bestämmas bör det ske med utgångspunkt i att leverantörerna ska få sina kostnader för att lämna ut trafikuppgifter i enskilda ärenden ersatta. Samtidigt går det inte att komma ifrån att om kostnaderna för de brottsbekämpande myndigheterna blir för höga så kan det påverka deras möjligheter att effektivt bedriva brottsutredningar och använda lagrade trafikuppgifter som det är tänkt. Det låter sig inte göras att exakt beräkna vad varje enskilt utlämnande av trafikuppgifter från leverantörerna till de brottsbekämpande myndigheterna innebär för kostnader och använda beräkningen för att hitta principerna för ersättning. Kostnaderna varierar mellan olika leverantörer, bl.a. beroende på vilka uppgifter som begärs ut och när verkställigheten ska ske.

För både leverantörerna och de brottsbekämpande myndigheterna måste det vara en fördel om ersättningen för utlämnande av trafikuppgifter kan regleras på enklaste sätt. Om ersättningen ska bestämmas för varje enskilt ärende leder det till administrativa kostnader för båda parter och det riskerar dessutom att hämma effektiviteten både i leverantörernas och de brottsbekämpande myndigheternas verksamheter. Ersättningens storlek bör därför bestämmas enligt vissa schabloner som bygger på beräkningar av leverantörernas kostnader i olika typer av ärenden.

Hittills har ersättningen vid utlämnande av uppgifter bestämts generellt efter förhandlingar mellan Säkerhetspolisen och de största leverantörerna eller, när sådant avtal inte funnits, efter förhandling mellan den brottsbekämpande myndigheten och leverantören i det enskilda fallet. Att t.ex. Säkerhetspolisen för förhandlingar med leverantörerna för de brottsbekämpande myndigheternas räkning skulle kunna vara ett alternativ för att fastställa generella ersättningsbelopp även i fortsättningen. Vi har dock förstått att det har varit mycket svårt för Säkerhetspolisen och de största leverantörerna att komma överens och förhandlingarna har varit både resurskrävande och tidsödande. Säkerhetspolisen har generella avtal med mindre än en handfull leverantörer. Enligt uppgift tog det mellan två och tre år av ständigt pågående förhandlingar innan överenskommelserna nåddes. De överenskommelser som har träffats gäller inte heller alla leverantörer.

Lagringsskyldigheten kommer att gälla hundratals leverantörer och det går inte i förväg att göra ett säkert antagande om vilka av dem som kommer att lämna ut uppgifter eller i vilken omfattning. Enligt vår bedömning skulle det bli orimligt med en ordning som innebär att mycket stora resurser såväl hos leverantörerna som hos

de brottsbekämpande myndigheterna skulle behöva läggas ned för att bestämma schablonersättningar för olika typer av utlämnanden när samtidigt inte samtliga leverantörer blir bundna av det som överenskoms. Ett alternativ skulle kunna vara att Säkerhetspolisen fick förhandla med leverantörerna som ett kollektiv t.ex. genom en branschorganisation. På så sätt skulle ersättningens storlek bli densamma för alla leverantörer som är anslutna till organisationen eller som har deltagit vid förhandlingen. Vi har dock kunnat konstatera att det inte finns något branschorgan som liknar t.ex. det som finns i Danmark och det är tveksamt om det finns någon på leverantörssidan som skulle kunna förhandla för de övriga. En överenskommelse skulle heller inte bli bindande för de leverantörer som inte varit med och således inte reglera ersättningsfrågorna fullt ut.

Det av resurs- och tidsskäl överlägset bästa sättet att reglera ersättningsnivån är att tillsynsmyndigheten (PTS) fastställer schabloner och ger riktlinjer för vad som ska gälla i de situationer där det finns anledning att avvika från schablonerna. Ett system med schablonersättning ger en enkel och snabb handläggning för både leverantörer och de brottsbekämpande myndigheterna. Schablonersättningar med förutbestämda nivåer för ersättningen ger också minskade administrationskostnader och möjliggör en effektiv handläggning. Genom att ersättningens storlek är bestämd på förhand är den också förutsebar för alla parter. En på det sättet bestämd ersättning kommer givetvis inte att exakt motsvara kostnaden i varje enskilt ärende. Det ligger i sakens natur att leverantörerna ibland kommer att få en högre ersättning än vad deras kostnader kanske motiverar och att de ibland får en något lägre ersättningen än vad som motsvarar deras kostnader. Om avvikelserna blir för stora bör dock schablonersättningen inte tillämpas utan en ersättning bestämmas till ett belopp som motsvarar kostnaderna i det enskilda fallet.

För att uppnå effektivitet och förutsebarhet bör schablonerna gälla under relativt lång tid. En förebild kan vara den ordning som gäller för fastställande av ersättning till exempelvis rättshjälpsbiträden enligt 27 § rättshjälpslagen (1996:1619) och till offentliga försvarare enligt 21 kap. 10 § RB. I de fallen har regeringen föreskrivit i 19 § rättshjälpsförordningen (1997:404) respektive 2 § förordningen (1997:406) om offentlig försvarare m.m. att Domstolsverket fastställer taxor för ersättningen.

Utgångspunkten vid bestämmandet av schablonerna bör vara att leverantörerna ska få ersättning för sina kostnader. Vi har i avsnitt

13.6.3 identifierat de kostnader som uppstår för leverantörerna när uppgifter lämnas ut. Det är fråga om kostnader för tekniska system för att enkelt kunna söka efter de uppgifter som en begäran om utlämnande omfattar och kostnader för drift och underhåll av systemen. Det är också fråga om kostnader för den personal som ska hantera och lämna ut uppgifterna samt kostnader för att hitta ett gemensamt gränssnitt till mottagaren så att uppgifterna enkelt kan lämnas ut. Andra faktorer som skulle kunna påverka nivån för schablonbeloppen är vilka typer av uppgifter som efterfrågas (om det avser fast eller mobil telefoni eller Internet), det antal trafikuppgifter som begäran avser och hur många utlämnanden som måste ske samt tidpunkten när utlämnande begärs och när det verkställs. Schablonbeloppen bör bestämmas utifrån de kostnader som en leverantör med goda rutiner har i samband med utlämnande av trafikuppgifter.

För att ge de brottsbekämpande myndigheterna möjlighet att påverka hur schablonbeloppen bestäms och insyn i beräkningen bör de fastställas efter samråd med de myndigheter som har ärenden om hemlig teleövervakning och utlämnanden enligt lagen om elektronisk kommunikation. Även leverantörernas synpunkter bör naturligtvis inhämtas.

Vi vill tydliggöra att det vid hemlig teleövervakning är möjligt för de brottsbekämpande myndigheterna att få tillgång till såväl historiska uppgifter som uppgifter framåt i tiden från det att myndigheten begärde verkställighet (realtidsuppgifter, se avsnitt 2.3.1). Det ingår inte i vårt uppdrag att författningsreglera ersättningen vid utlämnande av realtidsuppgifter enligt reglerna om hemlig teleövervakning. Den reglering vi föreslår avser således endast de historiska uppgifterna, dvs. alla uppgifter som inte fortlöpande läses av. Eftersom hemlig teleövervakning ofta omfattar såväl historiska uppgifter som realtidsuppgifter, måste tillsynsmyndigheten ta hänsyn till detta när ersättningens storlek bestäms i föreskrifter. Avsikten är inte att leverantören i de fallen ska få dubbla ersättningar, dels för de historiska uppgifterna enligt föreskrifterna, dels för realtidsuppgifter enligt avtal mellan de brottsbekämpande myndigheterna och leverantörerna. Det bör också tydliggöras att ersättningen inte kommer att gälla för de fall andra uppgifter lämnas ut vid hemlig teleövervakning eller enligt lagen om elektronisk kommunikation än dem som lagras enligt vårt förslag.

14 Konkurrens

14.1 Sammanfattning av våra bedömningar

- Lagringsskyldigheten innebär en viss inverkan på konkurrensen.
- Möjligheten att ge undantag från skyldigheten att lagra trafikuppgifter och att anlita annan för att fullgöra lagringen kan mildra effekterna för de små leverantörerna och därmed ge minskad negativ effekt på deras investeringsvilja och möjligheter att stanna kvar på marknaden.

14.2 Inledning

Våra förslag innebär att leverantörerna ska stå för kostnaderna för att identifiera, spara och lagra trafikuppgifter med en hög säkerhet och att de brottsbekämpande myndigheterna ska ersätta leverantörerna när uppgifter lämnas ut.

Som våra direktiv förutsätter har vi vid utformningen av våra förslag beaktat behovet av en väl fungerande konkurrens på marknaden i allmänhet samt förslagens inverkan på konkurrensen mellan stora och små aktörer och hur förslagen påverkar möjligheterna till marknadstillträde. Vi har också tagit hänsyn till hur förslagen påverkar såväl etablerade som presumtiva aktörers investeringsvilja.

I detta kapitel redogör vi först övergripande för gällande konkurrensregleringar inom marknaden för elektronisk kommunikation. Därefter ges en översiktlig beskrivning av marknadsförhållandena inom olika områden och hur konkurrensen utvecklats. Slutligen redogör vi för hur kostnaderna för våra förslag kan väntas påverka företags möjligheter att träda in på marknaden och konkurrensen mellan stora och små företag.

14.3 Gällande konkurrensregleringar

14.3.1 Generella regler i konkurrenslagen

Konkurrenslagen (1993:20) innehåller generella regler på konkurrensområdet. Konkurrenslagens ändamål är att undanröja och motverka hinder för en effektiv konkurrens i fråga om produktion av och handel med varor, tjänster och andra nyttigheter. Lagen bygger på den konkurrensrättsliga förbudsprincipen som innebär att vissa åtgärder anses vara konkurrensbegränsande och därmed så skadliga att de förbjuds. Konkurrenslagens grundläggande materiella bestämmelser utgörs av de generella förbuden mot dels konkurrensbegränsande samarbete mellan företag (6 §), dels missbruk av företags dominerande ställning (19 §). Från förbudet mot konkurrensbegränsande samarbete mellan företag finns vissa undantagsbestämmelser (8, 8 a, 18 c och 18 e §§).

Enligt 6 § är avtal mellan företag förbjudna om de har till syfte att hindra, begränsa eller snedvrida konkurrensen på ett märkbart sätt eller om de ger ett sådant resultat. I bestämmelsens andra stycke anges vissa avtal som typiskt sett är märkbart konkurrensbegränsande, t.ex. avtal som innebär att produktion, marknader, teknisk utveckling eller investeringar begränsas eller kontrolleras. Med avtal jämställs enligt 3 § samordnade förfaranden och beslut av en sammanslutning av företag.

Förbudet mot missbruk av dominerande ställning i 19 § riktar sig mot åtgärder som företag med dominerande marknadsställning vidtar mot andra företag eller konsumenter. Till skillnad från 6 § handlar förbudet i 19 § om ett företags eller en företagsgrupps ensidiga agerande. För att ett förfarande ska vara förbjudet krävs att ett eller flera företag dels har en dominerande ställning på marknaden, dels missbrukar denna ställning. I bestämmelsens andra stycke exemplifieras vissa förfaranden som kan utgöra missbruk. Med begreppet dominerande ställning avses en stark ekonomisk ställning som möjliggör att ett företag agerar oberoende i förhållande till konkurrenter, kunder och i sista hand konsumenter.

Förbuden mot konkurrensbegränsande samarbete och missbruk av dominerande ställning används för att komma till rätta med observerade förfaranden på marknaden i efterhand. Genom att förbudsbestämmelserna och risken för sanktioner vid överträdelser påverkar företagens agerande får bestämmelserna också en preventiv effekt. Ett ingripande med stöd av lagen mot t.ex. ett företags missbruk av en dominerande ställning innebär inte bara att det do-

minerande företagets agerande stoppas utan det sänder också en signal till dominerande företag på andra marknader.

14.3.2 Specifika regler i lagen om elektronisk kommunikation

När marknaden för elektronisk kommunikation år 1993 öppnades för konkurrens övervägdes om en sektorspecifik särreglering skulle införas eller om de generella konkurrensrättsliga reglerna i konkurrenslagen skulle vara tillräckliga för en fungerande konkurrens på marknaden för elektronisk kommunikation. Telelagen kom till mot bakgrund av att man bedömde att en särreglering var nödvändig. År 2003 ersattes Telelagen, med anledning av ny EG-reglering, av lagen om elektronisk kommunikation. Lagen om elektronisk kommunikation är en tämligen långtgående reglering som avser att skapa förutsättningar för en fungerande konkurrens.

Syftet med lagen är att skapa en enhetlig och teknikneutral lagstiftning för all elektronisk kommunikation så att enskilda och myndigheter ska få tillgång till säkra och effektiva (konkurrensutsatta och flexibla) elektroniska kommunikationer och så att de elektroniska kommunikationerna ska ge största möjliga utbyte när det gäller urvalet av överföringstjänster samt deras pris och kvalitet. Syftet ska främst uppnås genom att skapa förutsättningar för en effektiv konkurrens och främja den internationella harmoniseringen på området.

Lagen innehåller verktyg för att främja en sund konkurrens i de fall konsumenternas behov inte tillgodoses av marknaden eller då konkurrensen riskerar att påverkas negativt. Ett sådant verktyg är regleringen om samtrafik. Att samtrafik mellan leverantörerna finns är en grundläggande förutsättning för att abonnenterna hos olika leverantörer ska kunna nå varandra. När en abonnent som har abonnemang hos en viss mobilleverantör ringer en abonnent hos en annan mobilleverantör krävs att leverantörernas nät är sammankopplade och att samtal kan kopplas fram. Samtrafik är också en förutsättning för att nya leverantörer ska kunna komma in på marknaden. I 4 kap. 1 § föreskrivs därför en skyldighet att förhandla om samtrafik med den som tillhandahåller eller avser att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster. Den som kontrollerar tillträde till slutanvändare kan också enligt 4 kap. 3 § förpliktas att bedriva samtrafik på marknadsmässiga villkor för att säkerställa att slutanvändare kan nå varandra. PTS kan ge-

nom tillsyn säkerställa att samtrafikavgifterna är kostnadsorienterade.

I 4 kap. 4-12 §§ finns bestämmelser om förpliktelser som, om det anses nödvändigt för att skapa en fungerande konkurrens, kan åläggas den som bedöms ha ett betydande inflytande på en viss bestämd marknad. Reglerna innebär att en leverantör kan förpliktas att i ett referenserbjudande eller på annat sätt offentliggöra vissa uppgifter, att tillämpa icke-diskriminerande villkor, att särredovisa och rapportera specificerad verksamhet med anknytning till samtrafik och andra former av tillträde, att uppfylla rimliga krav på tillträde till och användning av nät och tillhörande installationer i syfte att tillhandahålla elektroniska kommunikationstjänster samt att i vissa fall iaktta kostnadstäckning eller tillämpa kostnadsorienterad eller annan prissättning för specificerade typer av samtrafik och andra former av tillträde. Förpliktelsen kan också avse tillämpning viss kostnadsredovisningsmetod.

Av 8 kap. 5-7 §§ framgår att PTS fortlöpande ska fastställa vilka produkt- och tjänstemarknader som har sådana särdrag att det kan vara motiverat att införa skyldigheter enligt lagen. Kommissionen har i en rekommendation över relevanta produkt- och tjänstemarknader identifierat olika marknader som bör analyseras för att fastställa om det råder effektiv konkurrens eller om någon aktör har betydande inflytande på en marknad (2003/311/EG). Om det finns företag med ett betydande inflytande på de marknader som identifierats i kommissionens rapport kan PTS ålägga det företaget särskilda skyldigheter enligt 4 kap. 4-12 §§ och 5 kap. 13 och 14 §§ för att åtgärda konkurrensproblemen. Skyldigheterna ska vara proportionella vilket innebär minsta nödvändiga ingripande för att nå ett uppställt mål. Om PTS konstaterar att det inte finns någon aktör med betydande inflytande på den identifierade marknaden kan inte några skyldigheter åläggas. Om det råder effektiv konkurrens ska tidigare fattade beslut om skyldigheter upphävas.

PTS har meddelat ett antal beslut där främst TeliaSonera har bedömts ha ett betydande inflytande på flera av de marknader som kommissionen har identifierat, bl.a. på marknaderna för tillträde till det fasta telenätet och bitströmstillträde, och därmed ålagt företaget olika skyldigheter. Flera av PTS beslut har dock överklagats och därmed inte trätt i kraft.

14.4 Konkurrensen på marknaden för elektronisk kommunikation

Enligt statistik från SCB:s företagsregister uppgick antalet företag som tillhandahåller elektroniska kommunikationstjänster och nät inom näringsgrenen 64201 (nätdrift samt underhåll inom telekommunikation)[1] till 487 år 2005. Cirka 80 procent av dessa företag var förhållandevis små och hade en inhemsk omsättning som uppgick till högst 9,9 miljoner kronor. Drygt 6 procent av företagen hade en inhemsk omsättning mellan 10 och 19,9 miljoner kronor och knappt 5 procent hade en omsättning mellan 20 och 49,9 miljoner kronor. Vidare hade knappt 2 procent en inhemsk omsättning mellan 50 och 99,9 miljoner kronor och knappt 4 procent hade en inhemsk omsättning mellan 100 och 499,9 miljoner kronor. Drygt 4 procent hade en omsättning som översteg 500 miljoner kronor.

