Lagrådsremiss

Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG

Regeringen överlämnar denna remiss till Lagrådet.

Stockholm den 11 november 2010

Beatrice Ask

Ulf Wallentheim
(Justitiedepartementet)

Lagrådsremissens huvudsakliga innehåll

I lagrådsremissen lämnas förslag till genomförande av Europaparlamentets och rådets direktiv 2006/24/EG om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG. Direktivet syftar till att harmonisera medlemsstaternas regler om skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra trafik- och lokaliseringsuppgifter, samt uppgifter som behövs för att identifiera en abonnent eller användare för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal av allvarliga brott.

De uppgifter som ska lagras svarar – enkelt uttryckt – främst på frågorna om vem som kommunicerade med vem, när det skedde, var de som kommunicerade befann sig och vilken typ av kommunikation som användes. Uppgifterna får inte avslöja innehållet i en kommunikation.

I lagrådsremissen föreslås att det i lag förs in bestämmelser som bl.a. anger ändamålen med lagringsskyldigheten och vilka teknikområden som omfattas. Den närmare tekniska beskrivningen av vilka uppgifter som ska lagras bedöms lämpligast att ta in i förordning.

Förslaget innebär att de olika sätten att kommunicera är uppdelade på ett mer teknikneutralt sätt än i direktivet. Lagringstiden föreslås vara sex månader. Lagringsskyldigheten föreslås, utöver de uppgifter direktivet kräver, även gälla vid misslyckad uppringning och för uppgifter om lokalisering av mobil kommunikationsutrustning vid kommunikationens slut.

Förslaget innebär vidare att leverantörerna ska stå för kostnaderna för lagring, säkerhet och anpassning av systemen medan det allmänna ska

ersätta leverantörerna för de kostnader som avser utlämnande av uppgifter i enskilda ärenden.

Slutligen föreslås särskilda bestämmelser för att skapa ett tillfredsställande skydd för de uppgifter som lagras.

Lagändringarna föreslås träda i kraft den 1 juli 2011.

Innehållsförteckning

1 Beslut

Regeringen har beslutat att inhämta Lagrådets yttrande över förslag till

1. lag om ändring i rättegångsbalken,
2. lag om ändring i lagen (2003:389) om elektronisk kommunikation.

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om ändring i rättegångsbalken

Härigenom föreskrivs att 27 kap. 25 § rättegångsbalken ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
27 kap.	
25 §[1]	
Har rätten lämnat tillstånd till hemlig teleavlyssning eller hemlig teleövervakning, får de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen användas.	
I lagen (2003:389) om elektronisk kommunikation finns bestämmelser om hemlig teleavlyssning och hemlig teleövervakning som gäller för den som driver verksamhet som avses i *6 kap. 19 §* den lagen.	I *6 kap.* lagen (2003:389) om elektronisk kommunikation finns bestämmelser om hemlig teleavlyssning och hemlig teleövervakning som gäller för den som driver verksamhet som avses i den lagen.

[1] Senaste lydelse 2003:391

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

Härigenom föreskrivs[2] i fråga om lagen (2003:389) om elektronisk kommunikation

dels att 6 kap. 1 och 5 §§ samt rubriken till 6 kap. ska ha följande lydelse,

dels att det i lagen ska införas sju nya paragrafer, 6 kap. 3 a § och 16 a–16 f §§, samt närmast före 6 kap. 16 a § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
6 kap. Integritetsskydd	**6 kap.** ***Behandling av trafikuppgifter samt*** **integritetsskydd**
	1 §
I detta kapitel avses med	
elektroniskt meddelande: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst, utom information som överförs som del av sändningar av ljudradio- och TV-program som är riktade till allmänheten via ett elektroniskt kommunikationsnät om denna information inte kan sättas i samband med den enskilde abonnenten eller användaren av informationen,	
	Internetåtkomst: möjlighet till överföring av ip-paket som ger användaren tillgång till Internet,
	meddelandehantering: utbyte eller överföring av elektroniskt meddelande som inte är samtal och inte heller är information som överförs som del av sändningar av ljudradio- och TV-program,
	misslyckad uppringning: uppringning som kopplas fram utan att nå en mottagare,
	telefoni: elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan,
trafikuppgift: uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande.	

[2] Jfr 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).

Begreppen *behandling*, *personuppgiftsansvarig* och *samtycke* har i kapitlet samma innebörd som i personuppgiftslagen (1998:204).

3 a §

Den som är skyldig att lagra uppgifter enligt 16 a § ska vidta särskilda tekniska och organisatoriska åtgärder för att skydda de lagrade uppgifterna vid behandling.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om säkerhetsåtgärder enligt första stycket.

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*,* 13*, 16 a eller 16 c* §.

Lagring och annan behandling av trafikuppgifter m.m. för brottsbekämpande syften

16 a §

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

Skyldigheten att lagra uppgifter enligt första stycket omfattar uppgifter som genereras eller behandlas vid telefoni, meddelandehantering, Internetåtkomst och tillhandahållande av kapacitet för att få Internetåtkomst (anslutningsform). Även vid misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas.

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

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om vilka uppgifter som ska lagras enligt denna paragraf.

16 b §

Tillsynsmyndigheten får i enskilda fall besluta om undantag från skyldigheten att lagra uppgifter enligt 16 a §, om det finns synnerliga skäl. Beslutet får förenas med villkor.

Beslutet om undantag får återkallas om villkoren i beslutet inte har följts eller det finns andra särskilda skäl.

16 c §

Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2 eller 3 eller enligt 27 kap. 19 § rättegångsbalken.

16 d §

Lagring enligt 16 a § ska pågå under sex månader från den dag kommunikationen avslutades. Därefter ska den som är skyldig att lagra uppgifterna utplåna dem.

Om uppgifterna har begärts utlämnade inom den i första stycket angivna tidsfristen, men ännu inte har lämnats ut, ska uppgifterna lagras till dess att ett utlämnande har skett. Därefter ska uppgifterna utplånas av den som är skyldig att lagra dem.

16 e §

Den som är skyldig att lagra uppgifter enligt 16 a § har rätt till ersättning när lagrade uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om ersättningen som avses i första stycket.

16 f §

Den som är skyldig att lagra uppgifter enligt 16 a § ska bedriva verksamheten så att uppgifterna kan lämnas ut utan dröjsmål och informationen enkelt kan tas om hand samt så att verkställandet inte röjs.

Denna lag träder i kraft den 1 juli 2011.

3 Ärendet och dess beredning

Efter bombattentaten i Madrid den 11 mars 2004 fick rådet för rättsliga och inrikes frågor (RIF) i uppdrag av Europeiska rådet att snarast anta gemensamma åtgärder i fråga om lagring av trafikuppgifter. Ett antal länder, däribland Sverige, utarbetade förslag som presenterades under sommaren 2004.

Europaparlamentet och rådet antog den 15 mars 2006 direktivet 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. Fortsättningsvis benämns detta som direktivet eller direktivet om lagring av trafikuppgifter. Det finns intaget som *bilaga 1*.

Direktivet syftar till att harmonisera medlemsstaternas regler om skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att lagra vissa uppgifter som genereras eller behandlas i samband med att en kommunikation sker med fast eller mobil telefoni, eller i viss omfattning på Internet. Uppgifter definieras i direktivet som trafik- och lokaliseringsuppgifter samt de uppgifter som behövs för att identifiera en abonnent eller användare.

Enligt direktivet skulle medlemsstaterna senast den 15 september 2007 ha genomfört bestämmelserna i nationell rätt. När det gäller Internetåtkomst, Internetbaserad e-post och Internettelefoni fanns en möjlighet att skjuta upp genomförandet av direktivet till och med den 15 mars 2009. Den möjligheten har Sverige utnyttjat.

Regeringen beslutade i maj 2006 att ge en särskild utredare i uppdrag att lämna förslag till hur direktivet om lagring av trafikuppgifter ska genomföras i svensk rätt. Utredningen tog namnet Trafikuppgiftsutredningen. Utredaren överlämnade i november 2007 betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76). En sammanfattning av betänkandet finns i *bilaga 2*. Lagförslaget finns i *bilaga 3*. Betänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. En sammanställning av remissyttrandena finns tillgänglig i Justitiedepartementet (dnr Ju2007/9590/BIRS).

4 Direktivet om lagring av trafikuppgifter

4.1 Syfte och tillämpningsområde

I enlighet med artikel 1.1 i direktivet om lagring av trafikuppgifter är syftet med direktivet att harmonisera medlemsstaternas bestämmelser om skyldighet att lagra vissa uppgifter för att på så sätt säkerställa att uppgifterna är tillgängliga för avslöjande, utredning och åtal av allvarliga brott. I direktivet definieras uppgifter som trafik- och lokaliseringsuppgifter samt de uppgifter som behövs för att identifiera en abonnent

eller användare (artikel 2.2a). I det följande används begreppet *trafikuppgifter* för alla dessa uppgifter.