Den snabba tekniska utvecklingen inom olika delar av marknaden för elektronisk kommunikation och den ökade konkurrensen har lett till kraftiga prissänkningar och till ett större och mer varierat utbud av teleprodukter. Utvecklingen har gjort det möjligt för nya företag att anlägga egna nät, dvs. duplicera (delar av) infrastrukturen och utveckla nya produkter. Enligt statistik från SCB har konsumentpriserna för teletjänster och teleutrustning minskat med ca 28 procent mellan åren 1993 och 2006. Under motsvarande period har KPI ökat med ca 17 procent. Detta betyder att priserna för teletjänster och teleutrustning, jämfört med KPI, fallit med drygt 38 procent.

Enligt PTS uppgick den sammanlagda omsättningen på marknaden för elektronisk kommunikation år 2006 till knappt 49 miljarder kronor. Intäkter från fasta samtalstjänster (inklusive fasta avgifter) utgjorde ca 40 procent av omsättningen medan mobila samtalstjänster svarade för ca 35 procent. Ca 25 procent av intäkterna härrörde från datakommunikations- och Internettjänster.[2]

I det följande ges en översiktlig beskrivning av antalet leverantörer och hur omsättningen fördelas mellan leverantörer av olika storlek. För ingående beskrivningar av andra marknadsförhållanden hänvisas till rapporter från bl.a. PTS.

[1] Näringsgren 64201 omfattar styrning, kontroll och felhantering av telenät och mobilradiosystem, tillhandahållande av telefon-, telegram-, telex- och datakommunikationstjänster o.d. samt Internetaccess.
[2] Uppgifterna är hämtade från Svensk telemarknad 2006

14.4.1 Fasta samtalstjänster

Marknaden för fasta samtalstjänster har, såsom den definierats i PTS statistikrapporter, förändrats påtagligt sedan marknaden öppnades för konkurrens år 1993. När det skedde svarade Telia för i princip hela marknaden. Förvalsreformen och införandet av nummerportabilitet har bidragit till att öka konkurrensen och numera finns ett stort antal leverantörer som konkurrerar med TeliaSonera. Enligt PTS tillhandahöll närmare 75 leverantörer under år 2006 fasta samtalstjänster (inklusive IP-baserad telefoni)[3]. Ungefär 30 leverantörer var dock verksamma enbart gentemot företagskunder.

Marknadsandelarna kan beräknas på basis av antalet abonnemang, intäkter, trafikminuter eller antalet samtal. Vidare kan en uppdelning göras i olika kundkategorier. Oavsett vilken av dessa variabler som används vid beräkningen blir resultatet att tio leverantörer svarar för närmare 90 procent av marknaden. Dessa får betecknas som (relativt) stora leverantörer och vissa ingår dessutom i samma koncern. T.ex. ägs både Glocalnet och Bredbandsbolaget av norska Telenor. Den störste leverantören TeliaSonera, svarar i genomsnitt för närmare 60 procent av marknaden när beräkningen görs som ett ovägt genomsnitt av alla variablerna. I jämförelse med de tio största leverantörerna är övriga leverantörer förhållandevis små.

14.4.2 Mobila samtalstjänster

Alltsedan GSM-näten togs i bruk under år 1992 har det rått konkurrens på marknaden för infrastruktur (radioaccessnät). Av samtliga mobilteleleverantörer i Sverige är det sex som har egna mobilnät; TeliaSonera, Tele2, Telenor, Hi3G (3), Spring Mobil och Nordisk Mobiltelefon. Enligt PTS tillhandahöll omkring 20 leverantörer mobila teletjänster under år 2006. Några av dessa vänder sig enbart till företagskunder.

Baserat på totala intäkter svarade fyra, relativt sett stora leverantörer (och nätägare) för drygt 95 procent av marknaden år 2006. Leverantören 3:s marknadsandel har stadigt ökat sedan inträdet år 2003.

PTS konstaterar i rapporten Svensk telemarknad 2006 att fristående tjänstetillhandahållare (med undantag för leverantören Djuice

[3] Detta definieras av PTS som sådan IP-baserad telefoni där en traditionell telefon kan anslutas till accessnätet.

som köpts upp av Telenor) ytterst marginellt kunnat påverka priskonkurrensen på den svenska marknaden. Detta beror enligt PTS dels på utformningen av tredjepartsavtalen med mobilnätsleverantörerna, dels på att mobilleverantörerna har kunnat välja bort de tjänstetillhandahållare som utgjort ett hot mot den egna verksamheten.

Trots detta har konkurrensen under senare år ökat, vilket bl.a. hänger samman med leverantören 3:s inträde på marknaden och Telenors etablering i Sverige. En annan faktor som bidragit till ökad konkurrens är införandet hösten 2001 av nummerportabilitet för digital mobiltelefonitjänst. Sedan reformen trädde i kraft har antalet porteringar stadigt ökat och i slutet av juli 2007 hade närmare 2 500 000 nummer porterats.

Sammantaget kan sägas att det råder konkurrens på marknaden och att det har blivit allt billigare att ringa mobilsamtal. Internationell statistik visar att Sverige (tillsammans med övriga nordiska länder) tillhör de länder där mobilleverantörer erbjuder de billigaste abonnemangsformerna. Mobilleverantörerna marknadsför många olika abonnemangstyper till varierande priser och valmöjligheterna har också ökat betydligt.

14.4.3 Datakommunikations- och Internettjänster

Marknaden för bredbandsaccess innefattar dels datakommunikationstjänster, dels Internettjänster. Marknaden kan vidare delas upp beroende på vilka kundkategorier som tjänsterna vänder sig till. Det finns ett stort antal leverantörer som erbjuder abonnemang via olika tekniker eller olika tekniska lösningar. Enligt PTS fanns det under år 2006 minst 130 leverantörer som tillhandahöll datakommunikationstjänster och det fanns minst 170 leverantörer som tillhandahöll Internetaccess. En relativt stor andel av de sistnämnda är små och lokalt verksamma. Den genomsnittliga omsättningen för dessa leverantörer var knappt 7 miljoner kronor, enligt uppgifter från PTS.

Marknaden är i hög grad fragmenterad. Som exempel på det kan nämnas de lokala IT-infrastrukturer, s.k. stadsnät, som många kommuner har utvecklat. Enligt Svenska Stadsnätsföreningen har majoriteten av kommunerna lokalt etablerade stadsnät. Den vanligaste accessformen i Sveriges stadsnät är fiberanslutningar. Av företrädare för stadsnäten har 40 procent uppgett att de tillhandahål-

ler bredbandsbaserade tjänster, vanligen Internetaccess, i egen regi och i eget namn.

När det gäller Internettjänster svarar enligt PTS sju av marknadens största leverantörer för närmare 85 procent av marknaden. Tre av leverantörerna ingår i samma koncern. TeliaSonera är den största leverantören på marknaden med en marknadsandel om cirka 40 procent.

14.5 Inverkar våra förslag på konkurrensen?

Bedömning: Lagringsskyldigheten innebär en viss inverkan på konkurrensen.

Möjligheten att ge undantag från skyldigheten att lagra trafikuppgifter och att anlita annan för att fullgöra lagringen kan mildra effekterna för de små leverantörerna och därmed ge minskad negativ effekt på deras investeringsvilja och möjligheter att stanna kvar på marknaden.

14.5.1 Kostnader för att identifiera, spara och lagra uppgifter

Marknadstillträde för nya leverantörer

En viktig faktor för ett företags möjligheter att träda in på en marknad är de beräknade etableringskostnaderna för nödvändiga tekniska investeringar (t.ex. utrustning av olika slag) och kostnaderna för lokaler, personal etc. Stora etableringskostnader medför en högre finansiell risk som i sin tur motiverar krav på högre avkastning.

Vid tillträde på marknaden har ett företag alltid kostnader för att anskaffa den tekniska utrustning som verksamheten kräver. Om tekniska system tas fram som standard och uppfyller de krav som direktivet om lagring av trafikuppgifter ställer är det vår bedömning att merkostnaden för de nödvändiga lagringsfunktionerna blir låg i förhållande till etableringskostnaden i övrigt. För de företag som vill träda in på marknaden inom en relativt snar framtid finns det därför inte något skäl att räkna med att kostnaderna för tekniska system blir något ytterligare etableringshinder. Vi bedömer inte heller att kostnaderna för drift och underhåll eller administrativa kostnader kommer att vara så stora att de isolerat skulle utgöra något etableringshinder. Vår samlade bedömning blir således att våra

förslag inte kommer att påverka nya leverantörers möjligheter till marknadstillträde eller investeringsvilja.

Etablerade leverantörer

De totala kostnaderna för lagringsskyldigheten är mycket begränsade i förhållande till marknadens omsättning. Det innebär att marknaden som helhet torde påverkas endast marginellt av att lagringsskyldigheten införs. Detta säger dock inte något om hur enskilda företag påverkas och hur enskilda företags agerande kan påverka konkurrensen på marknaden.

Frågan om hur konkurrensen mellan stora och små företag påverkas för redan etablerade leverantörer måste i stället bedömas mot bakgrund av konkurrensförhållandena på marknaden för elektronisk kommunikation och med hänsyn till den mycket stora variation i de verksamheter som de leverantörer som omfattas av lagringsskyldigheten bedriver. Vissa leverantörer tillhandahåller nät, andra tillhandahåller tjänster och en del tillhandahåller både nät och tjänster. Vissa leverantörer har en mycket omfattande verksamhet med många kunder och stort verksamhetsområde medan andra bedriver en begränsad lokal verksamhet. Variationerna är också stora mellan leverantörernas tekniska system. Vissa leverantörer har system som redan till stor del kan vara anpassade till de regler vi föreslår medan andra leverantörers system kräver relativt sett större investeringar. Investeringskostnaderna för två verksamheter som utåt sett är likartade till innehåll och omfattning kan variera. Marknaden kännetecknas också av en snabb teknisk utveckling och marknadsdynamik och förändras hela tiden.

Mot den bakgrunden är det svårt för oss att med tillräcklig grad av säkerhet dra någon slutsats om vilka effekter lagringsskyldigheten får för konkurrensen mellan de redan etablerade leverantörerna. Våra bedömningar måste därför stanna vid ett antal antaganden som bygger på de faktorer som vi faktiskt kan bedöma.

Kostnaderna för ny teknik, anpassning av befintlig teknik, drift och underhåll samt administration och kostnadernas betydelse är till viss del beroende av verksamhetens omfattning. De kostnader som de stora leverantörerna får för att genomföra lagringsskyldigheten är relativt sett låga i förhållande till deras omsättning. För de stora leverantörerna kan vi inte se att kostnaderna är av sådan betydelse att de kommer att påverka deras möjlighet att finnas kvar på

marknaden och därmed påverka konkurrensen. De stora leverantörernas investeringsvilja kan dock påverkas när nya tjänster införs.

När det däremot gäller de leverantörer som bedriver verksamhet av begränsad omfattning kan kostnaderna för att genomföra lagringsskyldigheten vara en relativt stor del av deras omsättning. Kostnaderna för de små leverantörerna ökar också relativt sett mer än för de stora leverantörerna. Det medför att det finns en risk för att ökade kostnader, om de blir för höga, kan leda till att leverantörerna blir tvungna att träda ut från marknaden, vilket i så fall kan leda till en minskad konkurrens. De små leverantörerna kan alltså bedömas ha en nackdel i konkurrenshänseende i förhållande till de stora leverantörerna

Sådana eventuella negativa effekter kan emellertid mildras. Vi föreslår att PTS ska ha möjlighet att efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen i enskilda fall medge undantag från lagringsskyldigheten (se avsnitt 7.2.3). Undantagen är tänkta för situationer när leverantören bedriver en verksamhet av så liten omfattning att det vid en avvägning mellan det brottsbekämpande intresset av att leverantören lagrar uppgifter och kostnaden för detta inte framstår som rimligt att kräva att leverantören fullgör lagringsskyldigheten. En leverantör kan också i stället för att själv bära hela kostnaden för investeringar, för drift och underhåll och administration anlita någon annan för att fullgöra lagringen (se avsnitt 7.5). Genom att anlita annan kan den lagringsskyldige minska sina kostnader om den anlitade har en sådan volym på verksamheten att lagringen kan skötas mer effektivt. Vi bedömer att dessa båda möjligheter kan mildra effekterna för de små leverantörerna och därmed ge minskad negativ effekt på deras investeringsvilja och möjligheter att stanna kvar på marknaden.

14.5.2 Kostnader för att lämna ut uppgifter

Vi har föreslagit att de brottsbekämpande myndigheterna ska lämna ersättning till leverantörerna när trafikuppgifter lämnas ut. Utgångspunkten är att ersättningen ska täcka de kostnader som en begäran om utlämnande har orsakat. Vi bedömer att leverantörernas kostnader för att lämna ut trafikuppgifter och den ersättning som de brottsbekämpande myndigheterna betalar inte bör innebära några nämnvärda effekter för konkurrensen eller begränsa möjligheterna till marknadstillträde. Kostnaderna för utlämnande av trafikuppgifter och ersättningen för dessa kostnader torde inte heller

påverka etablerade eller presumtiva leverantörers investeringsvilja negativt.

14.5.3 Konkurrensen i ett EU-perspektiv

Flera av de leverantörer som omfattas av lagringsskyldigheten har verksamhet i ett eller flera andra länder. Konkurrensförhållandena inom och mellan olika EU-länder torde påverkas av hur enskilda länder reglerar lagringsskyldigheten och av hur principerna för kostnadsansvaret bestäms i de olika medlemsländerna. För att konkurrensfrågorna ska kunna bedömas i ett EU-perspektiv krävs ingående kännedom om förhållandena i varje medlemsland. Det har inte varit möjligt att göra den bedömningen inom ramen för vårt uppdrag. Vi kan dock konstatera att den lagringstid vi föreslår överensstämmer med den lagringstid som har bestämts eller övervägs i många andra medlemsländer. Också våra förslag om fördelning av kostnader liknar vissa av de system som tillämpas eller övervägs i andra länder.

15 Statistik

15.1 Sammanfattning av våra förslag

- Statistik ska föras över
  – antalet verkställda beslut om hemlig teleövervakning respektive utlämnanden enligt lagen om elektronisk kommunikation,
  – vilka typer av brott som ärendena har avsett,
  – hur lång tid som har förlöpt från det att respektive trafikuppgift lagrades till dess att den brottsbekämpande myndigheten begärde tillgång till uppgiften och
  – antalet ärenden där myndigheternas begäran om att få tillgång till trafikuppgifter inte har kunnat tillgodoses av leverantörerna samt vilka typer av brott ärendena har avsett.
- För de ärenden som handläggs av Säkerhetspolisen och som rör rikets säkerhet ska det inte föras någon statistik.
- De brottsbekämpande myndigheterna ska ansvara för statistiken. Uppgifterna ska sammanställas av Rikspolisstyrelsen och rapporteras till regeringen.

15.2 Behovet av statistik

Enligt artikel 10 i direktivet om lagring av trafikuppgifter ska medlemsstaterna säkerställa att kommissionen varje år får statistik om lagring av de uppgifter som genereras eller behandlas i samband med allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät. Statistiken ska innefatta följande.

1. De fall där information skickats till behöriga myndigheter i enlighet med nationell lagstiftning.

2. Den tid som gått från det datum då uppgifterna lagrades och det datum då den behöriga myndigheten begärde överförande av uppgifterna.

3. De fall där en begäran om uppgifter inte kunde tillgodoses.

Enligt artikel 14 i direktivet om lagring av trafikuppgifter ska kommissionen senast den 15 september 2010 till Europaparlamentet och rådet översända en utvärdering av tillämpningen av direktivet och dess inverkan på de ekonomiska aktörerna och konsumenterna. Utvärderingen ska beakta den fortsatta utvecklingen av tekniken för elektronisk kommunikation och den statistik som översänts till kommissionen i enlighet med artikel 10. Utvärderingens syfte är att avgöra om det är nödvändigt att ändra direktivets bestämmelser, särskilt vad avser de uppgifter som ska lagras och lagringstiderna.

Redan i dag förs statistik rörande hemlig teleövervakning som redovisas till regeringen inför den parlamentariska kontroll över tillämpningen av bestämmelserna som utövas av riksdagen. Det är Åklagarmyndigheten och Rikspolisstyrelsen som sammanställer statistiken och överlämnar den till regeringen tillsammans med uppgifter om den brottslighet som legat till grund för besluten om hemliga tvångsmedel. Regeringens skrivelse till riksdagen innehåller uppgifter om det totala antalet beslut om tillstånd till hemlig teleavlyssning och hemlig teleövervakning, vilka brott som besluten avsett, den genomsnittliga tiden som besluten gällt, antalet fall där tvångsmedlet haft betydelse för förundersökningen, antalet fall då förundersökningen lagts ned på grund av att brott inte kunde styrkas, antalet fall då verkställighet inte kunnat ske i önskad omfattning, t.ex. på grund av tekniska problem, antalet fall då ansökan om tvångsmedlet avslagits och om antalet fall där tillstånd till tvångsmedlet meddelats efter begäran om rättslig hjälp från annat land. De fall av hemlig teleövervakning som avser Säkerhetspolisens ärenden redovisas i särskild ordning och inte i den skrivelse som lämnas till riksdagen.

När de brottsbekämpande myndigheterna begär och får trafikuppgifter med stöd av lagen om elektronisk kommunikation är det i formell mening inte frågan om användning av hemligt tvångsmedel. Det förs ingen statistik över de fall där utlämnande sker enligt den lagen.