Direktivets syfte utvecklas i skäl 7–11 i ingressen till direktivet. Av skälen framgår i huvudsak att uppgifter om användningen av elektronisk kommunikation är värdefulla för att avslöja, utreda och åtala brott. Lagring av trafikuppgifter för viss typ av kommunikation har i många medlemsstater visat sig vara ett nödvändigt och effektivt redskap för de brottsbekämpande myndigheterna, framför allt när det gäller utredningar av allvarliga brott som organiserad brottslighet och terrorism. Både praktisk erfarenhet och forskning har visat på vikten av trafikuppgifter för att avslöja, utreda och åtala brott. Europeiska rådet har därför gett rådet i uppdrag att försöka anta gemensamma regler för att tillse att trafikuppgifter lagras under viss tid.

Av skäl 5 i ingressen framgår vidare att flera medlemsstater har antagit lagstiftning om skyldighet för tjänsteleverantörer att lagra trafikuppgifter. Lagstiftningen skiljer sig dock åt mellan medlemsstaterna. Skillnader i rättsliga och tekniska bestämmelser om lagring av trafikuppgifter utgör enligt skäl 6 hinder för den inre marknaden för elektronisk kommunikation. Tjänsteleverantörerna ställs inför olika krav när det gäller vilken typ av uppgifter som ska lagras och vilka villkor som gäller för lagringen. Målet med direktivet är följaktligen att harmonisera leverantörernas skyldighet att lagra uppgifter och säkerställa att de är tillgängliga för avslöjande, utredning och åtal av brott (skäl 21). Av skäl 23 framgår att direktivet inte syftar till att harmonisera tekniken för lagring av uppgifter. Det är enligt direktivet en fråga som måste lösas på nationell nivå.

Direktivet gäller, enligt artikel 1.2, trafikuppgifter om såväl fysiska som juridiska personer samt uppgifter som är nödvändiga för att kunna identifiera abonnenten eller den registrerade användaren. Däremot är direktivet inte tillämpligt på innehållet i kommunikationen.

4.2 Skyldigheten att lagra trafikuppgifter

4.2.1 Lagringsskyldighetens omfattning

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

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

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

En medlemsstat som står inför särskilda omständigheter kan enligt artikel 12 få möjlighet att förlänga den högst tillåtna lagringstiden. Kommissionen och övriga medlemsstater ska då underrättas om vidtagna åtgärder och skälen till dessa. Kommissionen har sex månader på sig att avgöra om åtgärderna ska förkastas eller kan godkännas.

4.2.2 Uppgifter som ska lagras

I artikel 2.2 i direktivet definieras vissa för direktivet viktiga begrepp. Med telefonitjänst avses uppringning (inbegripet rösttelefoni, röstmeddelanden, konferenssamtal och datatelefoni), extratjänster (inbegripet omstyrning och överflyttning av samtal) och meddelandeförmedling och multimedietjänster (inbegripet sms, ems och multimedietjänster).

Med användare 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.

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

Uppgifter som är nödvändiga för att *spåra och identifiera en kommunikationskälla* (punkten 1a), omfattar beträffande fast och mobil telefoni, det uppringande telefonnumret och abonnentens eller den registrerade användarens namn och adress. När det gäller Internetåtkomst, Internetbaserad e-post och Internettelefoni omfattas uppgift om tilldelat användar-id (som är ett unikt id som tilldelas den som abonnerar på eller registrerar sig på en Internetåtkomsttjänst eller en Internetkommunikationstjänst, artikel 2.2d). Användar-id och telefonnummer som tilldelats kommunikationen i det allmänna telenätet liksom namn på och adress till den abonnent eller registrerade användare som ip-adressen, användar-id eller telefonnumret tilldelades vid tidpunkten för kommunikationen omfattas också av lagringsskyldigheten.

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

adress till abonnenten eller den registrerade användaren och det användar-id som tilldelats den avsedda mottagaren av kommunikationen.

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

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

För att *identifiera användarnas kommunikationsutrustning* (punkten 1e) finns krav på lagring av det uppringande och det uppringda telefonnumret vid fast och mobil telefoni. När det gäller mobiltelefoni ska lagringen därutöver omfatta den uppringande respektive den uppringda partens IMSI (International Mobile Subscriber Identity) och IMEI (International Mobile Equipment Identity) samt, vid förbetalda anonyma tjänster, datum och tid för den första aktiveringen av tjänsten och den lokaliseringsbeteckning (cell-id) från vilken tjänsten aktiverades. Lokaliseringsbeteckning (cell-id) är identiteten hos den cell från vilken ett mobiltelefonsamtal påbörjades eller avslutades (artikel 2.2e). När det gäller Internetåtkomst, Internetbaserad e-post och Internettelefoni gäller lagringen uppringande telefonnummer och DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationens avsändare.

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

4.3 Hanteringen av lagrade trafikuppgifter

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

Medlemsstaterna ska säkerställa att de lagrade trafikuppgifterna, och annan relevant information, på begäran kan överföras till behöriga myndigheter utan dröjsmål (artikel 8).

Som ett minimum för datasäkerhet ska medlemsstaterna säkerställa att leverantörerna respekterar vissa i artikel 7 angivna principer när det gäller lagrade trafikuppgifter. De lagrade uppgifterna ska vara av samma kvalitet och vara föremål för samma säkerhet och skydd som uppgifterna

i nätverket. Lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda uppgifterna mot oavsiktlig eller olaglig förstöring, oavsiktlig förlust, oavsiktlig ändring eller otillåten eller olaglig lagring av, behandling av, tillgång till eller avslöjande av uppgifterna. Lämpliga tekniska och organisatoriska åtgärder ska vidare vidtas för att säkerställa att tillgång till uppgifterna endast ges särskilt bemyndigad personal. Uppgifterna ska vidare förstöras vid slutet av lagringstiden, utom uppgifter för vilka tillgång medgivits och som har bevarats.

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

I skäl 16 i ingressen erinras om tjänsteleverantörernas skyldigheter att vid behandlingen garantera uppgifternas kvalitet, sekretess och säkerhet i enlighet med 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. Enligt artikel 13 i direktivet om lagring av trafikuppgifter ska medlemsstaterna också se till att de nationella åtgärder som genomför bestämmelserna om rättslig prövning, ansvar och sanktioner i det förstnämnda direktivet blir tillämpliga även på de uppgifter som avses i nu aktuellt direktiv. Den rätt till ersättning som enligt direktiv 95/46/EG om behandling av personuppgifter tillkommer varje person som lidit skada till följd av otillåten behandling eller någon annan handling som är oförenlig med de nationella bestämmelser som genomför direktivet ska enligt skäl 19 i direktivet om lagring av trafikuppgifter gälla även för personuppgifter enligt det sist nämnda direktivet.

Medlemsstaterna åläggs vidare att införa sanktioner för att beivra otillåten avsiktlig tillgång till eller överföring av lagrade trafikuppgifter (artikel 13). Europarådskonventionen om IT-brottslighet från 2001 liksom Europarådskonventionen om skydd för enskilda vid automatisk databehandling av personuppgifter från 1981 ska också omfatta uppgifter som lagras i enlighet med direktivet om lagring av trafikuppgifter (skäl 20).

4.4 Utvärdering och genomförande av direktivet

Medlemsstaterna ska varje år, i enlighet med artikel 10, förse kommissionen med statistik över lagringen av trafikuppgifter. Redovisningen ska avse de fall information skickats till behöriga myndigheter, den tid som gått från att uppgifterna lagrades till att uppgifterna begärdes ut av den behöriga myndigheten samt de fall en begäran om uppgifter inte kunde tillgodoses. Statistiken ska dock inte omfatta personuppgifter.

Med statistiken som underlag skulle kommissionen enligt artikel 14 senast den 15 september 2010 till Europaparlamentet och rådet ha översänt en utvärdering av tillämpningen av direktivet och dess inverkan på de ekonomiska aktörerna och konsumenterna. Utvärderingen har dock försenats och är ännu inte färdigställd. I utvärderingen ska kommissionen beakta den fortsatta utvecklingen av tekniken för elektronisk kommunikation. Även synpunkter från den arbetsgrupp som inrättats genom artikel 29 i direktiv 95/46/EG om behandling av personuppgifter

ska beaktas. Syftet med utvärderingen är att avgöra om det är nödvändigt att ändra direktivets bestämmelser, särskilt när det gäller listan över uppgifter i artikel 5 och de lagringstider som direktivet föreskriver.

Med anledning av att den teknik som används för elektronisk kommunikation utvecklas snabbt har kommissionen, i enlighet med skäl 14, inrättat en grupp av experter för att få råd och uppmuntra utbyte av erfarenheter om bästa metoder i dessa frågor. Gruppen består av medlemsstaternas brottsbekämpande myndigheter, sammanslutningar inom den elektroniska kommunikationsindustrin, företrädare för Europaparlamentet samt dataskyddsmyndigheter, däribland Europeiska datatillsynsmannen.

Enligt artikel 15 ska medlemsstaterna genomföra direktivet i nationell lagstiftning senast den 15 september 2007. I fråga om lagring av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post får medlemsstaterna dock genom en förklaring till rådet och kommissionen vid antagande av direktivet skjuta upp genomförandet till den 15 mars 2009. Medlemsstaterna ska till kommissionen överlämna texterna till nationella bestämmelser som de antar inom det område som omfattas av direktivet.

5 Utgångspunkter för genomförandet

Ett genomförande av direktivet om lagring av trafikuppgifter innebär att olika intressen ställs mot varandra; de brottsbekämpande myndigheternas behov av effektiva verktyg för att kunna avslöja, utreda och lagföra brott ställs mot intresset av att skydda enskildas integritet. Direktivet har i sin utformning tagit hänsyn till och gjort en avvägning mellan dessa intressen, men även genomförandet av direktivet föranleder att dessa aspekter beaktas. Detsamma gäller den inverkan direktivet har på möjligheterna att konkurrera på lika villkor.

5.1 Brottsbekämpningens behov av och tillgång till trafikuppgifter och skyddet av enskildas integritet

Regeringens bedömning: Vid genomförande av direktivet om lagring av trafikuppgifter bör brottsbekämpningens behov av trafikuppgifter tillgodoses samtidigt som enskildas integritet värnas.

Utredningens bedömning överensstämmer i sak med regeringens.

Remissinstanserna: Ingen remissinstans har ifrågasatt att tillgången till trafikuppgifter är av stor vikt för brottsbekämpningen samtidigt som en lagring av trafikuppgifter innebär ett intrång i den personliga integriteten. *Svea hovrätt, Åklagarmyndigheten* och *Ekobrottsmyndigheten* har anfört att tillgången till trafikuppgifter många gånger är av avgörande betydelse för brottsbekämpningen, särskilt vad gäller allvarlig brottslighet. *Riksdagens ombudsmän (JO), Krisberedskapsmyndigheten, Data-*

inspektionen och *Amnesty International* har betonat vikten av att så långt det är möjligt begränsa de integritetsförluster lagringskravet för med sig, samtidigt som det konstateras att avvägningen mellan brottsbekämpning och integritetsskydd i allt väsentligt är given i direktivet. *Tullverket, IFPI Svenska Gruppen* och *Svenska Antipiratbyrån* har anfört att de anser att utredningen på ett tillfredsställande sätt har belyst avvägningen mellan behovet av tillgång till trafikuppgifter och skyddet för den personliga integriteten. *Stockholms handelskammare, Sveriges advokatsamfund, Juridiska fakultetsnämnden vid Lunds universitet, Svenska journalistförbundet, Konstnärliga och Litterära Yrkesutövares Samarbetsnämnd (KLYS)* och *Stiftelsen för Internetinfrastruktur (.SE)* har däremot framfört att de anser att utredningen i för stor omfattning betonat brottsbekämpningsintresset på bekostnad av integritetsskyddet. *Bahnhof AB* har, främst mot bakgrund av integritetsaspekten, avstyrkt att direktivet över huvud taget genomförs.

Ett antal remissinstanser har ifrågasatt utredningens bedömning att genomförandet av direktivet inte ger skäl att ändra reglerna om de brottsbekämpande myndigheternas tillgång till trafikuppgifter. JO har avstyrkt att utredningens förslag genomförs utan att man samtidigt genomför de förändringar av reglerna om utlämnande av trafikuppgifter som Beredningen för rättsväsendets utveckling (BRU) har föreslagit (SOU 2005:38). Även *Justitiekanslern (JK)* och Sveriges advokatsamfund har förespråkat en sådan samordning. *Svea hovrätt, Domstolsverket* och KLYS har ansett att det skulle vara en fördel för integritetsskyddet om det alltid var domstol som prövade frågan om utlämnande av trafikuppgifter, men har konstaterat att frågan inte ingått i utredningens uppdrag. Även Datainspektionen och *Säkerhets- och integritetsskyddsnämnden* har förespråkat en oberoende rättslig kontroll med hänvisning till integritetsskyddet. Svenska journalistförbundet har ifrågasatt om utlämnande av uppgifter enligt lagen om elektronisk kommunikation är förenligt med det proportionalitetskrav Europakonventionen om mänskliga rättigheter uppställer beträffande integritetsintrång.

Skälen för regeringens bedömning

Balansen mellan brottsbekämpningens behov och integritetsskyddet

De brottsbekämpande myndigheterna använder sig i stor utsträckning av trafikuppgifter för att avslöja, utreda och lagföra brott. I direktivet om lagring av trafikuppgifter framhålls också att trafikuppgifter är ett nödvändigt och effektivt redskap för de brottsbekämpande myndigheterna.

I betänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38), redogörs ingående för i vilken omfattning trafikuppgifter används (s. 322–325). Av denna redogörelse kan följande framhållas. Uppgifterna inhämtas i stort sett i varje utredning om allvarlig brottslighet som mord, våldtäkt, grovt narkotikabrott eller terroristbrott. I ett inledande skede av utredningen inhämtas trafikuppgifter som genererats i anslutning till en brottsplats. Uppgifterna tillsammans med annan information gör det möjligt för polisen att ”lägga pussel” och på så sätt ringa in misstänkta personer. Genom trafikuppgifter, t.ex. från

mobiltelefoner, kan polisen kartlägga hur ett brott planerats och genomförts, men även hur de misstänkta agerat efter att de genomfört ett brott, t.ex. vilka flyktvägar som använts. Uppgifterna kan också många gånger resultera i att personer helt avförs från en utredning. Beträffande Internetrelaterad brottslighet är utgångsläget ofta att ingen misstänkt person finns och att tillgången till trafikuppgifter är det enda sätt polisen kan komma en misstänkt på spåren. Sammanfattningsvis anges i betänkandet att tillgången till trafikuppgifter är av helt avgörande betydelse för att utreda viss typ av brottslighet. I Trafikuppgiftsutredningens betänkande har myndigheterna också lämnat exempel på konkreta fall där trafikuppgifter varit av stort värde för utredningen; t.ex. i utredningar om allvarliga vålds-, sexual- och tillgreppsbrott (SOU 2007:76 s. 133 f.).

Regeringen kan med hänsyn till vad som redovisats ovan konstatera att de brottsbekämpande myndigheterna har ett stort behov av att få tillgång till trafikuppgifter i sin verksamhet. Denna omständighet har inte heller någon av remissinstanserna ifrågasatt.

Möjligheterna för brottsbekämpande myndigheter att få tillgång till trafikuppgifter är beroende av vilka uppgifter som leverantörerna har lagrat för andra syften. Uppgifter kan sparas enligt lagen (2003:389) om elektronisk kommunikation t.ex. för abonnentfakturering, för betalning av avgifter för samtrafik och – om den som uppgifterna gäller har samtyckt till det – för marknadsföring. De kan också sparas för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Vilka uppgifter som lagras och den tid de lagras styrs alltså av helt andra faktorer än de brottsbekämpande myndigheternas behov. Utvecklingen inom området elektronisk kommunikation kan också förväntas leda till att nät- och tjänsteleverantörer i framtiden inte behöver lagra uppgifter för sin egen verksamhet i lika stor utsträckning som tidigare. Det medför att möjligheterna för brottsbekämpande myndigheter att få tillgång till dessa uppgifter kan komma att minska. Genom att införa en skyldighet att lagra vissa trafikuppgifter säkerställer direktivet om lagring av trafikuppgifter att trafikuppgifter finns tillgängliga för att användas i brottsutredningar.

Samtidigt som det således kan konstateras att tillgången till trafikuppgifter är av stor betydelse för att myndigheterna ska kunna utföra en effektiv brottsbekämpning medför lagringen av trafikuppgifter ett intrång i enskildas personliga integritet. Trafikuppgifter är i många fall uppgifter om enskildas personliga förhållanden och korrespondens. Den absoluta merparten av de uppgifter som nu föreslås ska lagras kommer naturligtvis aldrig att begäras utlämnade för brottsutredningar, utan kommer att utplånas efter lagringstidens slut utan att någon har tagit del av dem. Detta skiljer sig inte från vad som i dag gäller i fråga om de trafikuppgifter som nät- och tjänsteleverantörerna lagrar för egna syften och som är tillgängliga för de brottsbekämpande myndigheterna. Regeringen delar emellertid, i likhet med ett stort antal remissinstanser, utredningens bedömning att ett integritetsintrång sker genom att uppgifterna lagras, då detta bidrar till enskildas upplevelse av att få sin privata sfär och frihet att kommunicera inskränkt. Lagringen skulle kunna leda till att enskilda i viss utsträckning avstår från att använda elektroniska kommunikationsmedel i syfte att undvika att uppgifter registreras.

Den bestämmelse i regeringsformen som främst har betydelse för skyddet av den personliga integriteten är skyddet mot påtvingat kroppsligt ingrepp, kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev och förtrolig försändelse och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande (2 kap. 6 §). Enligt bestämmelsen är det förtroligheten i meddelanden av olika slag som skyddas i grundlagen (prop. 1973:90 s. 243 och 1975/76:209 s. 147 f.). Den i lagrådsremissen föreslagna lagringen av trafikuppgifter omfattar dock inte innehållet i befordrade meddelanden, vilket innebär att lagringen inte omfattas av nuvarande bestämmelser i regeringsformen.