Vid sidan av direktivet om lagring av trafikuppgifter finns det även från ett nationellt perspektiv skäl att föra statistik över de brottsbekämpande myndigheternas tillgång till trafikuppgifter. Med en mer utförlig statistik än den som finns i dag skulle det finnas ett bättre underlag för bedömningen av behovet av trafikuppgifter i brottsbekämpningen och ett underlag för bedömningen av systemets effektivitet. Statistiken skulle också bilda ett gott under-

lag för de brottsbekämpande myndigheternas egen tillsynsverksamhet. Också andra kontrollorgans möjligheter att utföra sina uppgifter förbättras med ett gott statistikunderlag. Den kanske viktigaste aspekten är dock att statistiken skulle kunna bidra till en ökad parlamentarisk kontroll av användningen av trafikuppgifter i brottsbekämpningen.

15.3 Uppgifter som ska omfattas av statistiken

Förslag: Statistik ska föras över
– antalet verkställda beslut om hemlig teleövervakning respektive utlämnanden enligt lagen om elektronisk kommunikation,
– vilka typer av brott som ärendena har avsett,
– hur lång tid som har förlöpt från det att respektive trafikuppgift lagrades till dess att den brottsbekämpande myndigheten begärde tillgång till uppgiften och
– antalet ärenden där myndigheternas begäran om att få tillgång till trafikuppgifter inte har kunnat tillgodoses av leverantörerna samt vilka typer av brott ärendena har avsett.

För de ärenden som handläggs av Säkerhetspolisen och som rör rikets säkerhet ska det inte föras någon statistik.

Av artikel 10 i direktivet om lagring av trafikuppgifter framgår vilka uppgifter som ska redovisas till kommissionen. I artikeln anges också att statistiken inte ska omfatta personuppgifter.

Direktivet uttrycker bl.a. att det ska föras statistik över *de fall* där information skickats till behöriga myndigheter samt *de fall* där en begäran om uppgifter inte har kunnat tillgodoses. I den engelska versionen av direktivet används uttrycket ”the cases”. Mot bakgrund av ändamålet med statistiken tolkar vi direktivet så att det inte enbart kan vara fråga om *antalet verkställda beslut* om hemlig teleövervakning respektive *antalet verkställda utlämnanden* enligt lagen om elektronisk kommunikation utan även uppgift om *vilka typer av brott* som ärendena har avsett. Statistiken ska också omfatta antalet ärenden där myndigheternas begäran om att få trafikuppgifter inte har kunnat tillgodoses av leverantörerna samt vilka typer av brott ärendena har avsett.

Det är enligt vår mening inte rimligt att tolka direktivet så att det också ska föras statistik över exakt vilka typer av trafikuppgifter som lämnas ut. Det sistnämnda skulle bl.a. medföra en enorm administrativ hantering och öka integritetsintrånget.

Vi har i avsnitt 6.7.4, 6.10.3 och 6.11.3 föreslagit att uppgift om datum och spårbar tid ska lagras vid såväl telefoni och meddelandehantering som Internetåtkomst. Främst genom de trafikuppgifterna blir det möjligt att uppfylla direktivets krav på att det ska föras statistik över hur lång tid som har förlöpt från det att respektive uppgift lagrades till dess att den brottsbekämpande myndigheten begärde tillgång till uppgiften.

En särskild fråga rör hur statistik över de ärenden som Säkerhetspolisen handlägger ska hanteras.

Säkerhetspolisens uppgift är att förebygga och avslöja brott mot rikets säkerhet (främst 18 och 19 kap. brottsbalken) och svara för terrorismbekämpning. Uppgifter om användningen av hemlig teleövervakning inom Säkerhetspolisen, även vid misstänkta terroristbrott, redovisas i ett sammanhang årligen till regeringen. De uppgifterna är belagda med sekretess enligt 2 kap. 2 § och 5 kap. 1 § sekretesslagen och anses vara av synnerlig betydelse för rikets säkerhet (se 7 § sekretessförordningen [1980:657]).

Som nyss nämndes ska den statistik som avses i direktivet om lagring av trafikuppgifter bl.a. omfatta uppgifter om antalet verkställda beslut om hemlig teleövervakning och vilka typer av brott ärendena har avsett samt om antalet ärenden där myndigheternas begäran om att få trafikuppgifter inte har kunnat tillgodoses av leverantörerna samt vilka typer av brott de har avsett.

Skulle ett sådant redovisningskrav finnas för de ärenden som rör brott mot rikets säkerhet, kommer uppgifter av synnerlig betydelse för rikets säkerhet att avslöjas. Detta får naturligtvis inte ske. Direktivet om lagring av trafikuppgifter kan inte på det sättet ta över nationella säkerhetsintressen. Vi har förstått att det inte är möjligt att ”avidentifiera” uppgifterna utan att det samtidigt blir möjligt att sluta sig till det faktiska förhållandet. Mot den bakgrunden ska det inte finnas något krav på att statistik vid misstänkta brott mot rikets säkerhet ska redovisas. Det bör framhållas att terroristbrott inte räknas som ett brott mot rikets säkerhet. För sådana brott ska alltså statistikkravet gälla.

15.4 Ansvaret för statistiken

Förslag: De brottsbekämpande myndigheterna ska ansvara för statistiken. Uppgifterna ska sammanställas av Rikspolisstyrelsen och därefter överlämnas till regeringen.

En fördel med att ge de brottsbekämpande myndigheterna ansvaret för att föra statistiken är att myndigheterna redan i dag har en sådan uppgift när det gäller tillämpningen av bestämmelserna om hemlig teleövervakning. Flera av de uppgifter som ska omfattas av statistiken i anledning av direktivet om lagring av trafikuppgifter samlas in redan i dag. Det rör antalet beslut om hemliga tvångsmedel och vilka brott besluten har avsett. Ett genomförande av direktivet kommer dock att ställa delvis nya krav på vilka uppgifter som ska samlas in, särskilt som det i dag inte förs någon statistik över utlämnanden enligt lagen om elektronisk kommunikation.

En alternativ ordning vad gäller ansvaret vore att leverantörerna får föra statistiken. Av flera skäl är det inte en lämplig lösning. Bl.a. skulle det vara en helt ny arbetsuppgift för leverantörerna. Uppgiften skulle kräva särskilda anpassningar i de tekniska systemen och ansvaret skulle bli spritt på ett stort antal aktörer, som dessutom skulle växla över tid. Till det kommer att statistikuppgifter hos leverantörerna skulle kunna avslöja sekretessbelagda uppgifter, t.ex. Säkerhetspolisens egen användning av hemlig teleövervakning.

Ett annat alternativ skulle vara att tillsynsmyndigheten för statistiken. Det framstår dock som en onödig omgång att ge den arbetsuppgiften till PTS.

Det mest lämpliga är att de brottsbekämpande myndigheterna, dvs. de myndigheter som får tillstånd enligt rättegångsbalken eller begär ut uppgifter enligt lagen om elektronisk kommunikation, för den statistik som direktivet om lagring av trafikuppgifter kräver. Uppgifterna bör sammanställas av Rikspolisstyrelsen och rapporteras till regeringen som ett underlag för regeringens redovisning till kommissionen.

16 Konsekvenser och genomförande

16.1 Sammanfattning av våra förslag och bedömningar

- Förslagen ger inte anledning till några resursförstärkningar för rättsväsendet.
- Förslagen innebär att Post- och telestyrelsen får nya uppgifter inom ramen för sin tillsynsverksamhet och att den verksamheten behöver tillföras resurser motsvarande 2,75 miljoner kronor om året under åren 2008–2010 och därefter en miljon kronor årligen. Det blir en fråga för Post- och telestyrelsen att bedöma om den kostnaden kan bäras inom ramen för de avgifter som myndigheten tar ut i dag.
- Förslagen i betänkandet ska träda i kraft den 1 januari 2009. Några övergångsbestämmelser ska inte finnas.

16.2 Konsekvenser

Bedömning: Förslagen ger inte anledning till några resursförstärkningar för rättsväsendet.

Förslagen innebär att Post- och telestyrelsen får nya uppgifter inom ramen för sin tillsynsverksamhet och att den verksamheten behöver tillföras resurser motsvarande 2,75 miljoner kronor om året under åren 2008–2010 och därefter en miljon kronor årligen. Det blir en fråga för Post- och telestyrelsen att bedöma om den kostnaden kan bäras inom ramen för de avgifter som myndigheten tar ut i dag.

Om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, landsting, företag eller andra enskilda, ska enligt 14 kommittéförordningen (1998:1474) en beräkning av

dessa konsekvenser redovisas i betänkandet. Om förslagen innebär samhällsekonomiska konsekvenser i övrigt, ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för staten, kommuner eller landsting, ska en finansiering föreslås.

Våra förslag innebär att kostnaderna för att fullgöra lagringsskyldigheten ska fördelas mellan det allmänna och leverantörerna. Fördelningen innebär att leverantörerna ska stå för kostnaderna som är förenade med lagringsskyldigheten medan det allmänna ska betala en ersättning till leverantörerna när uppgifter lämnas ut i enskilda ärenden. Ersättningens storlek ska fastställas av PTS efter samråd med Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen och Tullverket samt med leverantörerna.

I avsnitt 13 och 14 har vi redogjort för våra överväganden beträffande de kostnader som leverantörerna ska stå för och lagringsskyldighetens inverkan på konkurrensen. Det som nu ska övervägas är vilka kostnader våra förslag medför för de brottsbekämpande myndigheterna och andra myndigheter som berörs av våra förslag och förslagens konsekvenser i övrigt.

Våra förslag innebär inte någon förändring av de bestämmelser som reglerar förutsättningarna för att de brottsbekämpande myndigheterna ska få tillgång till trafikuppgifter, dvs. reglerna om hemlig teleövervakning enligt rättegångsbalken och utlämnande av uppgifter enligt lagen om elektronisk kommunikation. I dag fattar domstol beslut om hemlig teleövervakning i omkring 1 000 fall om året och polisen begär ut uppgifter med stöd av lagen om elektronisk kommunikation i omkring 8 000 fall. Tillgång till trafikuppgifter är av avgörande betydelse i utredningar om allvarlig brottslighet. Eftersom våra förslag innebär att trafikuppgifterna kommer att vara tillgängliga vid begäran, skulle det kunna förväntas att de leder till en mycket stor ökning av fall där de brottsbekämpande myndigheterna begär ut uppgifter och får betala för det. Hur många fall det blir torde dock huvudsakligen inte bero på att trafikuppgifterna blir tillgängliga utan snarare på en rad andra faktorer som har med resursanvändningen totalt sett hos de brottsbekämpande myndigheterna att göra. Vår bedömning är att de brottsbekämpande myndigheterna kommer att begära ut trafikuppgifter i något ökad utsträckning i förhållande till vad som gäller i dag. Det innebär att domstolarna, Åklagarmyndigheten och Ekobrottsmyndigheten kommer att få marginellt ökade kostnader för att handlägga ärendena. Polisen handlägger ärenden både enligt rättegångsbalken och lagen om elektronisk kommunikation och kommer att få de förhållandevis största kostnadsökningarna. Det rör sig framför allt om

ersättningar för utlämnande av trafikuppgifter och kostnader för införskaffande av viss utrustning samt informations- och utbildningsinsatser. Även Tullverket kommer att få kostnader för motsvarande åtgärder.

I bedömningen av rättsväsendets kostnader måste också vägas in att våra förslag innebär möjligheter till ganska stora effektivitetsvinster för rättsväsendet och att allvarliga brott kan utredas och lagföras snabbare. Det kan i och för sig leda till att kostnaderna ökar inom vissa sektorer av rättsväsendet. Om t.ex. polisen blir effektivare kan det leda till en ökad arbetsbörda med krav på ökade resurser för åklagare och domstolar. Men totalt sett torde rättsväsendets olika insatser vid utredning och lagföring av allvarlig brottslighet effektiviseras.

Vi bedömer att våra förslag om lagringsskyldigheten i sig inte kommer att medföra så många tillkommande ärenden årligen att det på grund av detta finns behov av några resursförstärkningar för rättsväsendet. Vi har bedömt kostnaden för ersättning till leverantörerna vid utlämnande till 20 miljoner kronor. Det överensstämmer väl med de uppgifter vi har fått om nivån på ersättning som betalas till leverantörerna i dag. Vi utgår från att den nivån kommer att tillämpas även i fortsättningen. Enligt vår bedömning blir rättsväsendets kostnader för systemet inte högre än de effektivitetsvinster som blir möjliga genom våra förslag. Vi bedömer därmed att våra förslag inte medför behov av att tillföra rättsväsendet ytterligare resurser.

På ett område ser vi att det finns behov av att tillföra resurser. PTS har tillsyn enligt lagen om elektronisk kommunikation. I det uppdrag PTS har ingår alltså redan i dag att ha tillsyn över hur leverantörerna sparar, utplånar och avidentifierar trafikuppgifter enligt 6 kap. LEK. PTS har dock hittills inte bedrivit en särskilt omfattande verksamhet på det området. PTS kommer enligt vår bedömning att behöva lägga ner resurser på att åstadkomma en effektiv tillsyn över leverantörernas lagring av trafikuppgifter och för att lägga fast en ordning för ersättningar vid utlämnande av trafikuppgifter. PTS behöver bl.a. utfärda säkerhetsföreskrifter och föreskrifter om ersättning, medge undantag från lagringsskyldigheten i enskilda fall och i övrigt bygga upp tillsynsverksamheten så att den på ett effektivt sätt kan bidra till att de brottsbekämpande myndigheterna får så stor nytta i sin verksamhet som möjligt av lagrade trafikuppgifter och så att skyddet för den personliga integriteten upprätthålls. En stor del av de åtgärder som PTS behöver vidta omfattas redan av myndighetens ansvar enligt lagen om elektronisk

kommunikation. Vad som tillkommer genom våra förslag är uppgifterna att meddela föreskrifter, medge undantag från lagringsskyldigheten och ha tillsyn över leverantörernas lagring av trafikuppgifter. PTS har bedömt att verksamheten behöver tillföras i genomsnitt omkring 2,75 miljoner kronor om året under åren 2008–2010 och därefter cirka en miljon kronor årligen. Kostnaden för PTS hela verksamhet finansieras i dag till cirka 90 procent av avgifter som tas ut av bl.a. leverantörer. Det blir en fråga för PTS att bedöma om de tillkommande kostnader som våra förslag medför kan bäras inom ramen för de avgifter som myndigheten tar ut i dag (se 8 kap. 17 § LEK).

Vi bedömer att det inte uppkommer något behov av resursförstärkning för Datainspektionen med anledning av våra förslag.

Förslagens betydelse för brottsbekämpningen har redovisats på flera ställen i betänkandet. Sammantaget innebär våra förslag ökade kostnader för leverantörerna och effektivitetsvinster för brottsbekämpningen. Vi bedömer att de långsiktiga samhällsekonomiska effekterna av våra förslag uppväger den belastning som förslagen åtminstone initialt innebär för leverantörerna.

16.3 Genomförande

Förslag: Förslagen i betänkandet ska träda i kraft den 1 januari 2009. Några övergångsbestämmelser ska inte finnas.

I direktivet om lagring av trafikuppgifter åläggs medlemsstaterna att genomföra bestämmelserna i nationell rätt senast den 15 september 2007. När det gäller Internetåtkomst, e-post och Internettelefoni finns dock en möjlighet att skjuta upp genomförandet av direktivet till och med den 15 mars 2009. Den möjligheten har Sverige utnyttjat.

Direktivet om lagring av trafikuppgifter beslutades i mars 2006. Under åren 2007 och 2008 kommer ett flertal länder i Europa att ha genomfört hela eller delar av direktivet i nationell rätt. Det är rimligt att de leverantörer som blir lagringsskyldiga enligt vårt förslag får viss tid på sig för att anpassa verksamheten. Samtidigt har leverantörerna redan nu möjlighet att dra nytta av de erfarenheter som finns hos leverantörer i andra länder och av den teknik för lagring som har utvecklats. Vi anser därför att förslagen i betänkandet bör kunna träda i kraft den 1 januari 2009. Några övergångsbestämmelser till de föreslagna författningsändringarna behövs inte.

17 Författningskommentar

17.1 Förslaget till lag om ändring i sekretesslagen (1980:100)

5 kap. 1 §

Sekretess gäller för uppgift som hänför sig till

1. förundersökning i brottmål,

2. angelägenhet, som avser användning av tvångsmedel i sådant mål eller i annan verksamhet för att förebygga brott,

3. verksamhet som rör utredning i frågor om näringsförbud eller förbud att lämna juridiskt eller ekonomiskt biträde,

4. åklagarmyndighets, polismyndighets, Skatteverkets, Tullverkets eller Kustbevakningens verksamhet i övrigt för att förebygga, uppdaga, utreda eller beivra brott,

5. Finansinspektionens verksamhet som rör övervakning enligt lagen (2005:377) om straff för marknadsmissbruk vid handel med finansiella instrument, eller

6. Post- och telestyrelsens verksamhet för prövning av frågor om undantag enligt 6 kap. 6 c § andra stycket lagen (2003:389) om elektronisk kommunikation,

om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs.

För uppgift som --- Tullverkets brottsbekämpande verksamhet.

Sekretess enligt första --- misstanke om brott.

Utan hinder av --- motsvarande äldre bestämmelser.

Sekretess gäller inte --- högst fyrtio år.

Sekretess med hänsyn främst till intresset att förebygga och beivra brott regleras i 5 kap. sekretesslagen. I 5 kap. 1 § den lagen finns regler till skydd för det allmännas brottsförebyggande och brottsbeivrande verksamhet. Uppgifter som hänför sig till den verksam-

heten kan också skyddas genom bestämmelserna i 2 kap. sekretesslagen om sekretess med hänsyn till bl.a. rikets säkerhet.