I propositionen En reformerad grundlag (2009/10:80) har regeringen föreslagit att grundlagsskyddet för den personliga integriteten ska stärkas. I propositionen föreslås bl.a. att en ny bestämmelse införs som anger att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden (2 kap. 6 § andra stycket regeringsformen). Inskränkningar genom lag föreslås dock vara tillåtna enligt de förutsättningar som anges i nuvarande 2 kap. 12 § regeringsformen. Det innebär bl.a. att en begränsning av den utvidgade rätten till skydd för den personliga integriteten kommer att vara tillåten endast under förutsättning att den tillgodoser ett ändamål som är godtagbart i ett demokratiskt samhälle. Det innebär också att en begränsning inte får gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den eller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen. Förslagen har, med några mindre justeringar, antagits av riksdagen som vilande i juni 2010 (bet. 2009/10:KU19, prot. 2009/10:130). Riksdagen kan förväntas pröva förslagen en andra gång under hösten 2010. Lagändringarna föreslås träda i kraft den 1 januari 2011.

Grundlagsskyddet för den personliga integriteten kompletteras till viss del av det skydd som följer av artikel 8 i den europeiska konventionen av den 4 november 1950 angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen). Konventionen gäller sedan 1995 som svensk lag. Enligt artikel 8 har var och en rätt till respekt för sitt privat- och familjeliv, hem och korrespondens. Åtnjutandet av rätten till respekt för privat- och familjelivet får inskränkas endast med stöd av lag i den utsträckning det i ett demokratiskt samhälle är nödvändigt med hänsyn till vissa närmare angivna ändamål, bl.a. bekämpning av brott. Av Europadomstolens praxis följer att det krävs att det finns ett angeläget samhälleligt behov (”pressing social need”) för att en inskränkning ska vara tillåten. Inskränkningen måste vidare framstå som proportionell i förhållande till det syfte som den avser att tillgodose. Enligt 2 kap. 23 § regeringsformen får lag eller annan föreskrift inte meddelas i strid med Sveriges åtaganden enligt Europakonventionen.

Som ovan redovisats har ett stort antal remissinstanser framhållit vikten av integritetsskyddet. Någon remissinstans har också, med hänvisning till integritetsaspekter, avstyrkt att direktivet genomförs. Vissa anser att utredningen har hittat en bra balans mellan brottsbekämpningsintresset och integritetsskyddet, medan andra anser att brottsbekämpningsintresset fått för stort utrymme på integritetsskyddets bekostnad.

Inledningsvis kan påpekas att det redan i direktivet, som ett antal remissinstanser också anför, görs en avvägning mellan de intressen som nu är aktuella. 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 avslöjas, utreds och lagförs respektive skyddet för enskildas integritet. 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. Sverige är som medlemsstat i Europeiska unionen skyldigt att genomföra direktivet.

Sveriges skyldighet att genomföra direktivet hindrar emellertid inte att integritetsfrågorna vid genomförandet kan beaktas på olika sätt, vilket direktivet också utgår ifrån. En utgångspunkt bör då vara att vid regleringen av lagringen skapa ett transparent system som gör det möjligt för medborgarna att förutse vilka uppgifter som kommer att lagras och hur de typiskt sett används i brottsbekämpningen. I detta ligger att lagring ska medges endast om det följer av direktivet eller kan motiveras med stöd av artikel 15.1 i direktivet 2002/58/EG om integritet och elektronisk kommunikation. I syfte att öka rättssäkerheten och skyddet för den personliga integriteten väljer regeringen också att, i större utsträckning än Trafikuppgiftsutredningen, föreslå att den nya regleringen sker genom ändring i lag. Härigenom ökar riksdagens kontroll (se avsnitt 6).

Integritetsfrågorna ska vidare beaktas vid bedömningen av var lagringen ska ske, av vem uppgifterna ska lagras, hur länge de ska få lagras innan de ska utplånas samt vilka andra villkor som ska gälla för lagringen (se avsnitt 6 och 7). För att minimera risken för otillbörliga integritetsintrång mot den enskilde, och för att skapa tillit till systemet, måste vidare såväl det tekniska som det organisatoriska skyddet för de lagrade uppgifterna vara tillräckligt. De rättsliga regler som blir tillämpliga om trafikuppgifter ändå skulle komma att spridas i strid mot lagen måste också verka tillräckligt avhållande och vara reparativa. En säker lagring fordrar vidare en aktiv tillsynsverksamhet (se avsnitt 8).

Sammanfattningsvis är såväl en effektiv brottbekämpning som skyddet för enskildas personliga integritet frågor av stor betydelse. Vid genomförande av direktivet ska därför såväl brottsbekämpningens behov av effektiva verktyg som behovet av att skydda enskildas integritet beaktas. Utformningen av lagringskravet ska skapa en balans mellan dessa båda intressen.

Tillgången till trafikuppgifter

Möjligheten att bedriva en effektiv brottsbekämpning med hjälp av trafikuppgifter samt vilka avgränsningar som krävs med hänsyn till integritetsskyddet avgörs till betydande del av de bestämmelser som reglerar under vilka förutsättningar de brottsbekämpande myndigheterna ska ha tillgång till uppgifterna.

Direktivet ålägger medlemsstaterna att lagra vissa trafikuppgifter så att de finns tillgängliga för att kunna lämnas ut och användas för avslöjande, utredning och åtal avseende allvarlig brottslighet. I direktivet regleras inte närmare under vilka förutsättningar de brottsbekämpande myndighe-

terna ska ha möjlighet att få ta del av trafikuppgifterna eller hur förfarandet för utlämnandet ska gå till. I skäl 25 i direktivet anges att när det gäller tillgång till trafikuppgifter ska de nationella reglerna respektera de grundläggande rättigheterna i Europakonventionen. Vidare ska medlemsstaterna, enligt ett uttalande från rådet, vid bedömningen av om de nationella brott som möjliggör utlämnande av trafikuppgifter är tillräckligt allvarliga 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), se *bilaga 5,* och till brott där telekommunikation ingår. I övrigt är det upp till varje medlemsstat att i sin nationella lagstiftning ställa upp de villkor som gäller för att få tillgång till trafikuppgifterna.

Enligt gällande regler kan de brottsbekämpande myndigheterna få tillgång till trafik- och abonnemangsuppgifter antingen efter ett beslut enligt rättegångsbalken om hemlig teleövervakning eller enligt lagen om elektronisk kommunikation. För att hemlig teleövervakning ska få användas ska det brott förundersökningen avser, med några undantag, ha ett minimistraff på sex månaders fängelse (27 kap. 19 § rättegångsbalken). Om trafikuppgifter ska lämnas ut med stöd av lagen om elektronisk kommunikation krävs att uppgifterna gäller misstankar om brott med minst två års fängelse som straffminimum (6 kap. 22 § första stycket 3). För abonnemangsuppgifter gäller att sådana uppgifter kan lämnas ut beträffande misstanke om brott där fängelse är föreskrivet för brottet och gärningen i det enskilda fallet kan föranleda annan påföljd än böter (6 kap. 22 § första stycket 2). För en närmare redogörelse för dessa regler hänvisas till betänkandet (se s. 56–71).

Som ett antal remissinstanser (*JO, JK, Svea Hovrätt, Domstolsverket, Datainspektionen, Säkerhets- och integritetsskyddsnämnden* och *Sveriges advokatsamfund)* har påpekat bör frågan om de brottsbekämpande myndigheternas tillgång till trafikuppgifter ses över. I maj 2005 överlämnade Beredningen för rättsväsendets utveckling (BRU) sitt delbetänkande Tillgång till elektronisk kommunikation (SOU 2005:38). I betänkandet föreslås bl.a. att de brottsbekämpande myndigheternas tillgång till uppgifter som angår särskilda elektroniska meddelanden uteslutande ska regleras i 27 kap. rättegångsbalken och att bestämmelserna om detta i lagen om elektronisk kommunikation upphävs.

I december 2007 beslutade regeringen att komplettera underlaget i vissa delar och tillsatte en särskild utredare för att överväga bl.a. vissa frågor om inhämtning av uppgifter om elektronisk kommunikation inom polisens underrättelseverksamhet och under förundersökning innan det finns någon skäligen misstänkt gärningsman. Utredningen, som antog namnet Polismetodutredningen, har redovisat sina överväganden i nu nämnda delar i delbetänkandet En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen (SOU 2009:1). Även i det betänkandet föreslås att de aktuella bestämmelserna i lagen om elektronisk kommunikation ska upphävas och att inhämtande av uppgifter som angår särskilda elektroniska meddelanden i förundersökningar enbart ska kunna ske enligt reglerna om hemlig teleövervakning. Hemlig teleövervakning föreslås kunna användas även när det saknas en skäligen misstänkt person. I underrättelseverksamhet ska uppgifter kunna inhämtas med stöd av en ny lag. Uppgifterna föreslås få inhämtas avseende brott

av i stort sett samma svårighetsgrad som i dag. Säkerhets- och integritetsskyddsnämndens tillsyn föreslås omfatta användningen av de nya befogenheterna att inhämta uppgifter om viss elektronisk kommunikation i underrättelseverksamhet. Polismetodutredningens delbetänkande avses inom kort att behandlas i en lagrådsremiss om de brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation.