I den nu aktuella paragrafens *första stycke* har en sjätte punkt lagts till. Frågan behandlas i avsnitt 7.2.3. Sekretess ska gälla för uppgift som hänför sig till PTS verksamhet för prövning av frågor om undantag från lagringsskyldigheten enligt den föreslagna 6 kap. 6 c § andra stycket LEK, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs. Enligt den angivna bestämmelsen i lagen om elektronisk kommunikation får regeringen eller den myndighet som regeringen bestämmer meddela undantag i enskilda fall. I förslaget till förordning om lagring av trafikuppgifter m.m. för brottsbekämpande syften (se avsnitt 17.3) bestäms att PTS får meddela undantagen efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen. Om sådana begränsningar i lagringsskyldigheten blir offentliga skulle det kunna resultera i att PTS verksamhet för att på ett riktigt sätt avgränsa kretsen lagringsskyldiga leverantörer och brottsbekämpningen motverkas eller den framtida verksamheten skadas. Bestämmelsen i 5 kap. 1 § sekretesslagen är utformad så att sekretessen gäller oavsett hos vilken myndighet uppgiften finns. Sekretess kommer också att gälla om uppgiften finns hos förvaltningsdomstol efter exempelvis ett överklagande av PTS beslut. Enligt 12 kap. 4 § sekretesslagen kan domstolen förordna att sekretessen ska bestå även om uppgifterna har tagits in i domstolens beslut.

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

6 kap. 3 §

Den som tillhandahåller en allmänt tillgänglig elektronisk kommunikationstjänst ska vidta lämpliga åtgärder för att säkerställa att behandlade uppgifter skyddas. Den som tillhandahåller ett allmänt kommunikationsnät ska vidta de åtgärder som är nödvändiga för att upprätthålla detta skydd i nätet. Åtgärderna ska vara ägnade att säkerställa en säkerhetsnivå som, med beaktande av tillgänglig teknik och kostnaderna för att genomföra åtgärderna, är anpassad till risken för integritetsintrång.

Lagringsskyldiga enligt 6 a § ska dessutom vidta särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter.

Paragrafen reglerar skyldigheten för leverantörer att vidta åtgärder för att säkerställa att behandlade uppgifter skyddas mot integritetsintrång.

Andra stycket i bestämmelsen är nytt och uttrycker de särskilda krav som gäller för skyddet av trafikuppgifter som lagras för brottsbekämpande syften. De lagringsskyldiga leverantörerna har skyldighet att vidta särskilda tekniska och organisatoriska åtgärder för ett tillräckligt skydd vid behandlingen av lagrade trafikuppgifter. Det innebär att leverantörerna ska säkerställa att uppgifterna i lagret har en hög kvalitet och ett tillräckligt skydd mot integritetsintrång. Leverantörerna måste med andra ord enligt 6 kap. 6 a § LEK lagra rätt uppgifter och enligt den nu aktuella bestämmelsen skydda uppgifterna mot sådana integritetsintrång som kan uppkomma genom exempelvis uppsåtlig eller oaktsam otillåten användning, spridning, förstöring eller förvanskning av uppgifterna. Frågan behandlas i avsnitt 8.

Till skillnad mot bestämmelsen i första stycket innehåller andra stycket ingen möjlighet att bestämma säkerhetsnivån genom en avvägning mellan teknik, kostnader och risken för integritetsintrång. Tekniska och organisatoriska åtgärder måste vidtas av leverantörerna som säkerställer en tillräckligt hög nivå på skyddet. Skillnaden i den säkerhetsnivå som leverantörerna ska ha jämfört med deras skyldigheter enligt första stycket uttrycks genom uttrycket ”särskilda” åtgärder som säkerställer ett ”tillräckligt skydd”, i stället för uttrycket ”lämpliga åtgärder”, som används i första stycket.

Enligt den föreslagna 6 kap. 6 c § LEK meddelar regeringen eller den myndighet som regeringen bestämmer föreskrifter om säkerheten (se vidare avsnitt 17.3 rörande förordningen om lagring av trafikuppgifter m.m. för brottsbekämpande syften). Föreskrifter kan ges om att trafikuppgifterna ska vara enkelt sökbara och logiskt skilda från övrig verksamhet och om att leverantörerna ska säkerställa att endast särskilt behörig personal har tillgång till trafikuppgifterna.

Behandling av trafikuppgifter m.m.

6 kap. 5 §

Trafikuppgifter som avser användare som är fysiska personer eller avser abonnenter och som lagras eller behandlas på annat sätt av den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 §, ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande, om de inte sparas för sådan behandling som anges i 6, 6 a eller 13 §.

I bestämmelsen finns huvudregeln om behandling av trafikuppgifter. Den innebär att när en sådan uppgift inte längre behövs för att överföra ett elektroniskt meddelande måste den utplånas eller avidentifieras. Som framgår får uppgifterna sparas för viss behandling (se 6 kap. 6 och 13 §§ LEK), t.ex. abonnentfakturering. Paragrafen har kompletterats med en hänvisning till den föreslagna 6 kap. 6 a § LEK om lagringsskyldighet för brottsbekämpande syften som också innebär ett undantag från huvudregeln. Enligt den föreslagna 6 kap. 6 b § LEK ska trafikuppgifter som lagras för brottsbekämpande syften utplånas vid utgången av lagringstiden. I detta fall räcker det således inte med att uppgiften avidentifieras.

Begreppet trafikuppgifter definieras i 6 kap. 1 § LEK som uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande. Den definitionen är för snäv för att träffa samtliga de uppgifter som lagringsskyldigheten enligt den föreslagna 6 kap. 6 a § LEK omfattar, t.ex. uppgifter om tjänster, om Internetanslutning, om slutpunkter och om typ av kapacitet för överföring. Rubriken närmast före den nu aktuella bestämmelsen har därför ändrats så att ”m.m.” lagts till efter ”trafikuppgifter”.

6 kap. 6 a §

Den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § och som genererar eller behandlar uppgifter som avses i 20 § första stycket 1 och 3 ska lagra uppgifterna för brottsbekämpande syften.

Lagrade uppgifter får behandlas endast

1. för att lämnas ut enligt 22 § första stycket 2 och 3 eller 27 kap. 19 § rättegångsbalken, eller

2. enligt 30 § första stycket personuppgiftslagen (1998:204).

Paragrafen är ny.

I *första stycket* regleras vilka leverantörer som ska vara skyldiga att lagra uppgifter. Frågan behandlas i avsnitt 7.2. Lagringsskyldigheten ansluter till anmälningsplikten enligt bestämmelsen i 2 kap. 1 § LEK. Det innebär således att den som bedriver en anmälningspliktig verksamhet enligt 2 kap. 1 § LEK är skyldig att lagra sådana uppgifter som anges i 6 kap. 20 § första stycket 1 och 3 LEK för brottsbekämpande syften. Lagringsskyldigheten gäller leverantörer av allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning och av allmänt tillgängliga elektroniska kommunikationstjänster. En tolkningsfråga blir om den som levererar en e-posttjänst eller Internettelefonitjänst utan att samtidigt leverera nät och som i och för sig torde vara lagringsskyldig, faktiskt omfattas av anmälningsplikten i 2 kap. 1 § LEK. PTS har, utan att ta ställning i frågan i något enskilt ärende, redovisat den uppfattningen att tjänsteleverantören, för att vara anmälningspliktig, på ett fysiskt eller rättsligt sätt (genom innehav eller avtal) måste råda över någon del av överföringen. Om överföringen av signaler sker över ett kommunikationsnät och/eller via en kommunikationstjänst som är helt fristående från tjänsteleverantören, är denne enligt PTS inte anmälningspliktig om det samtidigt är så att leverantören inte har rättslig möjlighet att påverka några förhållanden i överföringen, som till exempel överföringskapacitet eller kvalitet. Som en följd av den uppfattning PTS har redovisat torde det stora flertalet av de leverantörer som tillhandahåller e-posttjänster och Internettelefonitjänster utan att samtidigt leverera nät vara anmälningspliktiga och därmed skyldiga att lagra trafikuppgifter.

I första stycket anges också vilka uppgifter som ska lagras. Sådana uppgifter som anges i 6 kap. 20 § 1 och 3 ska lagras. Dessa bestämmelser reglerar fler typer av uppgifter än dem som ska lagras för brottsbekämpande syften. Vilka uppgifter som specifikt ska lagras enligt första stycket framgår av den föreslagna bestämmelsen i 6 kap. 6 c § LEK som hänvisar till den föreslagna förordningen om lagring av trafikuppgifter m.m. för brottsbekämpande syften (se avsnitt 17.3).

Av första stycket framgår vidare att en förutsättning för lagringsskyldigheten är att den enskilde leverantören genererar eller behandlar uppgiften. Leverantören har alltså inte någon skyldighet att ”skaffa sig” alla de uppgifter lagringsskyldigheten omfattar. Med uttrycket behandla avses samma slags åtgärder som framgår av

3 § PUL, nämligen varje åtgärd eller serie av åtgärder som vidtas i fråga om uppgifterna, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring. Det innebär i princip att om uppgifterna någon gång finns hos leverantören, även om det bara rör sig om en ytterst kort tid, ska de lagras.

I *andra stycket* regleras för vilka ändamål uppgifter som har lagrats enligt första stycket får behandlas. Uppgifterna får behandlas endast i tre situationer, för att lämnas ut enligt 6 kap. 22 § första stycket 2 och 3 LEK, för att lämnas ut enligt ett beslut om hemlig teleövervakning enligt 27 kap. 19 § RB, och om annan anlitats för att lagra uppgifterna. Alla annan behandling av uppgifterna är förbjuden innan uppgifterna ska utplånas enligt den föreslagna 6 kap. 6 b §.

Behandling för utlämnande enligt rättegångsbalken och lagen om elektronisk kommunikation behöver inte kommenteras särskilt. Behandling av personuppgifter när annan anlitas för lagringen regleras i 30 § första stycket PUL. Den som anlitas blir personuppgiftsbiträde enligt personuppgiftslagen och det kan vara en annan leverantör eller en tredje man. I 30 § andra stycket PUL finns bestämmelser som gäller kvaliteten och säkerheten i ett personuppgiftsbiträdes behandling av uppgifterna. Det innebär att säkerheten för uppgifterna när de behandlas av den som har anlitats för lagringen ska ske enligt leverantörens instruktioner. De krav som ställs på leverantören avseende säkerheten regleras i 6 kap 3 § andra stycket LEK. Den lagringsskyldige har alltså alltid kvar alla de skyldigheter mot myndigheter och enskilda som följer med lagringsskyldigheten, t.ex. att uppgifterna lagras enligt första stycket och att särskilda tekniska och organisatoriska åtgärder vidtas enligt 6 kap. 3 § andra stycket för att säkerställa ett tillräckligt skydd vid behandlingen. De brottsbekämpande myndigheterna ska alltid kunna vända sig till den lagringsskyldige med begäran om utlämnande av uppgifterna. Ett utlämnande får inte fördröjas på grund av ett avtal med annan om lagringen (se nedan kommentaren till 6 kap. 19 a § LEK).

6 kap. 6 b §

Lagring enligt 6 a § ska pågå under ett år från det datum kommunikationen ägde rum. Vid lagringstidens slut ska uppgifterna utplånas, om de inte har begärts utlämnade men ännu inte lämnats ut eller den lagringsskyldige annars har rätt att fortsätta behandla dem.

Paragrafen är ny och reglerar lagringstidens längd och åtgärder från leverantörens sida vid den tidens slut. Frågan behandlas i avsnitt 7.3.

Lagringstidens längd är enligt bestämmelsens *första mening* ett år från det datum kommunikationen ägde rum. Vid telefoni och meddelandehantering blir kommunikationens slut utgångspunkten för lagringstidens beräkning. Utgångspunkten vid Internetåtkomst blir i stället avloggningen och vid verksamhet som tillhandahåller kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst, när abonnemanget eller avtalet upphör.

Av bestämmelsens *andra mening* framgår att uppgifterna ska utplånas vid lagringstidens slut. Utplåningen ska ske omedelbart därefter. Skulle de brottsbekämpande myndigheterna ha begärt ut uppgifterna från leverantören under den ettåriga lagringstiden men ännu inte fått dem när ett år har gått, ska leverantören dock inte utplåna uppgifterna förrän utlämnande har skett.

Efter den ettåriga lagringstiden kan leverantören ha rätt att fortsätta behandla uppgifterna enligt andra bestämmelser, t.ex. enligt 6 kap. 6 § LEK om uppgifterna krävs för abonnentfakturering. Enligt 6 kap. 5 § LEK har en leverantör normalt möjlighet att välja mellan att utplåna eller att avidentifiera uppgifterna. Direktivet om lagring av trafikuppgifter anger att uppgifterna ska förstöras vid lagringstidens slut. Att uppgifterna enligt den föreslagna bestämmelsen ska utplånas innebär en förstärkning av integritetsskyddet jämfört med alternativet att avidentifiera uppgifterna enligt 6 kap. 5 § LEK. Skulle leverantören ha rätt att fortsätta behandla uppgifterna efter den ettåriga lagringstiden, ska de logiskt inte längre behandlas som uppgifter som har lagrats enligt den föreslagna bestämmelsen i 6 kap. 6 a § LEK. Om uppgifterna sparas enligt andra bestämmelser ska de utplånas eller avidentifieras enligt bestämmelsen i 6 kap. 5 § LEK.

6 kap. 6 c §

Regeringen meddelar föreskrifter om lagringsskyldighet enligt 6 a §.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om säkerhet enligt 3 § andra stycket och får i enskilda fall medge undantag från lagringsskyldigheten enligt 6 a §.

Paragrafen är ny och innebär dels att regeringen genom föreskrifter preciserar den lagringsskyldighet som föreskrivs i den föreslagna 6 kap. 6 a § LEK, dels att regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om säkerhet enligt 6 kap. 3 § andra stycket LEK. Regeringen eller den myndighet som regeringen bestämmer får enligt paragrafen också medge undantag från lagringsskyldigheten i enskilda fall. Förslaget till förordning om lagring av trafikuppgifter m.m. för brottsbekämpande syften kommenteras i avsnitt 17.3.

6 kap. 6 d §

Lagringsskyldiga enligt 6 a § har rätt till ersättning när lagrade trafikuppgifter lämnas ut enligt 22 § första stycket 2 och 3 eller 27 kap. 19 § rättegångsbalken. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om ersättningen.

Paragrafen är ny och behandlar frågan om ersättning till lagringsskyldiga för utlämnande av de lagrade uppgifterna vid hemlig teleövervakning och enligt lagen om elektronisk kommunikation. Det är med andra ord fråga om ersättning för utlämnande av de uppgifter som lagras med stöd av den föreslagna 6 kap. 6 a § LEK. Frågan behandlas i avsnitt 13.8.4.

Enligt *första stycket* har leverantören rätt till ersättning när lagrade trafikuppgifter lämnas ut. Det är den myndighet som har begärt uppgifterna, dvs. den brottsbekämpande myndigheten, som ska betala ersättningen. Det är inte meningen att ersättning ska utgå för varje utlämnande utan bestämmelsen innebär att ersättning ska betalas för varje begäran, alltså först när alla uppgifter enligt en viss begäran har lämnats ut.

Enligt *andra stycket* meddelar regeringen eller den myndighet som regeringen bestämmer föreskrifter om ersättningen. Förslaget

till förordning om lagring av trafikuppgifter m.m. för brottsbekämpande syften kommenteras i avsnitt 17.3.

6 kap. 19 a §

Lagringsskyldiga enligt 6 a § ska bedriva verksamheten så att uppgifterna enkelt kan tas om hand och lämnas ut utan dröjsmål.

Paragrafen är ny och reglerar leverantörernas anpassning av systemen för lagringsskyldighetens fullgörande. Frågan behandlas i avsnitt 7.4.

Bestämmelsen preciserar den anpassningsskyldighet som gäller för leverantörer enligt 6 kap. 19 § LEK och anger att de leverantörer som är lagringsskyldiga enligt den föreslagna 6 kap. 6 a § LEK ska bedriva verksamheten så att uppgifterna enkelt kan tas om hand av de brottsbekämpande myndigheterna. Det innebär att myndigheterna utan ansträngning ska kunna ta del av uppgifterna även om de skulle vara krypterade eller komprimerade. Uppgifterna måste dock alltid överlämnas på ett sådant sätt att säkerheten och skyddet för uppgifterna inte eftersätts. I vilken form uppgifterna ska överlämnas för att enkelt kunna tas om hand får avgöras i samråd mellan leverantörerna och myndigheterna. Ytterst blir det en fråga för tillsynsmyndigheten PTS att avgöra hur uppgifterna kan överföras på ett säkert sätt och lämnas ut så att de enkelt kan tas om hand.

I bestämmelsen anges också vilka krav som ställs på leverantörernas tillgänglighet så att en begäran om utlämnande kan verkställas så fort som möjligt. I bestämmelsen anges att uppgifterna ska lämnas ut utan dröjsmål. Det innebär att överföring av uppgifterna behöver påbörjas så snart det kan ske även om utlämnande av samtliga de uppgifter en begäran omfattar inte kan verkställas omedelbart. Om det tar olika lång tid att få fram uppgifterna ur leverantörens system, bör överlämnandet ske successivt och så snart uppgifterna blir tillgängliga. Hur snabbt uppgifterna kan överlämnas får avgöras av resurssituationen hos respektive leverantör. Utgångspunkten är dock att arbetet med att överföra informationen ska påbörjas inom någon enstaka timme räknat från när leverantören tar emot (i betydelsen blir medveten om) begäran. Det kan också betyda att leverantören behöver arbeta med verkställigheten utanför kontorstid. Det blir en fråga för de brottsbekämpande myndigheterna och leverantörerna och ytterst tillsynsmyndigheten att närmare precisera kravet på medverkan inom viss tid.

17.3 Förslaget till förordning (0000:00) om lagring av trafikuppgifter m.m. för brottsbekämpande syften

1 §

I denna förordning ges föreskrifter om lagring av trafikuppgifter m.m. enligt 6 kap. 3 § andra stycket, 6 a, 6 c och 6 d §§ lagen (2003:389) om elektronisk kommunikation.

I förordningens inledande bestämmelse anges att förordningen reglerar föreskrifter om lagring av trafikuppgifter enligt 6 kap. 3 § andra stycket, 6 a, 6 c och 6 d §§ LEK. Förordningen reglerar således frågor om säkerhet för lagrade trafikuppgifter, vilka uppgifter som ska lagras, möjligheten för myndighet att besluta föreskrifter och undantag i enskilda fall samt frågor om ersättning för utlämnande av uppgifter.

2 §

I denna förordning avses med

1. Internettelefoni: telefoni som använder IP-paket via Internet för överföring,

2. Internetåtkomst: möjlighet till överföring av IP-paket som ger användaren åtkomst till Internet,

3. meddelandehantering: överföring av elektroniskt meddelande som inte är samtal,

4. misslyckad uppringning: samtal som kopplats fram utan att få svar eller samtal som kopplats fram utan att nå mottagaren,

5. mobil telefoni: elektronisk kommunikationstjänst till mobil nätanslutningspunkt som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan och som inte samtidigt avser meddelandehantering,

6. slutpunkt: ändpunkt för varje lagringsskyldigs behandling av kommunikation,

7. telefoni: elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan och som inte samtidigt avser meddelandehantering.

I paragrafen definieras en del av de begrepp som används i förordningen.

I punkten 1 definieras Internettelefoni som telefoni som använder IP-paket via Internet för överföring.

I punkten 2 definieras *Internetåtkomst* som möjlighet till överföring av IP-paket som ger användaren åtkomst till Internet. Frågan behandlas i avsnitt 6.6.5. Där beskrivs Internetåtkomst så att användaren tilldelas en eller flera IP-adresser för kommunikation. Dessa IP-adresser kan vara av typerna fasta eller dynamiska.

I punkten 3 definieras *meddelandehantering* som överföring av elektroniskt meddelande som inte är samtal. Frågan behandlas i avsnitt 6.6.4. Det rör sig i dessa fall om överföring av meddelanden vanligtvis med SMS, MMS och elektronisk post och alltså tjänster som främst använder protokoll som SMTP och SMPP.

I punkten 4 definieras *misslyckad uppringning* som ett samtal som kopplats fram utan att få svar eller ett samtal som kopplats fram utan att nå mottagaren. När ett samtal kopplats fram utan att nå mottagaren får den uppringande parten ingen kontakt eller ett meddelande om att abonnenten inte kan nås för tillfället. Frågan behandlas i avsnitt 6.13. Utanför definitionen faller samtal som över huvud taget inte kopplas.

I punkten 5 definieras *mobil telefoni* som elektronisk kommunikationstjänst till mobil nätanslutningspunkt som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan och som inte samtidigt avser meddelandehantering.

I punkten 6 definieras *slutpunkt* som ändpunkt för varje lagringsskyldigs behandling av en kommunikation. Med uttrycket avses den tekniska utrustningen i en fysisk ändpunkt som står under leverantörens kontroll och som är gränssnitt mot kund eller abonnent, såsom telefonväxlar, routers, portnummer, utrustningsidentitet, MAC-adresser och abonnemangsidentitet.

I punkten 7 definieras *telefoni* som elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan. Frågan behandlas i avsnitt 6.6.3. Definitionen ansluter till hur telefonitjänst definieras i 1 kap. 7 § LEK. Enligt definitionen i 1 kap. 7 § LEK måste det kunna gå att genomföra nödsamtal för att kommunikationstjänsten ska anses vara telefoni. Om lagringsskyldigheten enbart skulle träffa sådana telefonitjänster, skulle skyldigheten bli för snäv. Av den anledningen finns inte kravet på

möjlighet till nödsamtal i den definition som anges i punkten 7. Telefoni enligt förslaget ska omfatta fall där s.k. E.164-nummer används. I definitionen i punkten 7 finns det tillägget att det inte samtidigt ska vara fråga om meddelandehantering (se ovan punkten 3).

3 §

Den som är lagringsskyldig enligt 6 kap. 6 a § lagen (2003:389) om elektronisk kommunikation ska lagra de uppgifter som anges i 4-9 §§.

I bestämmelsen anges att den som är lagringsskyldig enligt den föreslagna 6 kap. 6 a § LEK, dvs. den som bedriver verksamhet som är anmälningspliktig enligt 2 kap. 1 § LEK, ska lagra de uppgifter som närmare anges i 4-9 §§. En generell begränsning av lagringsskyldigheten finns dock i 6 kap. 6 a § LEK som anger att skyldigheten endast gäller i fråga om uppgifter som den enskilde leverantören genererar eller behandlar. Lagringstidens längd och skyldigheten att utplåna lagrade uppgifter vid lagringstidens slut regleras i den föreslagna 6 kap. 6 b § LEK.

4 §

Vid telefoni ska uppgifter om följande lagras:
– uppringande telefonnummer,
– nummer som slagits och nummer till vilka samtalet styrts,
– uppgifter om abonnent och registrerad användare,
– datum och spårbar tid då kommunikationen påbörjades och avslutades,
– den tjänst som använts, samt
– slutpunkter.

I bestämmelsen anges vilka uppgifter som ska lagras vid telefoni. Begreppet telefoni definieras i 2 § och omfattar fast och mobil telefoni och de flesta Internettelefonitjänster. De uppgifter som anges i denna paragraf ska alltså lagras oavsett vilken typ av telefoni det är fråga om. I 5 och 6 §§ anges vissa uppgifter som ska lagras därutöver och som är specifika för mobil telefoni respektive Internettelefoni. Uppgifter om meddelandehantering ska inte lagras enligt denna bestämmelse. De uppgifter om meddelandehantering som ska lagras anges i 7 §.

Frågan om *uppringande telefonnummer* behandlas i avsnitt 6.7.1. Med telefonnummer avses inte enbart det som normalt betecknas som ett telefonnummer utan även andra användar-ID som används vid de olika sätt för kommunikation som faller under definitionen för telefoni, t.ex. Internettelefoni. Användar-ID definieras i artikel 2 i direktivet om lagring av trafikuppgifter som ett unikt ID som tilldelas personer när de abonnerar på eller registrerar sig på en Internetåtkomsttjänst eller en Internetkommunikationstjänst.

Frågan om *nummer som slagits och nummer till vilka samtalet styrts* behandlas i avsnitt 6.7.2. Det innefattar uppgift om uppringt telefonnummer men täcker också andra nummer som slagits utan att sifferkombinationen är så fullständig att det anses vara ett telefonnummer, t.ex. felslagna nummer eller nummer där den som slagit har glömt ett utlandsprefix.

Frågan om *uppgifter om abonnent och registrerad användare* behandlas i avsnitt 6.7.3. De uppgifter som avses är namn och adress samt person- eller organisationsnummer rörande den uppringande och den uppringde. Skyldigheten rör inte enbart uppgifter om abonnenter utan även om registrerade användare. Med det sistnämnda begreppet avses en fysisk eller juridisk person eller enhet som använder en allmänt tillgänglig elektronisk kommunikationstjänst för privat eller affärsmässigt bruk, utan att nödvändigtvis ha abonnerat på denna tjänst (artikel 2 i direktivet om lagring av trafikuppgifter). Finns en registrerad användare vid sidan av en abonnent ska alltså uppgifter rörande *båda* dessa lagras, under förutsättning att den uppgiften genereras eller behandlas av leverantören.

Frågan om *datum och spårbar tid då kommunikationen påbörjades och avslutades* behandlas i avsnitt 6.7.4. För att kvaliteten hos uppgifterna ska bli så hög och precis som möjligt ska tiden vara spårbar. Med spårbar tid avses tidsangivelse där förhållandet till UTC (SP) (Universal Time, Coordinated), alltså den offentligt tillgängliga tidstandarden, redovisas.

Frågan om uppgifter om *den tjänst som använts* behandlas i avsnitt 6.7.5. Det rör sig t.ex. om uppgifter om röstbrevlåda och uppgifter om funktioner för vidarekoppling och/eller omstyrning av samtal. Uppgifterna ska lagras oavsett om samtal skett eller inte.

Frågan om *slutpunkter* behandlas i avsnitt 6.7.6. Begreppet slutpunkt definieras i 2 § som ändpunkt för varje lagringsskyldigs behandling av kommunikation. Med det avses den tekniska utrustningen i en fysisk ändpunkt som står under leverantörens kontroll och som är gränssnitt mot kund eller abonnent, såsom telefonväx-

lar, routers, portnummer, utrustningsidentitet, MAC-adresser och abonnemangsidentitet.

5 §

Vid mobil telefoni ska utöver det som anges i 4 § uppgifter om följande lagras:
– uppringande parts abonnemangsidentitet och utrustningsidentitet,
– uppringd parts abonnemangsidentitet och utrustningsidentitet,
– lokaliseringsinformation för kommunikationens början och slut, samt
– datum, spårbar tid och lokaliseringsinformation för den första aktiveringen av en förbetald anonym tjänst.

I bestämmelsen anges vilka uppgifter utöver de som anges i 4 § som ska lagras vid mobil telefoni. Begreppet mobil telefoni definieras i 2 § som elektronisk kommunikationstjänst till mobil nätanslutningspunkt som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan och som inte samtidigt avser meddelandehantering.

Frågan om *den uppringande och den uppringda partens abonnemangsidentitet och utrustningsidentitet* behandlas i avsnitt 6.8.1. Med abonnemangsidentitet och utrustningsidentitet avses i dagsläget det som brukar benämnas IMSI- och IMEI-nummer. IMSI-numret (International Mobile Subscriber Identity) är kopplat till abonnentens telefonnummer (abonnemanget), medan IMEI-numret (International Mobile Equipment Identity) är identiteten på utrustningen (hårdvaran).

Frågan om *lokaliseringsinformation för kommunikationens början och slut* behandlas i avsnitt 6.8.2. Den information som ges är uppgift om det geografiska område i form av cell-ID som täcks av den basstation som hade kontakt med mobiltelefonen under kommunikationen.

Frågan om *datum, spårbar tid och lokaliseringsinformation för den första aktiveringen av en förbetald anonym tjänst* behandlas i avsnitt 6.8.3. Med spårbar tid avses tidsangivelse där förhållandet till UTC (SP) (Universal Time, Coordinated), alltså den offentligt tillgängliga tidstandarden, redovisas. Lokaliseringsinformationen ska ge uppgift om det geografiska område i form av cell-ID som täcks av den basstation som hade kontakt med mobiltelefonen vid den första aktiveringen av abonnemanget.

6 §

Vid Internettelefoni ska utöver det som anges i 4 § uppgifter om följande lagras:
– uppringande parts IP-adresser, samt
– uppringd parts IP-adresser.

I bestämmelsen anges vilka uppgifter utöver de som anges i 4 § som ska lagras vid Internettelefoni. Begreppet Internettelefoni definieras i 2 § som telefoni som använder IP-paket via Internet för överföring.

Frågan om *uppringande och uppringd parts IP-adresser* behandlas i avsnitt 6.9.1. Med IP-adresser avses den eller de IP-adresser som användes vid samtalet. För att IP-adressen ska ge information som behövs för brottsutredningar måste den kunna kopplas till en användare (givetvis under förutsättning att den uppgiften genereras eller behandlas av leverantören).

7 §

Vid meddelandehantering ska uppgifter om följande lagras:
– avsändarens och mottagarens meddelandeadress,
– uppgifter om abonnent och registrerad användare,
– datum och spårbar tid för på- och avloggning i meddelandetjänsten,
– datum och spårbar tid för avsändande och mottagande av meddelande, samt
– den tjänst som har använts och spårbar tid för användandet.

I bestämmelsen anges vilka uppgifter som ska lagras vid meddelandehantering. Begreppet meddelandehantering definieras i 2 § som överföring av elektroniskt meddelande som inte är samtal. Det rör främst SMS, MMS och elektronisk post.

Frågan om *avsändarens och mottagarens meddelandeadress* behandlas i avsnitt 6.10.1. Med sådana adresser avses e-postadresser, telefonnummer eller annan användar-ID. Användar-ID är enligt artikel 2 i direktivet om lagring av trafikuppgifter ett unikt ID som tilldelats den som abonnerar på eller registrerar sig på bl.a. en Internetkommunikationstjänst.

Frågan om *uppgifter om abonnent och registrerad användare* behandlas i avsnitt 6.10.2. Det rör sig om samma typer av uppgifter som ska lagras vid telefoni enligt 4 §, alltså namn och adress samt

person- eller organisationsnummer rörande avsändaren och mottagaren. Skulle det vid sidan av en abonnent finnas en registrerad användare ska uppgifter lagras även rörande denne (se kommentaren till 4 §).

Frågan om *datum och spårbar tid för på- och avloggning i meddelandetjänsten* samt *datum och spårbar tid för avsändande och mottagande av meddelandet* behandlas i avsnitt 6.10.3. Med spårbar tid avses tidsangivelse där förhållandet till UTC (SP) (Universal Time, Coordinated), alltså den offentligt tillgängliga tidstandarden, redovisas.

Frågan om uppgifter om *den tjänst som har använts och spårbar tid för användandet* behandlas i avsnitt 6.10.4. Med tjänst avses exempelvis vidaresändning och/eller omstyrning. Uppgifterna ska lagras oavsett om utbyte av meddelande har skett eller inte. Med spårbar tid avses tidsangivelse där förhållandet till UTC (SP) (Universal Time, Coordinated), alltså den offentligt tillgängliga tidstandarden, redovisas.

8 §

Vid Internetåtkomst ska uppgifter om följande lagras:
– användarens IP-adresser,
– uppgifter om abonnent och registrerad användare,
– datum och spårbar tid för på- och avloggning i Internettjänsten,
– typen av Internetanslutning som använts, samt
– slutpunkter.

I bestämmelsen anges vilka uppgifter som ska lagras vid Internetåtkomst. Begreppet Internetåtkomst definieras i 2 § som möjlighet till överföring av IP-paket som ger användaren åtkomst till Internet.

Frågan om *användarens IP-adresser* behandlas i avsnitt 6.11.1. Skulle IP-adressen ändras under pågående kommunikation, ska även uppgift om ny IP-adress lagras.

Frågan om *uppgifter om abonnent och registrerad användare* behandlas i avsnitt 6.11.2. Det rör sig om samma typer av uppgifter som ska lagras vid telefoni och meddelandehantering enligt 4 och 7 §§, alltså namn och adress samt person- eller organisationsnummer. Skulle det vid sidan av en abonnent finnas en registrerad användare ska uppgifter lagras även rörande denne (se kommentaren

till 4 §). Uppgifterna måste under hela lagringstiden kunna kopplas till användarens IP-adresser.

Frågan om *datum och spårbar tid för på- och avloggning i Internettjänsten* behandlas i avsnitt 6.11.3. Med spårbar tid avses tidsangivelse där förhållandet till UTC (SP) (Universal Time, Coordinated), alltså den offentligt tillgängliga tidstandarden, redovisas.

Frågan om *typen av Internetanslutning som använts* behandlas i avsnitt 6.11.4. Med typ av Internetanslutning avses anslutning via DSL, modem för 3G, GPRS, fast telefoni etc.

Frågan om *slutpunkter* behandlas i avsnitt 6.11.5. Begreppet slutpunkt definieras i 2 § som ändpunkt för varje lagringsskyldigs behandling av kommunikation. Med det avses den tekniska utrustningen i en fysisk ändpunkt som står under leverantörens kontroll och som är gränssnitt mot kund eller abonnent, såsom telefonväxlar, routers, portnummer, utrustningsidentitet, MAC-adresser och abonnemangsidentitet. Med slutpunkt avses även uppgifter om vilken leverantör som tillhandahåller den kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst (se vidare 9 §).

9 §

Vid verksamheter som tillhandahåller kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst ska uppgifter om följande lagras:
– uppgifter om abonnent,
– vilken typ av kapacitet för överföring som har använts och spårbar tid för användandet, samt
– slutpunkter.

Paragrafen reglerar lagringsskyldigheten vid verksamheter som tillhandahåller kapacitet som ger möjlighet till överföring av IP-paket för att få Internetåtkomst. Här är det fråga om det som i strukturen av lagringsskyldigheten (se avsnitt 6.6) benämns anslutningsform.

Frågan om *uppgifter om abonnent* behandlas i avsnitt 6.12.1. Det rör sig om samma typer av uppgifter som ska lagras vid telefoni, meddelandehantering och Internetåtkomst enligt 4, 7 och 8 §§, alltså namn och adress samt person- eller organisationsnummer (se kommentaren till 4 §).