5.2 Konkurrensaspekter

Regeringens bedömning: Vid genomförandet av direktivet bör hänsyn tas till den inverkan på konkurrensen som lagringsskyldigheten kan medföra.

Utredningens bedömning överensstämmer i huvudsak med regeringens.

Remissinstanserna: De flesta remissinstanser har inte framfört några invändningar mot utredningens bedömning. Flera remissinstanser har dock pekat på att lagringsskyldigheten som införs kommer att ha en negativ inverkan på konkurrensen. *IT&Telekomföretagen* och *Post- och telestyrelsen (PTS)* har bl.a. framfört att konkurrensen kan snedvridas beroende på om leverantörerna har nya eller äldre system som måste anpassas och om det rör stora eller små leverantörer. .*SE* har angett att lagringsskyldigheten medför en tröskel för nyetablering. *Banverket* har ansett att en decentraliserad lagring snedvrider konkurrensen.

Skälen för regeringens bedömning: Genomförandet av direktivet om lagring av trafikuppgifter kommer att få konsekvenser för leverantörerna, bl.a. beträffande deras möjligheter att konkurrera med de tjänster som de tillhandahåller. Skyldigheten att lagra uppgifter kan exempelvis komma att medföra vissa tröskeleffekter vid nyetablering av aktuella tjänster. Lagringsskyldigheten kan också förväntas få olika konsekvenser beroende på om den leverantör som blir skyldig att lagra trafikuppgifter ska anpassa ett nyare eller äldre system eller om det rör sig om ett litet eller stort företag. Därigenom kan konkurrensen påverkas. En annan aspekt som kan påverka möjligheten att konkurrera är vilken typ av tjänst som kommer att omfattas av lagringsskyldigheten. I detta kan regeringen i och för sig dela remissinstansernas synpunkter.

Många verksamheter som bedrivs i privat regi är emellertid förknippade med olika samhälleliga krav. Det kan röra sig om allmänna krav som att det aktuella företaget ska organisera verksamheten med utrustning och personal för att se till att skatter betalas in till staten. Företag som bedriver verksamhet som har påverkan på miljön ställs därutöver inför särskilda krav, som förnyas med tiden, och som påverkar den pågående verksamheten men också möjligheterna till nyetablering. Detsamma gäller företag som nu är aktuella, dvs. de som tillhandahåller allmänna kommunikationsnät eller elektroniska kommunikationstjänster. Det är således inget nytt att andra intressen än rent företagsekonomiska, t.ex. att få in skatteintäkter, mildra påverkan på miljön eller brottsbekämpningsintressen, måste beaktas även om detta påverkar de privata aktörernas verksamhet.

Regeringen vill vidare framhålla att direktivet om lagring av trafikuppgifter bl.a. syftar till att främja den inre marknaden och förbättra konkurrensmöjligheterna bland leverantörerna inom EU. I direktivet konstateras att de stora skillnaderna mellan medlemsstaterna vad gäller lagring av trafikuppgifter utgör ett hinder för den inre marknaden, varför ett direktiv med en minimiharmonisering av lagringsskyldigheten kommer att förbättra möjligheterna att konkurrera på lika villkor. I huvudsak kommer leverantörerna således att ställas inför samma krav inom EU, vilket enligt regeringens mening främjar konkurrensen.

Vad som anförts hindrar emellertid inte att man vid genomförandet av direktivet om lagring av trafikuppgifter tar hänsyn till de negativa konkurrensmässiga effekter ett genomförande kan tänkas ha, för att mildra dessa så långt som det är rimligt och möjligt. Ett förslag som har till syfte att mildra sådana effekter är den möjlighet som PTS ges att medge undantag från lagringsskyldigheten, helt eller delvis, 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 fullt ut fullgör lagringsskyldigheten (se avsnitt 7.2). Ett annat förslag som syftar till att mildra negativa konkurrensmässiga effekter är att de myndigheter som begär ut trafikuppgifter ska ersätta leverantörerna för de kostnader som uppstår (se avsnitt 9.2). Ett tredje förslag med samma syfte är att de som är skyldiga att lagra uppgifter ska få möjlighet att uppdra åt annan att utföra lagringen (se avsnitt 7.1). Regeringen återkommer till dessa frågor i respektive avsnitt.

6 Lagringsskyldighetens utformning

6.1 Uppgifter som genereras eller behandlas ska lagras

Regeringens förslag: Lagringsskyldigheten ska omfatta uppgifter som leverantören någon gång genererar eller behandlar. De uppgifter som ska lagras ska inte få avslöja kommunikationens innehåll.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: De flesta remissinstanserna har tillstyrkt utredningens förslag eller inte lämnat några synpunkter på förslaget. *Post- och telestyrelsen (PTS)* har påtalat att utredningens slutsats, att en lagringsskyldig leverantör enbart ska vara skyldig att lagra uppgifter som genereras av dennes tjänster, är mycket viktig och måste uttryckas med en tydligare formulering än i betänkandet. *Kungliga tekniska högskolan (KTH)* har också anfört att det vore lämpligt att förtydliga att uttrycket att ”behandla” uppgifter inte omfattar förmedling/överföring/transport av datatrafik som råkar innehålla sådana uppgifter som avses. *TeliaSonera AB* har efterlyst ett klargörande av att den vida tolkningen av formuleringen ”genererar eller behandlar” ska ses mot bakgrund av att den valts för att exkludera data som är av signaleringskaraktär och inte vidare behandlas eller registreras. *Swedish Network Users’ Society*

(*SNUS*) har anfört att ett förtydligande i lagtext eller författningskommentar behövs för att klargöra att operatörer, för att uppfylla sin lagringsskyldighet vid behandling av information, inte ska tvingas avkryptera eller tolka information som finns inuti ip-paket, dvs. information utöver sändar- och mottagaradresser. SNUS har vidare anfört att det måste tydliggöras huruvida lagringskravet ska omfatta inte bara nätleverantörer utan även andra aktörer som tillhandahåller e-posttjänster, Internettelefonitjänster och andra meddelandetjänster och som inte samtidigt levererar accessnät. *Juridiska fakultetsnämnden vid Stockholms universitet* har förespråkat ett förtydligande när det gäller vilka möjligheter leverantörer har att vid en senare tidpunkt självmant välja att upphöra att generera vissa uppgifter, på grund av att den egna verksamheten inte har något behov av dem, för att undvika att de underlåter att lagra viktiga uppgifter med hänvisning till att de inte längre behövs. *Stockholms handelskammare* har efterlyst en fördjupad analys av relationen mellan omständigheten att lagrade uppgifter inte får avslöja kommunikationens innehåll och det förhållandet att ip-adresser kan användas för att göra omfattande kartläggningar av en persons beteende.

Skälen för regeringens förslag: 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. Som utredningen konstaterat kommer leverantören alltså inte att ha skyldighet att ”skaffa sig” alla de uppgifter som nämns när lagringen regleras utan lagringsskyldigheten omfattar endast de trafikuppgifter som genereras eller behandlas i den egna verksamheten. Direktivet innebär därmed inget hinder mot användande av exempelvis anonyma kontantkort, där några uppgifter om användarens identitet inte finns tillgängliga för lagring. Genereras eller behandlas däremot uppgifterna någon gång hos leverantören, även om det bara rör sig om en ytterst kort tid, ska de lagras. I direktivet har denna förhållandevis vida förutsättning införts för att i möjligaste mån undvika att uppgifter inte lagras för att de inte varit föremål för en mer konkret hantering eller användning av leverantören. Med anledning av vad *Juridiska fakultetsnämnden vid Stockholms universitet* anfört får dock framhållas att direktivet inte kan tolkas på så sätt att en uppgift måste genereras eller behandlas även om den uppgiften inte behövs för att kunna tillhandahålla det nät eller den tjänst som kan vara aktuell. Direktivet innebär ingen ”genererings- eller behandlingsskyldighet”.

Som *PTS, KTH, TeliaSonera AB* och *SNUS* indirekt påtalat är avsikten att en nät- eller tjänsteleverantör endast ska lagra uppgifter som genereras eller behandlas i anslutning till det nät eller den tjänst som leverantören tillhandahåller. Det krävs inte att leverantören ska tillhandahålla såväl nät som en tjänst utan det räcker med endera.

SNUS har anfört att ett förtydligande i lagtext eller författningskommentar behövs för att klargöra att operatörer, för att uppfylla sin lagringsskyldighet vid behandling av information, inte ska tvingas avkryptera eller tolka information som finns inuti ip-paket, dvs. information om data som ska överföras utöver sändar- och mottagaradresser. Inga uppgifter som avslöjar kommunikationens innehåll får lagras enligt direktivet. Det framgår uttryckligen av artikel 5.2. Bestämmelsen tydliggör att direktivet inte syftar till att skapa förutsättningar för att ta del av

kommunikationen i sig. Utredningens förslag till lagring av trafikuppgifter utgår alltså från detta, vilket bör framgå av de nya bestämmelserna. Innehållet i ip-paketen, i den mån detta utgör innehållet i kommunikationen, omfattas således inte av lagringsskyldigheten. En lagringsskyldig leverantör är dock skyldig att lagra uppgifter om t.ex. avsändar- och mottagaradresser, eller andra uppgifter som omfattas av direktivet, i den mån de genereras av eller behandlas i de tjänster leverantören själv tillhandahåller, även om uppgifterna på grund av den teknik som används måste avkrypteras för att vid en eventuell förfrågan lämnas ut.