Frågorna om *vilken typ av kapacitet för överföring som har använts och spårbar tid för användandet samt slutpunkter* behandlas i avsnitt 6.12.2. Typ av kapacitet är exempelvis DSL (vilket i sin tur kan ske med hjälp av leverantörer av t.ex. bitströmsaccess), fiberoptiska anslutningar, 3G (UMTS), GSM (GPRS), vanliga traditionella telefonmodem och WLAN (trådlöst nät). Begreppet slutpunkt definieras i 2 § som ändpunkt för varje lagringsskyldigs behandling av kommunikation. Med det avses den tekniska utrustningen i en fysisk ändpunkt som står under leverantörens kontroll och som är gränssnitt mot kund eller abonnent, såsom telefonväxlar, routers, portnummer, utrustningsidentitet, MAC-adresser, abonnemangsidentitet. Vid Internetåtkomst via mobiltelefon eller mobiltelefonmodem för 3G (UMTS) och för GSM (GPRS) är slutpunkterna rörliga. I dessa fall innefattar uppgifter om slutpunkter samma lokaliseringsinformation som vid mobil telefoni (jfr 5 §).

10 §

Lagringsskyldigheten för uppgifter enligt 4-6 §§ gäller även vid misslyckad uppringning.

I bestämmelsen anges att de uppgifter som ska lagras vid telefoni (4-6 §§), oavsett om det rör sig om fast telefoni, mobil telefoni eller Internettelefoni, ska lagras även vid misslyckad uppringning. Frågan behandlas i avsnitt 6.13. Begreppet misslyckad uppringning definieras i 2 § som samtal som kopplats fram utan att få svar eller samtal som kopplats fram utan att nå mottagaren.

11 §

Post- och telestyrelsen får efter samråd med Rikspolisstyrelsen och Datainspektionen meddela verkställighetsföreskrifter om säkerhet enligt 6 kap. 3 § andra stycket lagen (2003:389) om elektronisk kommunikation.

Enligt den föreslagna 6 kap. 6 c § andra stycket LEK meddelar regeringen eller den myndighet som regeringen bestämmer säkerhetsföreskrifter. Frågan behandlas i avsnitt 8.4. I den nu aktuella paragrafen anges att PTS får meddela verkställighetsföreskrifter om säkerhet enligt 6 kap. 3 § andra stycket LEK. Sådana föreskrifter

kan exempelvis avse att trafikuppgifterna ska vara enkelt sökbara, att uppgifterna ska vara logiskt skilda från leverantörernas övriga verksamhet och att endast behörig personal ska ha tillgång till uppgifterna.

Att trafikuppgifterna bör vara enkelt *sökbara* syftar både till en hög kvalitet i lagringen och till ett högt integritetsskydd. En god sökbarhet gör att leverantörerna snabbt kan få fram de trafikuppgifter som är relevanta när de brottsbekämpande myndigheterna begär att få uppgifterna. Genom olika sökbegrepp, som namn och telefonnummer, är det möjligt att snabbt söka igenom stora mängder med information. Med högre precision i sökbegreppen ökar träffsäkerheten i urvalet. Om sökbarheten är god kommer, i förhållande till den totala mängden trafikuppgifter, endast en begränsad mängd uppgifter att tas fram och hanteras vidare av leverantörerna och de brottsbekämpande myndigheterna. Detta minskar risken för att irrelevant information blir tillgänglig för ett mänskligt öga.

Trafikuppgifter för brottsbekämpning som är *logiskt skilda* från de övriga trafikuppgifter som leverantörerna lagrar tar sikte på integritetsskyddet. Säkerheten för lagrade trafikuppgifter påverkas av var i leverantörernas system trafikuppgifterna finns. Om uppgifterna hålls logiskt skilda ökar också möjligheterna till en effektiv sökning. Vissa trafikuppgifter kan behöva lagras för flera syften samtidigt. Precis som fallet är enligt nuvarande ordning måste leverantören ha kontroll över med vilket stöd varje uppgift finns lagrad. Så snart det inte finns något lagligt stöd för att fortsätta behandlingen av uppgifter som lagrats enligt 4-9 §§ måste de utplånas. Att uppgifterna bör vara logiskt skilda från leverantörernas övriga verksamhet innebär inte att uppgifterna ska finnas på två ställen, utan i stället att det är möjligt att klart skilja ut för vilket ändamål respektive uppgift finns lagrad. Om uppgifterna efter lagringstidens slut får sparas enligt andra bestämmelser i 6 kap. LEK kan det vara tillräckligt att uppgifterna i stället avidentifieras.

Att *endast behörig personal har tillgång till trafikuppgifterna* tar sikte på säkerheten. I 6 kap. 3 § andra stycket föreskrivs att leverantörerna ska vidta särskilda tekniska och organisatoriska åtgärder för att säkerställa ett tillräckligt skydd vid behandlingen av lagrade uppgifter. I det ligger bl.a. ett krav på att endast särskilt behörig personal hanterar uppgifterna. Många leverantörer har redan i dag särskilt avdelad personal som handlägger utlämnande av trafikuppgifter. En del leverantörer har säkerhetsskyddsavtal med Säkerhetspolisen, som resulterar i att endast särskild personal har tillgång till

sådana uppgifter som kan ha betydelse för rikets säkerhet. Leverantörerna bör vidta de särskilda tekniska och organisatoriska åtgärder som krävs för att endast särskilt behörig personal har tillgång till och hanterar trafikuppgifterna i systemen och vid ett utlämnande. Det rör sig om åtgärder i form av tillträdeskontroll, åtkomstkontroll, behandlingshistorik och loggar m.m.

I paragrafen anges att den kompetens som finns hos Rikspolisstyrelsen och Datainspektionen ska tas till vara i arbetet med säkerhetsföreskrifter. Det framgår av PTS skyldighet att samråda med de myndigheterna innan föreskrifter meddelas. Även enskilda leverantörers synpunkter kan givetvis inhämtas.

PTS möjligheter att meddela föreskrifter för tillsynen i övrigt på området för elektronisk kommunikation regleras i 4 § förordningen om elektronisk kommunikation.

12 §

Post- och telestyrelsen får efter samråd med Åklagarmyndigheten och Rikspolisstyrelsen i enskilda fall medge undantag från lagringsskyldigheten enligt 6 kap. 6 a § första stycket lagen (2003:389) om elektronisk kommunikation.

Enligt den föreslagna 6 kap. 6 c § andra stycket LEK får regeringen eller den myndighet som regeringen bestämmer i enskilda fall medge undantag från lagringsskyldigheten (jfr 36 § förordningen om elektronisk kommunikation och 6 kap. 19 § fjärde stycket LEK). Frågan behandlas i avsnitt 7.2.3.

I den nu aktuella paragrafen anges att PTS i enskilda fall får medge undantag från lagringsskyldigheten. Det är den enskilde leverantören som kan initiera frågan om undantag genom ansökan till PTS. Leverantörens lagringsskyldighet gäller till dess att PTS har beslutat om undantag. Bestämmelsen är utformad på samma sätt som möjligheten till undantag från anpassningsskyldigheten enligt 6 kap. 19 § fjärde stycket LEK. Om PTS beslutar att en viss leverantör ska vara undantagen från lagringsskyldigheten innebär det att leverantören över huvud taget inte behöver lagra uppgifter. Undantagen är tänkta för de fall där en leverantör bedriver en verksamhet av så liten omfattning att det vid en avvägning mellan det brottsbekämpande intresset av att leverantören lagrar uppgifter och kostnaden för detta inte framstår som rimligt att kräva att leverantören fullgör lagringsskyldigheten. Vid en bedömning av vilket in-

tresse som finns från de brottsbekämpande myndigheternas sida av att en viss verksamhet anpassas för lagring av trafikuppgifter är dessa myndigheters uppfattning helt avgörande. Syftet med lagringsskyldigheten i sig får givetvis inte urholkas. Därför anges det i paragrafen att PTS ska samråda med Åklagarmyndigheten och Rikspolisstyrelsen innan undantag från lagringsskyldigheten medges. De nämnda myndigheterna kan också inhämta synpunkter från andra myndigheter inför ett sådant samråd, t.ex. från Ekobrottsmyndigheten, Tullverket och lokal polismyndighet, som har särskild kunskap om viss brottslighet. Innan undantag medges bör som regel leverantören ha uttömt möjligheten att anlita annan för att fullgöra lagringen. Möjligheten att medge undantag kommer därmed att behöva tillämpas sparsamt. PTS beslut om att medge undantag kan tidsbegränsas och kan komma att omprövas om verksamheten får större omfattning. PTS beslut om undantag får enligt 22 a § förvaltningslagen (1986:223) överklagas hos allmän förvaltningsdomstol. Enligt förslaget till ändring av 5 kap. 1 § sekretesslagen ska det gälla sekretess för uppgifter som hänför sig till PTS verksamhet för prövning av frågor om undantag, om det kan antas att syftet med beslutade eller förutsedda åtgärder motverkas eller den framtida verksamheten skadas om uppgiften röjs (se avsnitt 17.1).

13 §

Post- och telestyrelsen får efter samråd med Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen och Tullverket meddela föreskrifter om den ersättning som lagringsskyldiga har rätt till enligt 6 kap. 6 d § lagen (2003:389) om elektronisk kommunikation.

Enligt den föreslagna 6 kap. 6 d § LEK meddelar regeringen eller den myndighet regeringen bestämmer föreskrifter om den ersättning för utlämnandet som lagringsskyldiga har rätt till. Frågan om ersättning behandlas i avsnitt 13.8.4.

I den nu aktuella paragrafen anges att PTS får meddela föreskrifter om ersättning. Föreskrifterna bör ges i form av vissa schablonbelopp. Schablonbeloppen bör bestämmas utifrån de kostnader som en leverantör med goda rutiner har i samband med utlämnande av trafikuppgifter. Det rör sig t.ex. om kostnader för tekniska system för att enkelt kunna söka efter uppgifter som omfattas av myndighetens begäran, kostnader för den personal som ska hantera

och lämna ut uppgifterna (t.ex. för arbete utanför kontorstid), kostnader för att hitta ett gemensamt gränssnitt till mottagaren och kostnader för drift och underhåll av de tekniska systemen. Däremot täcker ersättningen inte kostnaderna för själva lagringen, dvs. kostnaderna för att identifiera, spara och lagra uppgifterna.

PTS ska samråda med Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen (bl.a. Säkerhetspolisen och Rikskriminalpolisen) och Tullverket innan föreskrifterna meddelas. Även leverantörers synpunkter bör givetvis vägas in när ersättningsfrågorna regleras.

Det är den brottsbekämpande myndighet som begär uppgifter som ska betala ersättning. I en och samma utredning kan myndigheten behöva betala ersättning till flera leverantörer. Myndigheten kan också behöva betala ersättning till samma leverantör vid flera tillfällen i samma utredning om begäran sker flera gånger, dvs. när det är fråga om flera beslut om hemlig teleövervakning eller flera begäran om utlämnande enligt lagen om elektronisk kommunikation.

I avsnitt 7.4 behandlas frågan om att en leverantör ska bedriva verksamheten så att uppgifterna enkelt kan tas om hand och lämnas ut utan dröjsmål (se den föreslagna 6 kap. 19 a § LEK). Det innebär att överföring av uppgifter från leverantören till myndigheten kan behöva ske vid flera tillfällen för att verkställa en och samma begäran. Ersättningen ska utgå för varje begäran oavsett hur många utlämnanden eller ”delleveranser” som behöver göras inom ramen för varje begäran.

Skyldigheten att utge ersättning inträder först när den brottsbekämpande myndigheten har fått samtliga uppgifter som kan levereras, dvs. när leverantören har helt verkställt en begäran om utlämnande av trafikuppgifter.

Särskilt yttrande av Hans-Olof Lindblom

Lagringsskyldighetens omfattning bör vara noggrant reglerad i av Riksdagen beslutad lag och endast Riksdagen bör få besluta om väsentliga förändringar i lagringsskyldighetens omfattning

Med hänsyn till de långtgående effekter lagring av trafikuppgifter kan ha för alla medborgare och deras privatliv bör lagringsskyldighetens omfattning noggrant regleras i av Riksdagen beslutad lag och på ett sätt som garanterar att behovet av utvidgningar i lagringsskyldighetens omfattning övervägs lika noga. Enligt min mening bör således Riksdagens medverkan också krävas för att väsentliga ändringar av lagringsskyldighetens omfattning ska få genomföras. Mot den bakgrunden kan jag inte acceptera utredningens föreslagna författningsreglering. Detta eftersom utredningens lagförslag innehåller en mycket allmänt utformad regel i fråga om vilka uppgifter som ska lagras och som överlämnar till regeringen att inom en alltför vid ram besluta om vilka närmare uppgifter om medborgarnas kommunikation som ska lagras.

Beslutet att lagra kommunikationsuppgifter för att bekämpa allvarlig brottslighet är en extraordinär åtgärd av aldrig tidigare skådat slag med historiska dimensioner. Det inkräktar på medborgarnas dagliga liv och kan riskera de grundläggande värden och friheter som alla europeiska medborgare har och vårdar.

Dessa ord av Artikel 29-gruppen belyser vilka grundläggande värden och friheter som nu står på spel. Att Riksdagens medverkan och beslut ska krävas för sådana ingrepp i enskildas liv framstår som helt givet. Emellertid innebär förslaget i betänkandet att EG-direktivets mycket detaljerade reglering av vilka uppgifter som ska lagras genomförs genom bestämmelser i lagen om elektronisk kommunikation (LEK) som anger att lagringsskyldigheten omfattar uppgifter om abonnemang och annan uppgift som angår ett sär-

skilt elektroniskt meddelande (uppgifter som avses i 6 kap. 20 § först stycket 1 och 3 LEK). Enlig lagförslaget meddelar regeringen föreskrifter om lagringsskyldighet. Detta innebär att Riksdagen överlämnar till regeringen att inom en mycket vid ram bestämma vilka uppgifter om enskildas kommunikation som ska lagras. Den rättsliga ramen innebär i sig en väsentlig utvidgning i förhållande till den lagringsskyldighet som EU beslutat om genom antagande av lagringsdirektivet (2006/24/EG). Utredningens lagförslag innebär också att Riksdagen överlämnar till regeringen att vid behov besluta om förändringar av lagringsskyldighetens omfattning. Även om utredningen i sitt förslag till förordningsreglering i huvudsak föreslår en lagringsskyldighet som följer EG-direktivets krav finns det med utredningens lagtekniska utformning en risk för att lagringsskyldigheten i Sverige med tiden kan komma att få en omfattning som väsentligt avviker från EG-direktivet och som Riksdagen då inte haft att särskilt ta ställning till.

Som framgått anser jag att det bör vara Riksdagen som beslutar om lagringsskyldighetens omfattning och väsentliga förändringar av den såsom eventuella avvikelser och utvidgningar i förhållande till EG-direktivet. Det kan ske genom att man i lagen om elektronisk kommunikation (LEK) inför en detaljreglering motsvarande den i EG-direktivet. Att göra det i 6 kap. LEK passar dock mindre bra med hänsyn till att det kapitlet har rubriken integritetsskydd. Mot en detaljreglering i LEK kan också anföras författningstekniska skäl hänförliga till hur den lagen i övrigt är utformad. Ett alternativ kan då istället vara reglering i en särskild ny lag med detaljerade bestämmer om vilka uppgifter som ska lagras och de övriga bestämmelser som föranleds av lagringsdirektivet, såsom bestämmelser om ändamål, säkerhet och utlämnande.

Frågan om bestämmelserna om tillgången till trafikuppgifter behöver ändras kräver ytterligare analys

Med hänsyn till rättsäkerhetsaspekterna och mot bakgrund av syftet med lagringsdirektivet anser jag att frågan om bestämmelserna om utlämnade av trafikuppgifter behöver analyseras närmare.

I betänkandet gör utredningen bedömningen att den föreslagna lagringen av trafikuppgifter inte ger anledning att förändra bestämmelserna om utlämnande enligt lagen om elektronisk kommunikation. Utredningen föreslår att de uppgifter som operatörer

m.fl. ska vara skyldiga att lagra ska få lämnas ut inte bara enligt reglerna i 27 kap. 19 § rättegångsbalken utan också enligt 6 kap. 22 § första stycket 2 och 3 lagen om elektronisk kommunikation (LEK).

Förutsättningarna för utlämnande av trafikuppgifter skiljer sig i väsentliga avseenden åt när det gäller utlämnande enligt reglerna i 27 kap. rättegångsbalken och de i lagen om elektronisk kommunikation (LEK). Ett utlämnande enligt LEK ställer inte krav på att det ska finnas en skäligen misstänkt person, att åtgärden ska bedömas ha synnerlig vikt för utredningen och att åtgärden enbart får avse enbart vissa teleadresser och telenät. Ett utlämnande enligt LEK förutsätter heller inte krav på tillstånd av domstol. Tidigare utredningar såsom BRU har visat på dessa skillnader och har lämnat förslag om upphävande av reglerna i LEK. För den enskilde skulle det innebära en ökad rättsäkerhet och en förstärkning av integritetsskyddet. Den obligatoriska lagringsskyldighet som nu föreslås innebär att uppgifter om enskildas kommunikation kommer att finnas lagrade i en helt annan omfattning än tidigare. Det innebär att det är än mer angeläget att åtgärda skillnaderna i rättsäkerhetskrav mellan utlämnande enligt rättegångsbalken och LEK. Till detta kommer att syftet med lagringen av trafikuppgifter enligt lagringsdirektivet är att uppgifterna ska finnas tillgängliga för utredning, avslöjande och åtal av allvarliga brott. Jag utesluter inte att det medför att förutsättningarna för utlämnande av trafikuppgifter som omfattas av lagringsdirektivet måste ställas högre än vad som nu gäller för uppgifter som operatörerna bevarar för sin verksamhet. Det kan ifrågasättas om utredningens förslag om att lagrade uppgifter ska få lämnas ut enligt LEK är förenligt med lagringsdirektivets syfte att komma åt allvarlig brottslighet. Det gäller särskilt förslaget om utlämnande enligt 6 kap. 22 § första stycket 2 LEK.