Stockholms handelskammare har efterlyst en fördjupad analys av relationen mellan omständigheten att lagrade uppgifter inte får avslöja kommunikationens innehåll och det förhållandet att ip-adresser kan användas för att avslöja en del om kommunikationens innehåll, vilket kan användas för att göra omfattande kartläggningar av en persons beteende. Det kan konstateras att inga uppgifter om kommunikationens innehåll får lagras enligt direktivets artikel 5.2. Av artikel 5.1 framgår dock att lagringsskyldigheten bl.a. omfattar uppgifter om vem som har haft en viss ip-adress, för att brottsutredande myndigheter ska kunna spåra och identifiera en kommunikationskälla. I detta sammanhang vill regeringen framhålla att privatpersoner normalt använder så kallade dynamiska ip-adresser, dvs. ip-adresser som byts slumpvis och oregelbundet. En användare har alltså i regel olika ip-adresser vid olika tillfällen. En uppgift om att en viss person hade en viss ip-adress vid ett visst tillfälle säger alltså i regel ingenting om vem som hade den adressen vid ett annat tillfälle. Av bl.a. den anledningen är det, rent tekniskt, inte möjligt att använda uppgifterna om ip-adressen för att t.ex. göra en mer allmän kartläggning av vad personen i fråga har gjort på Internet. Regeringens förslag innebär dessutom att möjligheterna att få ut uppgifter om ip-adresser begränsas så att endast brottsbekämpande myndigheter kan få tillgång till uppgifterna för att avslöja, utreda och åtala brott. Därutöver kan konstateras att direktivet inte omfattar uppgifter om besök på webbsidor (”surfning”) och att regeringens förslag inte går utöver direktivet på den punkten. Sammanfattningsvis omfattar lagringsskyldigheten alltså ip-adresser, men det är regeringens mening att det saknas förutsättningar för att göra allmänna kartläggningar av personers agerande på Internet enbart utifrån de ip-adresser som ska lagras med stöd av direktivet.

6.2 Lagringsskyldighetens struktur

Regeringens förslag: Lagringsskyldigheten ska struktureras i kategorierna telefoni, meddelandehantering, Internetåtkomst och anslutningsform. De uppgifter som lagras ska identifiera eller spåra kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typen av kommunikation, kommunikationsutrustning samt lokaliseringen av mobil kommunikationsutrustning vid kommunikationens början och slut. Denna utformning av lagringsskyldigheten ska regleras i lag.

Utredningens förslag överensstämmer delvis med regeringens. Utredningen har dock föreslagit att endast skyldigheten som sådan, att lagra trafikuppgifter för brottsbekämpande syften, ska lagregleras medan den närmare utformningen av lagringsskyldighetens omfattning ansetts kunna regleras i förordning.

Remissinstanserna: De flesta remissinstanserna har, när det gäller strukturen för lagringsskyldigheten, tillstyrkt utredningens förslag eller inte haft några invändningar mot förslaget. *IFPI Svenska Gruppen* och *Svenska Antipiratbyrån* har understrukit vikten av en teknikneutral reglering som tar höjd för den tekniska utvecklingen av fildelningsnätverk och så kallade anonymiseringstjänster.

När det gäller i vilken omfattning utformningen av lagringsskyldigheten ska regleras i lag har flertalet remissinstanser tillstyrkt utredningens avgränsning eller lämnat den utan invändning. *Riksdagens ombudsmän (JO)*, *Svea hovrätt, Länsrätten i Skåne län, Brottsförebyggande rådet, Datainspektionen, Statskontoret, Juridiska fakultetsnämnden vid Stockholms universitet, Sveriges advokatsamfund, Svenska journalistförbundet, Amnesty International, Telenor Sverige AB, Swedish Network Users' Society (SNUS)* samt *Konstnärliga och Litterära Yrkesutövares Samarbetsnämnd* (*KLYS)* har dock anfört att den närmare regleringen av lagringsskyldighetens omfattning bör ske genom lag och avstyrkt att den sker genom förordning, framför allt med hänsyn till det integritetsintrång som lagringen medför. Även *Domstolsverket* och *Skatteverket* har ifrågasatt om inte skyddet för den personliga integriteten kräver att lagringsskyldighetens omfattning regleras i lag och förespråkat att frågan övervägs ytterligare. *Teracom AB* och *IT&Telekomföretagen* har föreslagit att PTS ges i uppdrag att förtydliga kraven angående vilka uppgifter som ska lagras genom föreskrifter och anvisningar.

Skälen för regeringens förslag: Inledningsvis kan konstateras att det redan nu kan förutses att vissa av de uttryck som används i direktivet, t.ex. IMSI och IMEI, kan komma att vara föråldrade ganska snart. Direktivets uttryck om att det specifikt ska vara de uppgifter som anges i direktivet som ska omfattas av lagringsskyldighet (se artikel 3.1 i direktivet) bör enligt utredningen förstås så att lagringsskyldigheten ska omfatta de olika typer av uppgifter som framgår av artikel 5. Regeringen delar denna bedömning. *IFPI Svenska Gruppen* och *Svenska Antipiratbyrån* har understrukit vikten av en teknikneutral reglering som tar höjd för den tekniska utvecklingen. Regeringen instämmer i att en så teknikneutral lösning som möjligt bör väljas. Utgångspunkten är att de föreslagna bestämmelserna så långt det är möjligt, och med hänsyn tagen till direktivets krav, ska vara oberoende av den tekniska utvecklingen, samtidigt som behovet av tydliga och väl avgränsade regler ska beaktas.

IFPI Svenska Gruppen har i detta sammanhang påtalat att den tekniska utvecklingen av fildelningsnätverk går snabbt och att det finns en trend mot anonymisering av användare som försvårar eller omöjliggör för polis att identifiera en eventuell intrångsgörare, varför det är viktigt att lagringsskyldigheten är teknikneutral. I vilken utsträckning anonymiseringstjänster får anses omfattade av lagringsskyldigheten får avgöras utifrån vad som anförts i avsnitt 6.1. Uppgifter som genereras eller behandlas i verksamheten ska lagras av leverantören, i den utsträckning leverantören är lagringspliktig (se vidare i avsnitt 7.2). Regeringen anser

att utvecklingen på detta område bör följas, vilket i första hand är en uppgift för tillsynsmyndigheten.

Direktivet utgår från att de olika teknikområdena har ett ”vertikalt” förhållande till varandra, exempelvis så skiljs fast, mobil och Internettelefoni åt. I den tekniska realiteten är många lösningar i dagsläget emellertid kombinationer av eller integrerade med varandra. Som exempel har utredningen nämnt att en fast telefon eller en mobiltelefon kan användas för Internetåtkomst med vars hjälp Internettelefoni kan användas. Ett annat exempel som nämnts är att ett och samma samtal kan gå från en mobiltelefon till en fast telefon och att transitering kan ske med hjälp av Internettelefoni mellan mobilnätet och det fasta telenätet. Mot bakgrund av teknikutvecklingen, där olika sektorer gradvis växer samman (konvergens) har utredningen valt en lösning, där de olika teknikområdena är uppdelade på ett mer teknikneutralt sätt än vad som följer direkt av direktivet. Remissinstanserna har inte haft något att invända mot det, utan istället i vissa fall välkomnat en sådan lösning. Regeringen delar utredningens bedömning när det gäller lagringsskyldighetens struktur.

Som utredningen konstaterat är tydligheten i regleringen 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.

Ett sätt att få en så teknikneutral reglering som möjligt är att låta regleringen avspegla hur systemen rent faktiskt fungerar, dvs. som utredningen förespråkat, att anlägga ett mer ”horisontellt” synsätt vid tolkningen och genomförandet av direktivet. Sättet att strukturera de uppgifter som ska lagras bör därför ske enligt följande:

- telefoni,
- meddelandehantering,
- Internetåtkomst, och
- anslutningsform.

Med denna struktur, genom vilken regeringen frångått utgångspunkten att olika teknikområden ska åtskiljas, kommer exempelvis nya tekniker för kommunikationstjänster att kunna omfattas på ett enklare sätt. De förändringar som kan komma att krävas i framtiden blir med denna lösning mer begränsade än vad de annars hade blivit. För att klargöra vad som åsyftas med respektive kategori bör dessa anges tydligt i lag.

Vidare bör lagringskravet utformas utifrån ändamålen med lagringen, vilka anges i direktivet, nämligen att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typen av kommunikation, kommunikationsutrustningen, samt lokaliseringen av mobil kommunikationsutrustning. Slutligen bör lagringsskyldigheten beskrivas på detaljnivå, varvid utgångspunkten är de trafikuppgifter som anges i artikel 5 i direktivet. Som exempel på sådana uppgifter som för närvarande får anses omfattas av lagringskravet kan nämnas uppgifter om uppringande telefonnummer, nummer som slagits och uppgifter om abonnent och registrerad användare.