Av ingresspunkt 9 i EG-direktivet framgår att antagandet av ett instrument om lagring av trafikuppgifter ansetts som en, enligt artikel 8 i den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, nödvändig åtgärd. I ingresspunkt 25 erinras dock om att medlemsstaternas lagar eller lagstiftningsåtgärder om rätten till tillgång till och användning av uppgifterna måste till fullo respektera de grundläggande rättigheter som är garanterade i den konventionen. Det innebär enligt vad som närmare anges i samma ingresspunkt ett krav på att offentliga myndigheters intrång i rätten till privatliv måste stå i förhållande till vad som är nödvändigt och proportionerligt och därför tjäna

närmare angivna, tydliga och legitima syften samt utövas på ett sätt som är rimligt och relevant och som inte är överdrivet i förhållande till syftet med intrånget.

Enligt min mening har utredningen inte utfört en tillräcklig analys av om de regler för utlämnande som nu föreslås gälla för lagrade trafikuppgifter kommer att vara förenliga med kraven i den Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Enligt min bedömning kräver en sådan analys med nödvändighet bl.a. en närmare beskrivning av hur reglerna i LEK om utlämnande hittills tillämpats och noggranna överväganden kring hur tillämpningen kan komma att förändras av att operatörerna nu blir skyldiga att lagra och hålla trafikuppgifterna tillgängliga.

Särskilt yttrande av Per Furberg

Jag ansluter mig till Hans-Olof Lindbloms särskilda yttrande och vill för egen del tillägga följande:

Enligt min mening är det av vikt att lagstiftningen gör en tydlig åtskillnad mellan de uppgifter som måste lagras enligt lagringsdirektivet och de uppgifter som vi i Sverige väljer att på annan grund införa en lagringsskyldighet för.

Den skarpa skillnad som följer av berörda direktiv, mellan ett bevarande enligt kraven i lagringsdirektivet respektive lagring med stöd av undantagsbestämmelserna i direktivet om integritet och elektronisk kommunikation, kommer emellertid inte till närmare uttryck i utredningsförslaget. Den författningstekniska lösningen för samman dessa olika kategorier av uppgifter under samma bestämmelser. Därtill har motiven för förslagen i vissa fall utformats så att det som ett ”andrahandsalternativ” – om viss uppgift inte skulle omfattas av lagringsdirektivet – görs gällande att det i vart fall finns stöd i artikel 15.1 i direktivet om integritet och elektronisk kommunikation för en lagring (se t.ex. avsnitt 6:14). Utredningen redovisar dock inte någon närmare genomgång av de förutsättningar som måste vara uppfyllda för att kunna införa en lagringsskyldighet med stöd av undantagsbestämmelserna i artikel 15.1 och inte heller av hur länge lagring kan ske med ett sådant rättsligt stöd. Enligt min mening är förutsättningarna i dessa delar inte tillräckligt genomlysta.

Utredningen har gjort sådana extensiva tolkningar av artikel 11 i lagringsdirektivet – där det föreskrivs att artikel 15.1 i direktivet om integritet och elektronisk kommunikation inte skall tillämpas på ”uppgifter *som specifikt skall lagras*” enligt lagringsdirektivet (kursiverat här) – att direktivets detaljerade uppräkningar synes ha uppfattats närmast som exempel, inte som en avgränsning av vad som ”specifikt” skall få lagras. Jag ifrågasätter dessa tolkningars riktighet.

Vidare bör den argumentation från effektivitetssynpunkt som utredningen för fram i flera olika avsnitt uppmärksammas. Betänkandet innehåller visserligen ett inledande och ett avslutande avsnitt om integritetsfrågor. I övrigt präglas beskrivningarna emellertid av citat från BRU där rader av skäl för en ökad och effektivare användning av trafikuppgifter i brottsutredningar räknas upp och stöds av förstärkande ord, utan motsvarande uppräkningar av de integritetshänsyn som måste ställas mot effektivitetsskälen. Jag delar inte den bedömning som dessa uppräkningar indirekt ger uttryck för.

Slutligen vill jag påpeka att utredningens genomgång av vilka som skall anses vara lagringsskyldiga ger vid handen att en betydande gråzon kommer att finnas. Denna torde komma att drabba sådana mindre aktörer som vanligtvis saknar resurser för rättsutredningar. Dessa oklarheter kan dessutom komma att utgöra hinder i utvecklingen av nya elektroniska tjänster som tillhandahålls från Sverige. När en tjänst hamnar i denna gråzon torde tillhandahållaren i stället komma att förlägga tjänsten till andra länder än Sverige. Frågan blir också av betydelse från integritetssynpunkt. Enligt min mening behöver ärendet beredas ytterligare i denna del.

Kommittédirektiv

Genomförande av EG:s direktiv om lagring av trafikuppgifter

Dir. 2006:49

Beslut vid regeringssammanträde den 18 maj 2006

Sammanfattning av uppdraget

En särskild utredare får i uppdrag att lämna förslag till hur Europaparlamentens 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[4] skall genomföras i svensk rätt.

Utredaren skall lämna förslag till de författningsändringar som är nödvändiga och övriga åtgärder som direktivet kan ge anledning till. Utredningens arbete skall ske i nära samverkan med berörda myndigheter, näringsliv och företrädare för berörda branscher. Utredaren skall följa det arbete som EU:s organ och medlemsstaterna kan komma att initiera med anledning av de nationella genomförandena av direktivet.

Uppdraget skall redovisas senast den 1 april 2007.

[4] EUT L 105, 13.4.2006, s. 54 (Celex 32006L0024).

EG:s direktiv om lagring av trafikuppgifter

Efter bombattentaten i Madrid den 25 mars 2004 fick rådet för rättsliga och inrikes frågor (RIF) i uppdrag av Europeiska rådet att snarast anta gemensamma åtgärder om lagring av trafikuppgifter. Ett antal länder, däribland Sverige, utarbetade ett förslag som presenterades under sommaren 2004 och som förhandlades under 2004 och 2005.

Europaparlamentet och rådet antog den 15 mars 2006 direktiv 2006/24/EG om lagring av trafikuppgifter. Direktivet syftar till att harmonisera medlemsstaternas regler om de skyldigheter som leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät har att lagra vissa uppgifter som genereras eller behandlas i samband med att en kommunikation sker per fast eller mobil telefoni, eller på Internet. Med uppgifter avses i direktivet trafik- och lokaliseringsuppgifter samt de uppgifter som behövs för att identifiera en abonnent eller användare (nedan används begreppet trafikuppgifter; samtliga ovannämnda uppgifter avses emellertid). Tanken är att se till att trafikuppgifter skall finnas tillgängliga och kunna lämnas ut till de brottsbekämpande myndigheterna för att de skall kunna avslöja, utreda och åtala för allvarlig brottslighet, såsom denna definieras i nationell lag. Direktivet hindrar inte medlemsstaterna att i sin nationella lagstiftning införa eller behålla en längre gående lagringsskyldighet för andra trafikuppgifter än vad som följer av direktivet, eftersom artikel 15.1 i direktivet 2002/58/EG om integritet och elektronisk kommunikation alltjämt gäller för dessa delar.

Direktivet anger de kategorier av uppgifter som skall lagras. Dessa kategorier är uppdelade på fast och mobil telefoni samt Internetåtkomst, e-post och Internettelefoni. De uppgifter som skall lagras svarar främst, enkelt uttryckt, på frågorna *vem* kommunicerade med *vem*, *när* skedde det, *var* befann sig de som kommunicerade med varandra och *vilken* typ av kommunikation användes vid tillfället. Lagringsskyldigheten omfattar inte innehållet i en kommunikation. Direktivet anger lagringstiden för alla kategorier av trafikuppgifter till minst sex månader och högst två år, med möjlighet att ha en tidsbegränsad längre

lagringstid vid särskilda omständigheter. Dessa åtgärder skall i sådana fall godkännas av EG-kommissionen.

Direktivet innehåller också bestämmelser om bl.a. skydd av personuppgifter, statistik och utvärdering.

Behovet av en utredning

I svensk lagstiftning finns inga krav på att nät- och tjänsteleverantörer skall anpassa sin verksamhet för att kunna lagra historiska trafikuppgifter för brottsbekämpningsändamål. Tvärtom gäller enligt 6 kap. 5 § lagen (2003:389) om elektronisk kommunikation som huvudregel att trafikuppgifter skall *utplånas* eller *avidentifieras* när de inte längre behövs för att överföra ett elektroniskt meddelande. Undantag från denna ordning gäller enligt 6 kap. 6 och 8 §§ samma lag om uppgifterna behövs t.ex. för fakturering, betalning av samtrafikavgifter eller för att förhindra eller avslöja obehörig användning av ett nät eller en tjänst. I den mån trafikuppgifter finns kvar, kan polis och åklagare få tillgång till dessa t.ex. efter ett beslut om hemlig teleövervakning enligt 27 kap. rättegångsbalken. Även om en nät- och tjänsteleverantör enligt 6 kap. 19 § lagen om elektronisk kommunikation skall anpassa sin verksamhet så att ett beslut om hemlig teleövervakning kan verkställas (s.k. anpassningsskyldighet) innebär det inget krav på att trafikuppgifter måste lagras (se prop. 2002/03:74 s. 39). Anpassningsskyldigheten avser endast övervakning i realtid. För Sveriges del medför direktivets krav på att historiska trafikuppgifter skall lagras således ett behov av ändringar i lag.

Nät- och tjänsteleverantörers anpassningsskyldighet enligt 6 kap. 19 § lagen om elektronisk kommunikation omfattar enbart dem som tillhandahåller allmänna kommunikationsnät eller tjänster inom sådana nät; vid tjänster finns vissa begränsningar i anpassningsskyldigheten när det gäller datakommunikation. Det skall jämföras med direktivet som inte innehåller några sådana begränsningar. Detta innebär således att anpassningsskyldigheten måste utökas till att även omfatta de krav som direktivet anger beträffande historiska trafikuppgifter.

Enligt direktivet skall tillgången till trafikuppgifter regleras i nationell rätt, med beaktande av Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Polis och åklagare kan i dag få tillgång till historiska trafikuppgifter från en nät- eller tjänsteleverantör enligt vissa bestämmelser i lag. Som nämnts ovan kan det ske efter ett domstolsbeslut om hemlig teleövervakning enligt 27 kap. 19 § rättegångsbalken, varvid bl.a. som huvudregel krävs att det finns en person som är skäligen misstänkt för brott med ett minimistraff om sex månaders fängelse. Trafikuppgifterna kan även inhämtas genom att den tystnadsplikt som åligger nät- och tjänsteleverantörer enligt 6 kap. 20–21 §§ i lagen om elektronisk kommunikation bryts, se 6 kap. 22 § samma lag. För detta krävs att utredningen avser ett brott vars minimistraff är två års fängelse. Uppgifter om abonnemang kan dock lämnas ut om fängelse är föreskrivet för brottet och det bedöms kunna föranleda annan påföljd än böter.

Om det är en myndighet som bedriver televerksamhet gäller sekretesslagens (1980:100) bestämmelser (se 9 kap. 8 § och 14 kap. 2 § fjärde och femte styckena nämnda lag).

Syftet med direktivet är att trafikuppgifter skall lagras för att kunna lämnas ut och användas i utredningar av allvarlig brottslighet. Vad som är allvarlig brottslighet är upp till varje stat att avgöra, men enligt en förklaring till direktivet skall hänsyn tas till den lista som finns i artikel 2 i rambeslutet om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (2002/584/RIF), vilket kan medföra att vissa överväganden kan behöva göras vid det nationella genomförandet av direktivet.

De kostnader som uppkommer för nät- och tjänsteleverantörer i samband med att de skall anpassa sin verksamhet enligt 6 kap. 19 § lagen om elektronisk kommunikation belastar i dag nät- och tjänsteleverantörerna. Däremot kan dessa kräva ersättning vid verkställighet av ett beslut om hemlig teleövervakning eller vid utlämnande av uppgifter enligt 6 kap. 22 § samma lag. Det saknas däremot bestämmelser i lag eller annan författning om vilken nivå på ersättningen som nät- och tjänsteleverantörerna kan kräva i ett enskilt fall. Direktivet reglerar inte kost-

nadsfrågan i något avseende, men ett genomförande av direktivet medför att överväganden i dessa frågor måste ske.

Enligt 6 kap. 2 § lagen om elektronisk kommunikation gäller bestämmelserna i personuppgiftslagen (1998:204). Denna lag genomför direktivet 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (dataskyddsdirektivet), vars syfte bl.a. är att skapa ett skydd vid behandling av personuppgifter. Genom lagen om elektronisk kommunikation genomförs även direktivet om integritet och elektronisk kommunikation (2002/58/EG) som kompletterar dataskyddsdirektivet. Enligt direktivet om lagring av trafikuppgifter skall bestämmelserna om skydd vid behandling av personuppgifter enligt de nämnda direktiven även gälla vid lagring av historiska trafikuppgifter. Med hänsyn till att stora mängder trafikuppgifter kommer att lagras under en längre tid kan det finnas skäl att närmare se över om det behövs ytterligare skyddsregler, inklusive regler om informationssäkerhet.

Tidigare utredningsarbete

Genom kommittédirektiv som beslutades den 7 december 2000 (dir. 2000:90) upprättades Beredningen för rättsväsendets utveckling (BRU). En huvuduppgift för BRU var att öka effektiviteten och kvaliteten i rättsväsendets arbete. Genom åren har BRU lagt fram ett flertal förslag. I betänkandet Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74) föreslår BRU bl.a. att verkställighet av beslut om hemlig teleavlyssning och hemlig teleövervakning samt utlämnande av uppgifter enligt 6 kap. 22 § lagen om elektronisk kommunikation skall ske utan kostnader för de brottsbekämpande myndigheterna. Denna fråga bereds inom Regeringskansliet (Justitiedepartementet).

Genom tilläggsdirektiv den 20 november 2003 (dir. 2003:145) fick BRU i uppdrag att bl.a. göra en översyn av det regelverk som styr de brottsbekämpande myndigheternas möjligheter att få tillgång till innehållet i och uppgifter om elektronisk kommunikation. I maj 2005 överlämnades betänkandet

Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38). I betänkandet föreslås en modernisering av rättegångsbalkens terminologi i de bestämmelser som reglerar bl.a. hemlig teleövervakning. Anpassningsskyldigheten vidgas till att omfatta de verksamheter som i dag kan bli föremål för ett beslut om hemlig teleövervakning. Vidare föreslås att tillgången till trafikuppgifter uteslutande skall regleras i 27 kap. rättegångsbalken, vilket innebär att motsvarande bestämmelser i lagen om elektronisk kommunikation i huvudsak förs över till rättegångsbalken. En ändring som dock föreslås är att polis- och åklagarmyndighet alltid skall kunna få tillgång till uppgifter om abonnemang oavsett vilken påföljd brottet kan föranleda.

BRU föreslår att nät- och tjänsteleverantörerna även fortsättningsvis skall stå för de anpassningskostnader som krävs. Förslaget kommer enligt beredningen att leda till ökade kostnader för dessa, men kostnaderna kommer att kunna föras över till abonnenterna och för dem bli försumbara.

Med hänsyn till de då pågående förhandlingarna om det direktiv om lagring av trafikuppgifter som nu antagits lämnade BRU inte några förslag i frågan om skyldigheten för nät- och tjänsteleverantörer att bevara trafikuppgifter under viss tid för brottsbekämpande ändamål, även om denna fråga omfattades av tilläggsdirektivet. BRU beskrev dock det stora behovet för de brottsutredande myndigheterna att få tillgång till trafikuppgifter i förundersökningar och de problem som bristen i nuvarande lagstiftning innebär i detta avseende.

BRU:s betänkande bereds nu inom Regeringskansliet (Justitiedepartementet).

Uppdraget

Utredaren skall ta ställning till hur direktivet om lagring av trafikuppgifter skall genomföras i svensk rätt och lämna förslag till de författningsändringar som behövs.

Syftet med direktivet, dvs. att säkerställa att historiska trafikuppgifter finns tillgängliga och kan lämnas ut i brottsutredningar vid misstanke om allvarliga brott, är utgångspunkten vid genomförandet av direktivet. Genomförandet skall ske med hän-

syn till den tekniska utvecklingen som sker inom området för elektronisk kommunikation. Utredaren skall också beakta behovet av en väl fungerande konkurrens på marknaden i allmänhet samt hur förslagen i utredningen påverkar konkurrensen mellan stora och små aktörer och möjligheten till marknadstillträde. Utredaren skall vidare ta hänsyn till hur förslagen påverkar såväl etablerade som presumtiva aktörers investeringsvilja.

De bestämmelser som utredaren föreslår skall i möjligaste mån vara teknikneutrala. Samtidigt skall utredaren beakta behovet av tydliga och väl avgränsade regler.

Med hänsyn till att stora mängder trafikuppgifter skall lagras skall utredaren i anslutning till sina förslag belysa de integritetsaspekter som aktualiseras. Detta skall ske med utgångspunkt i 2 kap. regeringsformen samt artikel 8 i Europakonventionen så att det nationella genomförandet av direktivet är förenligt med dessa stadganden. Utredaren kan därvidlag föreslå regler som syftar till att stärka skyddet och motverka missbruk av personuppgifterna och som är förenliga med dataskyddsdirektivet (95/46/EG) och direktivet om integritet och elektronisk kommunikation (2002/58/EG), till vilka direktivet om lagring av trafikuppgifter hänvisar.