Sammanfattningsvis anser regeringen att denna uppdelning av regleringen av lagringskravet skapar en struktur som har bättre förutsättningar att stå sig över tiden.

När det gäller frågan om vad som ska regleras i lag och vad som i övrigt kan regleras i förordning eller genom myndighetsföreskrifter kan inledningsvis konstateras att det idag inte finns några bestämmelser som ålägger leverantörer av allmänna kommunikationsnät eller elektroniska kommunikationstjänster att lagra uppgifter. Lagen om elektronisk kommunikation ger däremot leverantörerna en möjlighet att lagra uppgifter för vissa angivna syften, t.ex. för abonnentfakturering eller om det är nödvändigt för att kunna förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. I vare sig lag eller förordning anges närmare vilka uppgifter som i dessa fall får lagras.

Utredningen har föreslagit att själva lagringsskyldigheten ska anges i lag medan den närmare utformningen i huvudsak kan regleras genom förordning. Många remissinstanser har invänt mot detta och anfört att den närmare regleringen av lagringsskyldighetens omfattning bör ske genom lag. Huvudskälet till detta är att integritetsintrångets omfattning bör återfinnas i lag för att inte kunna utvidgas utan riksdagens medverkan. Regeringen instämmer i vad flera remissinstanser påpekat, bl.a. att principen bör vara att lagringsskyldighetens omfattning bör regleras i lag. Däremot anser regeringen inte att lagringsskyldigheten in i minsta tekniska detalj behöver regleras i lag. Den mer tekniska specifikationen av lagringskravet kan ske i förordning. Som jämförelse kan framhållas att leverantörerna redan kan lagra trafikuppgifter för vissa angivna ändamål utan att det i lag anges vilka uppgifter som därmed avses. Regeringen anser dock att det i lag behövs en, i förhållande till utredningens förslag, närmare redogörelse för lagringsskyldighetens omfattning. Mot denna bakgrund bör det i lag regleras dels vilka teknikområden som omfattas, t.ex. telefoni, och dels ändamålet med lagringen, t.ex. för att identifiera och spåra en kommunikationskälla. När det gäller den tekniska beskrivningen av vad som ska lagras kan det regleras i förordning. Därigenom skapas en förhållandevis teknikneutral reglering i lag samtidigt som möjlighet finns att, genom förordningsändringar, följa den tekniska utvecklingen. De lagändringar som behövs bör göras i lagen om elektronisk kommunikation.

6.3 Teknikområden som omfattas av lagringsskyldigheten

Regeringens förslag: Med de kategorier som ska omfattas av lagringsskyldigheten avses följande.
– *Telefoni:* en elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan.
– *Meddelandehantering:* utbyte eller överföring av elektroniskt meddelande som inte är samtal eller information som överförs som del av sändningar av ljudradio- och TV-program.
– *Internetåtkomst:* möjlighet till överföring av ip-paket som ger användaren tillgång till Internet.
– *Anslutningsform*: den kapacitet som tillhandahålls för att få Internetåtkomst.

Utredningens förslag överensstämmer i huvudsak med regeringens förslag. Utredningen har dock gjort bedömningen att definitionerna kan framgå av förordning. Utredningen gör i sin definition av meddelandehantering inte undantag för information som överförs som del av sändningar av ljudradio- och TV-program.

Remissinstanserna har i sak tillstyrkt utredningens förslag eller inte framfört några synpunkter på förslaget.

Skälen för regeringens förslag: Begreppet telefonitjänst definieras i 1 kap. 7 § lagen om elektronisk kommunikation 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. 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”), varav de sistnämnda fås från en telefoninummerplan. Telefoninummerplanen är ett format och en struktur för hur telefonnummer fördelas på ett såväl internationellt som nationellt plan. Varje land har sitt specifika landsnummer (eller prefix) som sedan delas upp i riktnummer. Ett krav är att varje nummer ska vara öppet och kunna nås från alla elektroniska kommunikationsnät.

Många Internettelefonitjänster medger inte alltid att nödsamtal genomförs. Den definition av telefonitjänst som används i lagen om elektronisk kommunikation blir därmed för snäv för att kunna användas i detta sammanhang. Telefoni bör därför i nu aktuellt sammanhang, såsom utredningen föreslagit, definieras utan krav på att nödsamtal ska kunna genomföras.

Utredningen har föreslagit att en definition av *telefoni* ska omfatta situationer då E.164-nummer används, dvs. nummer ur en telefoninummerplan, av någon av den uppringande respektive uppringda parten. Regeringen delar den bedömningen. Definitionen av telefoni kommer därmed att inkludera fast och mobil telefoni och de flesta Internettelefonitjänster. Internettelefoni som bara använder andra ”adresser” som

identifiering omfattas däremot inte. En konsekvens av det kan bli att en del kommunikationstjänster för överföring av tal i realtid inte kommer att falla under lagringsskyldigheten. Med telefoni avses inte kommunikation som omfattas av begreppet meddelandehantering.

Lagringskravet enligt direktivet om trafikuppgifter omfattar lagring av meddelanden i form av främst elektronisk post, sms (Short Message Service) och mms (Multimedia Messaging Service). Utredningen har valt att använda begreppet *meddelandehantering* för att beskriva överföringen av sådana elektroniska meddelanden. Detta tydliggör den strävan som finns att använda sig av en horisontell struktur. Exempelvis kan ett sms skickas från såväl en mobil som fast telefon. Med meddelandehantering ska avses tjänster som använder sig av olika kommunikationsprotokoll, dvs. regler om hur kommunikationen ska ske, som SMTP (Simple Mail Transfer Protocol, RFC 2821 och RFC 2822), som är det vanligaste protokollet för att leverera elektronisk post, och SMPP (Short Message Peer-to-Peer Protocol v5.0) som utgör ett kommunikationsprotokoll för utbyte av sms-meddelanden. Regeringen anser att meddelandehantering ska definieras på det sätt utredningen föreslagit, dvs. utbyte eller överföring av elektroniskt meddelande, med undantag för sådana meddelanden som är samtal och därmed omfattas av definitionen av telefoni. Eftersom definitionen av elektroniskt meddelande även omfattar viss information som överförs som del av sändningar av ljudradio- och TV-program måste undantag också göras för sådana sändningar.

Direktivet omfattar vidare lagring av trafikuppgifter när det gäller *Internetåtkomst*. Med Internetåtkomst avses möjligheten att överföra s.k. ip-paket med hjälp av olika tekniker (anslutningsform) och som ger användaren tillgång till Internet. Med ip-paket avses ett telekommunikationspaket med data som ska överföras, inklusive en titelrad med bland annat sändarens namn och mottagarens ip-nummer. I praktiken innebär Internetåtkomst att användaren tilldelas en eller flera ip-adresser för kommunikation. Med ip-adress (Internet Protocol Adress) avses en unik adress som används för identifiering och kommunikation mellan två datorer på Internet med hjälp av Internet Protocol-standarden (ip). Ip-adresserna kan vara fasta adresser, dvs. de förändras inte när användaren ges åtkomst till Internet, oavsett tidpunkt, eller dynamiska adresser, dvs. de tilldelas användaren varje gång denne kopplar upp sig mot Internet. De dynamiska adresserna delas oftast ut med hjälp av protokollet DHCP (Dynamic Host Configuration Protocol). I de nya bestämmelserna som reglerar lagring av trafikuppgifter bör Internetåtkomst definieras som möjlighet till överföring av ip-paket som ger användaren tillgång till Internet.

Direktivet om lagring av trafikuppgifter anger inte uttryckligen *anslutningsform* som en särskild kategori inom vilken vissa uppgifter ska lagras. Utredningen har emellertid funnit att en sådan uppdelning bör göras. Det kan nämligen ibland röra sig om olika leverantörer avseende det abonnemang som möjliggör Internetåtkomsten respektive leveransen av själva nätkapaciteten. I sådana fall kan exempelvis ändpunkterna för en kommunikation via Internet inte spåras utan uppgift om vilken nätkapacitet som har använts. Regeringen delar därför bedömningen att den föreslagna uppdelningen är ett sätt att skapa den horisontella struktur för lagringen som bör eftersträvas. Med anslutningsform för Internet-

åtkomst avses alltså den kapacitet som ger möjlighet till överföring av ip-paket för att få Internetåtkomst. Ett exempel på anslutningsform är DSL (Digital Subscriber Line), vilken i sin tur kan ske med hjälp av leverantörer av t.ex. bitströmsaccess. Bitströmsaccess innebär att operatörer kan få tillträde till det metallbaserade accessnät som TeliaSonera äger, och därigenom erbjuda bredband via telenätet, oftast med ADSL. Andra exempel på anslutningsform är fiberoptiska anslutningar, 3G (UMTS), GSM (GPRS), vanliga traditionella telefonmodem och WLAN (trådlöst nät).