Anpassningsskyldigheten

Utredaren skall utforma en anpassningsskyldighet för nät- och tjänsteleverantörer när det gäller lagring av historiska trafikuppgifter enligt direktivet. I de förslag som utredaren lägger fram skall målsättningen vidare vara att trafikuppgifterna skall lagras endast hos en nät- eller tjänsteleverantör och inte hos flera sådana aktörer samtidigt. När det gäller hur lång tid uppgifterna skall lagras bör utgångspunkten för utredarens arbete vara att lagringstiden inte skall understiga ett år för någon typ av trafikuppgift. Andra lagringstider är dock möjliga om detta bedöms vara lämpligt.

Historiska trafikuppgifter är ofta av grundläggande betydelse vid utredning av allvarlig brottslighet. Det är därför av stor vikt att den anpassningsskyldighet som utformas resulterar i att de brottsbekämpande myndigheterna får tillgång till den informa-

tion de behöver. Vissa typer av trafikuppgifter omfattas dock inte av direktivets lagringsskyldighet. Utredaren skall därför utifrån artikel 15.1 i direktivet om integritet och elektronisk kommunikation (2002/58/EG) analysera de brottsbekämpande myndigheternas behov av att få tillgång till trafikuppgifter som inte uttryckligen följer av direktivets lagringsskyldighet. Lagringsskyldigheten skall emellertid inte omfatta andra trafikuppgifter än sådana som myndigheterna kan ha tillgång till i dag och som avser fast och mobil telefoni, samt Internetåtkomst, e-post och Internettelefoni.

När det sedan gäller vem som skall lagra de olika trafikuppgifterna anger direktivet leverantörer av *allmänna* kommunikationsnät eller *allmänt* tillgängliga elektroniska kommunikationstjänster. I detta ligger en begränsning i vilka nät- och tjänsteleverantörer som skall omfattas av anpassningsskyldigheten. Av samma skäl som anges ovan om de brottsbekämpande myndigheternas behov av att få tillgång till viktig information, skall utredaren överväga om sådana nät- och tjänsteleverantörer som inte omnämns i direktivet bör omfattas av en skyldighet att lagra och lämna ut trafikuppgifter.

Kostnadsfrågan

Ett genomförande av direktivet kommer att medföra kostnader dels för att genomföra den anpassningsskyldighet som direktivet medför, dels vid utlämnandet av trafikuppgifter i varje enskilt ärende.

I dag står nät- och tjänsteleverantörerna för den anpassningskostnad som följer av lagen om elektronisk kommunikation. Detta gäller dock endast hemlig teleövervakning i realtid eftersom anpassningsskyldigheten inte omfattar ett krav att lagra historiska trafikuppgifter. Däremot kräver dessa leverantörer som huvudregel ersättning när uppgifterna, i den mån de finns, skall tas fram och lämnas ut till de brottsbekämpande myndigheterna.

Utredaren skall analysera vilka kostnader som uppstår till följd av de förslag som läggs fram när det gäller att lagra historiska trafikuppgifter och att lämna ut trafikuppgifterna i enskil-

da ärenden. Utifrån dessa kostnadsberäkningar skall utredaren föreslå hur kostnaderna skall fördelas mellan det allmänna och nät- och tjänsteleverantörerna. Utredaren skall analysera och redogöra för olika alternativ till hur kostnaderna kan fördelas samt de för- och nackdelar de olika alternativen medför. När det gäller frågan om vem som skall stå för kostnaderna skall utredaren särskilt beakta vilken lösning som blir samhällsekonomiskt mest kostnadseffektiv.

Övriga frågor

Direktivet anger att det är upp till medlemsstaterna att i sin nationella lagstiftning reglera förutsättningarna att få tillgång till trafikuppgifterna. Utgångspunkten är att de förutsättningar som gäller i dag för att få tillgång till trafikuppgifter även skall gälla för de ytterligare trafikuppgifter som kommer att lagras till följd av direktivet. Utredaren skall emellertid analysera om direktivets hänvisning till Europakonventionen bör medföra ändringar i de förutsättningar som gäller för de brottsbekämpande myndigheterna att få tillgång till trafikuppgifter i ett enskilt ärende. Skulle utredaren vidare finna att direktivets fokus på allvarlig brottslighet och den koppling som görs till den lista över brott som finns i rambeslutet om en europeisk arresteringsorder och överlämnande mellan medlemsstaterna (2002/584/RIF) motiverar lagändringar i detta avseende, får utredaren föreslå nödvändiga lagändringar.

Utredaren skall, utöver vad som ovan har beskrivits närmare, ta ställning till om det krävs ytterligare åtgärder för direktivets genomförande i svensk lagstiftning.

Arbetsformer och redovisning av uppdraget

Förutom att utredaren skall arbeta med experter, sakkunniga och referensgrupper skall utredaren särskilt uppmärksamma behovet av samråd med berörda myndigheter samt med företrädare för berörda branscher och med näringslivet. Utredaren skall också följa det arbete som EU:s organ och medlemsstaterna kan komma att initiera med anledning av de nationella genom-

förandena av direktivet, t.ex. den s.k. artikel 29-gruppen, vilken har inrättats som ett rådgivande organ inom EU med stöd av artikel 29 i dataskyddsdirektivet.

Till stöd för sina bedömningar skall utredaren inhämta upplysningar om den rättsliga regleringen av motsvarande åtgärder och planerade förändringar i den nationella rätten i några av de närliggande EU-länderna, företrädesvis Danmark, Finland och de baltiska staterna men också i några andra jämförbara länder.

Utredaren skall under arbetet följa den fortsatta beredningen av BRU:s förslag i betänkandena Ökad effektivitet och rättssäkerhet i brottsbekämpningen (SOU 2003:74) och Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38). Utredaren skall vidare beakta det arbete som bedrivs av den parlamentariska kommitté som har i uppdrag att kartlägga och analysera sådan lagstiftning som berör den personliga integriteten (dir. 2004:51). Utredaren skall också uppmärksamma pågående arbeten och lagförslag samt sådana utredningar som initieras under arbetets gång på närliggande områden.

I den mån lagförslagen förväntas leda till kostnadsökningar för det allmänna skall utredaren föreslå hur dessa skall finansieras. Andra konsekvenser vid genomförandet av direktivet skall presenteras enligt bestämmelserna i kommittéförordningen (1998:1474).

Uppdraget skall redovisas senast den 1 april 2007. Utredaren är emellertid fri att dessförinnan, om utredaren finner detta möjligt, lämna ett delbetänkande som avser genomförandet av direktivet i de delar som gäller fast och mobil telefoni.

(Justitiedepartementet)

Kommittédirektiv

Tilläggsdirektiv till Trafikuppgifts-utredningen (Ju 2006:04)

Dir. 2007:37

Beslut vid regeringssammanträde den 15 mars 2007

Förlängd tid för uppdraget

Med stöd av regeringens bemyndigande den 18 maj 2006 gav chefen för Justitiedepartementet en särskild utredare i uppdrag att lämna förslag till hur Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (EUT L 105, 13.4.2006, s. 54, Celex 32006L0024) skall genomföras i svensk rätt (dir. 2006:49). Uppdraget skulle redovisas senast den 1 april 2007.

Utredningen har antagit namnet Trafikuppgiftsutredningen (Ju 2006:04).

Utredningstiden förlängs. Uppdraget skall i stället redovisas senast den 1 november 2007.

(Justitiedepartementet)

Statens offentliga utredningar 2007

Kronologisk förteckning

1. Telefonförsäljning. Jo.
2. Från socialbidrag till arbete.
   + Bilaga. Fördjupningsstudier.
   + Lättläst. Sammanfattning. S.
3. Föräldraskap vid assisterad befruktning. Ju.
4. Trafikinspektionen
   – en myndighet för säkerhet och skydd inom transportområdet. N.
5. Summa summarum – en fristående myndighet för utredning av anmälningar om brott av poliser och åklagare? Ju.
6. Målsägandebiträdet.
   Ett aktivt stöd i rättsprocessen. Ju.
7. Den nya inskrivningsmyndigheten. M.
8. Nya förutsättningar för ekobrottsbekämpning. Ju.
9. Svenskan i världen. UD.
10. Hållbar samhällsorganisation med utvecklingskraft. Fi.
11. Regional utveckling och regional samhällsorganisation. Fi
12. Hälso- och sjukvården. Fi.
13. Staten och kommunerna – uppgifter, struktur och relation. Fi.
14. Renovering av bostadsmarknad efterlyses!
    Om ungas möjligheter till en egen bostad.
    Rapport nr 1:
    Om bara någon kunde säga vad jag ska göra för att få en bostad så skulle jag göra det.
    Rapport nr 2:
    Måste man ha tur?
    Studier av yngre på bostadsmarknaden i svenska städer.
    Rapport nr 3:
    Effektiv bostadsservice och förmedling av bostäder – ur ett dubbelt användarperspektiv.
    Rapport nr 4:
    Unga vuxna på bolånemarknaden. M.
15. Stöd för framtiden – om förutsättningar för jämställdhetsintegrering.
    Idébok:
    Jämställd medborgarservice. Goda råd om jämställdhetsintegreringen. En idébok för chefer och strateger.
    Metodbok:
    JämStöd Praktika. Metodbok för jämställdhetsintegrering. IJ.
16. Ändrad könstillhörighet – förslag till ny lag. S.
17. Äktenskap för par med samma kön. Vigselfrågor. Ju.
18. Arbetsmarknadsutbildning för bristyrken och insatser för arbetslösa ungdomar. N.
19. Friskare tänder – till rimliga kostnader. S.
20. Administrativa sanktioner på yrkesfiskets område. Jo.
21. GMO-skador i naturen och Miljöbalkens försäkringar. M.
22. Skyddet för den personliga integriteten. Kartläggning och analys. Del 1+2. Ju.
23. Genomförande av tredje penningtvättsdirektivet. Fi.
24. Veterinär fältverksamhet i nya former. Jo.
25. Plats för tillväxt? Fi.
26. Alternativ tvistlösning. Ju.
27. Auktorisation av patentombud. N.
28. Tydliga mål och kunskapskrav i grundskolan. Förslag till nytt mål- och uppföljningssystem. U.
29. Hur tillämpas expropriationslagens ersättningsbestämmelser? Ju.
30. Två nya statliga specialskolor.
    + Lättläst+ Daisy. U.
31. Alltid redo! En ny myndighet mot olyckor och kriser. Fö.
32. Tillväxt genom turistnäringen. N.
33. Släpvagnskörning med B-körkort
    – när kan de nya EU-reglerna börja tillämpas? N.
34. Skolgång för barn som skall avvisas eller utvisas. Ju.

35. Flyttning och pendling i Sverige. Fi.
36. Bioenergi från jordbruket – en växande resurs. + Bilagedel. Jo.
37. Vård med omsorg – möjligheter och hinder. S.
38. Kunskapsläget på kärnavfallsområdet 2007. Nu levandes ansvar, framtida generationers frihet. M.
39. Framtidens polis. Ju.
40. Valsystem och representationseffekter. En jämförande studie av 25 länder. Ju.
41. Misstroendeförklaring och regeringsbildning 1994–2006. Regeltillämpning och författningspolitiska alternativ. Ju.
42. Från statsminister till president? Sveriges regeringschef i ett jämförande perspektiv. Ju.
43. Bättre arbetsmiljöregler II. Skyddsombud, beställaransvar, byggarbetsplatser m.m. A.
44. Tsunamibanden. Fi.
45. Utökat elektroniskt informationsutbyte. Fi.
46. Ansvarsfrågan vid odling av genmodifierade grödor. Jo.
47. Den osynliga infrastrukturen – om förbättrad samordning av offentlig IT-standardisering. N.
48. Patientdata och läkemedel m.m. S.
49. Organisationsform för VTI och SIKA. N.
50. Mångfald är framtiden. Ku.
51. Riksbankens finansiella oberoende. Fi.
52. Beslutanderätt vid gemensam vårdnad m.m. Ju.
53. Sjukhusens läkemedelsförsörjning. S.
54. Barnet i fokus En skärpt lagstiftning mot barnpornografi. Ju.
55. Betalningstider i näringslivet. N.
56. Revisionsutskott m.m.; Genomförande av 2006 års revisorsdirektiv. Ju.
57. Etiskt godkännande av djurförsök – nya former för överprövning. Jo.
58. Hamnstrategi – strategiska hamnnoder i det svenska godstransportsystemet. N.
59. Strategiska godsnoder i det svenska transportsystemet – ett framtidsperspektiv. N.
60. Sverige inför klimatförändringarna – hot och möjligheter. DVD medföljer. M.
61. Deluppföljning 2 av den kommunalekonomiska utjämningen – med förslag till förändringar i kostnadsutjämningen. Fi.
62. Utjämning av kommunernas LSS-kostnader – översyn och förslag. Fi.
63. En bättre viltförvaltning med inriktning på älg. Jo.
64. Studiestödsdatalag. U.
65. Domstolarnas handläggning av ärenden. Ju.
66. Rörelser i tiden. IJ.
67. Regeringsformen ur ett könsperspektiv. En övergripande genomgång. Ju.
68. Ett decennium med personval. Erfarenheter och utfall. Ju.
69. Bestämmelser om domstolarna i regeringsformen. Expertgruppsrapport. Ju.
70. Framtidens flygplatser – utveckling av det svenska flygplatssystemet. N.
71. En starkare företagsinteckning. Ju.
72. Kommunal kompetens i utveckling. Fi.
73. Kostnader för personlig assistans. Skärpta regler för utbetalning, användning och återbetalning av assistansersättning. S.
74. Upplåtelse av den egna bostaden. Fi.
75. Att styra staten – regeringens styrning av sin förvaltning. Fi.
76. Lagring av trafikuppgifter för brottsbekämpning. Ju.

Statens offentliga utredningar 2007

Systematisk förteckning

Riksbankens finansiella oberoende. [51]
Deluppföljning 2 av den kommunalekonomiska utjämningen – med förslag till förändringar i kostnadsutjämningen. [61]
Utjämning av kommunernas LSS-kostnader – översyn och förslag. [62]
Kommunal kompetens i utveckling. [72]
Upplåtelse av den egna bostaden. [74]
Att styra staten – regeringens styrning av sin förvaltning. [75]

Utbildningsdepartementet

Tydliga mål och kunskapskrav i grundskolan. Förslag till nytt mål- och uppföljningssystem. [28]
Två nya statliga specialskolor. + Lättläst+ Daisy. [30]
Studiestödsdatalag. [64]

Jordbruksdepartementet

Telefonförsäljning. [1]
Administrativa sanktioner på yrkesfiskets område. [20]
Veterinär fältverksamhet i nya former. [24]
Bioenergi från jordbruket – en växande resurs. + Bilagedel. [36]
Ansvarsfrågan vid odling av genmodifierade grödor. [46]
Etiskt godkännande av djurförsök – nya former för överprövning. [57]
En bättre viltförvaltning med inriktning på älg. [63]

Miljödepartementet

Den nya inskrivningsmyndigheten. [7]
Renovering av bostadsmarknad efterlyses!
Om ungas möjligheter till en egen bostad.
Rapport nr 1:
Om bara någon kunde säga vad jag ska göra för att få en bostad så skulle jag göra det.
Rapport nr 2:
Måste man ha tur?
Studier av yngre på bostadsmarknaden i svenska städer.
Rapport nr 3:
Effektiv bostadsservice och förmedling av bostäder – ur ett dubbelt användarperspektiv.
Rapport nr 4:
Unga vuxna på bolånemarknaden. [14]
GMO-skador i naturen och Miljöbalkens försäkringar. [21]
Kunskapsläget på kärnavfallsområdet 2007. Nu levandes ansvar, framtida generationers frihet. [38]
Sverige inför klimatförändringarna – hot och möjligheter. DVD medföljer. [60]

Näringsdepartementet

Trafikinspektionen – en myndighet för säkerhet och skydd inom transportområdet. [4]
Arbetsmarknadsutbildning för bristyrken och insatser för arbetslösa ungdomar. [18]
Auktorisation av patentombud. [27]
Tillväxt genom turistnäringen. [32]
Släpvagnskörning med B-körkort – när kan de nya EU-reglerna börja tillämpas? [33]
Den osynliga infrastrukturen – om förbättrad samordning av offentlig IT-standardisering. [47]
Organisationsform för VTI och SIKA. [49]
Betalningstider i näringslivet. [55]
Hamnstrategi – strategiska hamnnoder i det svenska godstransportsystemet. [58]
Strategiska godsnoder i det svenska transportsystemet – ett framtidsperspektiv. [59]
Framtidens flygplatser – utveckling av det svenska flygplatssystemet. [70]

Integrations- och jämställdhetsdepartementet

Stöd för framtiden – om förutsättningar för jämställdhetsintegrering.
Idébok:
Jämställd medborgarservice. Goda råd om jämställdhetsintegreringen. En idébokför chefer och strateger.
Metodbok:
JämStöd Praktika. Metodbok för jämställdhetsintegrering. [15]
Rörelser i tiden. [66]

Kulturdepartementet

Mångfald är framtiden. [50]

Arbetsmarknadsdepartementet

Bättre arbetsmiljöregler II. Skyddsombud, beställaransvar, byggarbetsplatser m.m. [43]