6.4 Lagringsskyldighet utöver direktivet

Regeringens förslag: Lagringsskyldigheten ska, utöver vad som följer av direktivet om lagring av trafikuppgifter, gälla även vid misslyckad uppringning och för uppgifter om lokalisering av mobil kommunikationsutrustning vid kommunikationens slut.

Utredningens bedömning överensstämmer med regeringens förslag.

Remissinstanserna: *Svea hovrätt, Åklagarmyndigheten, Tullverket* och *MälarEnergi AB* har tillstyrkt utredningens förslag att lagringsskyldigheten även ska omfatta misslyckad uppringning och lokaliseringsuppgifter för mobil kommunikationsutrustning vid kommunikations slut och anfört att förslaget innebär en bra avvägning mellan integritetsskydd och brottsbekämpning. *IFPI Svenska Gruppen* och *Svenska Antipiratbyrån* har anfört att regleringen även bör ta höjd för den tekniska utvecklingen av fildelningsnätverk. *Svenska Antipiratbyrån* anser med hänsyn därtill att det är olyckligt att till exempel FTP-servrar utesluts ur lagringsskyldigheten.

Stockholms handelskammare, Statskontoret, Post- och telestyrelsen (PTS), TeliaSonera AB, Sveriges advokatsamfund, Tele2 Sverige AB, Telenor Sverige AB, .SE samt *Konstnärliga och Litterära Yrkesutövares Samarbetsnämnd* (*KLYS)* har avstyrkt att kravet på lagring ska omfatta fler uppgifter än de som anges i direktivet. Skälen är dels att direktivet i sig anses innefatta ett tillräckligt intrång i den personliga integriteten, dels att förslaget innebär ökade kostnader och därmed riskerar att snedvrida konkurrensen. *Juridiska fakultetsnämnden vid Lunds universitet* har ifrågasatt behovet av att gå utöver kraven i direktivet. *IT&Telekomföretagen* har påtalat att de svenska särkraven kommer att innebära en särskild kostnad för de aktörer som inte har moderna telefonväxlar och servrar, eftersom särkraven kommer att kräva så stora anpassningar i äldre system att det inte är ekonomiskt försvarbart att inte ersätta dem med nya system, vilket innebär att aktörer på den svenska marknaden får en klar konkurrensnackdel i förhållande till aktörer i andra EU-länder. Dessa synpunkter delas av TeliaSonera AB och Tele 2 Sverige AB. Tele 2 Sverige AB har vidare lagt till att svenska särkrav innebär att operatörer verksamma i flera länder inte kan skräddarsy ett system som kan användas i samtliga medlemsstater och att arbetet med att ta fram ett system för att tekniskt efterkomma direktivets regler redan påbörjats med anledning av direktivets genomförande i andra medlemsstater, vilket

innebär svårigheter att i dagsläget lägga in annan typ av funktionalitet. TeliaSonera AB har anfört att det är tveksamt om lagring av data om cell-id vid samtliga mobilsamtals avslutande tillför värdefull information som är till nytta i sådan grad att det motiverar de omfattande kostnader för ytterligare anpassningar som kommer att behöva utföras i de tekniska systemen. PTS, liksom TeliaSonera AB, har förespråkat att lagstiftaren inväntar hur tillämpningen av direktivet utvecklar sig på europeisk nivå innan tillämpningsområdet i Sverige utvidgas till områden som inte uttryckligen berörs i direktivet. *Riksdagens ombudsmän (JO)* har, mot bakgrund av att brottsbekämpningsintresset bör väga relativt tungt sedan skälen för lagring väl bedömts motivera ett intrång i integritetsskyddet, inget att erinra mot att vissa uppgifter utöver direktivets krav omfattas av lagringsskyldigheten.

Skälen för regeringens förslag

Brottsbekämpande myndigheters behov

Enligt direktivet ska lagringsskyldighet gälla *misslyckad uppringning* under förutsättning att uppgifterna lagras eller loggas av leverantören (artikel 3). Om uppgifterna ”bara” genereras eller behandlas finns ingen lagringsskyldighet, utan det är upp till varje medlemsstat att i dessa fall avgöra om en sådan skyldighet ska införas eller inte.

Misslyckad uppringning innebär att samtal kopplas fram men att ingen svarar på uppringningen. Misslyckad uppringning kan också bero på att det skett ett ingrepp i driften av 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. Misslyckad uppringning omfattar däremot inte samtal som *inte* kopplas fram, dvs. när det inträffat något tekniskt fel och inget meddelande lämnas om att abonnenten inte kan nås.

De brottsbekämpande myndigheterna har anfört att de har behov av trafikuppgifter som gäller misslyckad uppringning. De har uppgett att i dagsläget lagras eller loggas uppgifter om misslyckad uppringning hos vissa leverantörer men inte hos andra. Myndigheterna har också anfört 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” ibland som ett kommunikationssätt mellan gärningsmän vid genomförandet av brott.

En lagringsskyldighet avseende misslyckad uppringning i den mån dessa uppgifter för närvarande inte lagras eller loggas innebär längre gående skyldighet än vad som följer av direktivet om lagring av trafikuppgifter. En sådan skyldighet kan dock införas med stöd av artikel 15.1

i direktivet om integritet och elektronisk kommunikation, bl.a. för brottsbekämpande syften.

Regeringen instämmer i de brottsbekämpande myndigheternas bedömning att det finns ett lika stort behov av uppgifter om misslyckad uppringning som av uppgifter om de samtal som har lyckats. Regeringen menar vidare att den begränsning som ligger i direktivet skulle kunna leda till att de brottsbekämpande myndigheterna inte får tillgång till uppgifter som de i dag får, dvs. om dessa uppgifter inte framöver lagras av leverantörerna. Utifrån ett brottsbekämpande perspektiv finns således stort värde i att lagringsskyldigheten gäller även vid misslyckad uppringning, utan den begränsning som ligger i direktivet om att uppgifterna inte bara ska vara behandlade utan även lagrade eller loggade av leverantören.

När det gäller uppgifter om samtal som inte kopplas fram så omfattas dessa inte av någon lagringsskyldighet enligt direktivet. De brottsbekämpande myndigheterna har uppgett att det inte finns något påtagligt behov av sådana uppgifter och utredningens förslag omfattar inte lagringsskyldighet i dessa fall. Regeringen delar utredningens bedömning att sådana samtal inte ska omfattas av lagringsskyldigheten.

Av direktivet följer att *lokaliseringsinformation* för mobil kommunikationsutrustning ska lagras för kommunikationens *början*. I stället för direktivets ”lokaliseringsbeteckning (cell-id)” använder regeringen, liksom utredningen, det vidare begreppet lokaliseringsinformation, eftersom det är ett mer teknikneutralt begrepp. Beträffande Internetåtkomst och anslutningsform finns det ett annat lagringskrav i direktivet som innebär att lokaliseringsinformation ska lagras. Uppgifter som är nödvändiga för att identifiera den kommunikationsutrustning som använts innebär, när det gäller Internetåtkomst och anslutningsform, att DSL (Digital Subscriber Line) eller annan slutpunkt för kommunikationsutrustningen ska lagras. Sådana slutpunkter omfattar bl.a. lokaliseringsinformation. Lokaliseringsinformation vid Internetåtkomst och anslutningsform som sker via mobil kommunikationsutrustning ska alltså lagras redan på den grunden.

De brottsbekämpande myndigheterna har anfört att de också har behov av att få lokaliseringsinformation avseende kommunikationens *slut*. Direktivet om lagring av trafikuppgifter medför ingen skyldighet att lagra dessa uppgifter. Utifrån samma övervägande som beträffande misslyckade uppringningar kan en skyldighet att lagra sådana uppgifter införas med stöd av artikel 15.1 i direktivet om integritet och elektronisk kommunikation, om det finns ett behov av uppgifterna för brottsbekämpningsändamål och lagringsskyldigheten bedöms vara en nödvändig åtgärd.

Som utredningen redovisat används mobiltelefoner 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 den mobila kommunikationsutrustningen befunnit sig vid påbörjandet av kommunikationen innebär enligt myndigheterna en begränsning i det brottsbekämpande arbetet. Det borde enligt myndigheterna finnas en lagringsskyl-

dighet för lokaliseringsuppgifter inte bara för kommunikationens början utan också för dess *slut* samt för *pågående kommunikation,* exempelvis en gång per minut.

TeliaSonera AB har anfört att lagring av kommunikationens slut skulle ge upphov till stora datavolymer samtidigt som det är tveksamt om det tillför så värdefull information att det motiverar de omfattande kostnader för ytterligare anpassningar som kommer att behöva utföras i de tekniska systemen.

Liksom utredningen kan regeringen också konstatera att lokaliseringsinformation för kommunikationens början många gånger inte alls är tillräckligt för de brottsbekämpande syftena. Om lokaliseringsinformation för kommunikationens slut inte lagras skulle det vara enkelt att i en kriminell verksamhet vilseleda myndigheterna med negativa följder för utredningsarbetet. Detta har också beaktats i exempelvis den danska regleringen, som föreskriver lagringsskyldighet för lokaliseringsuppgifter även rörande kommunikationens slut. Information om var en kommunikation avslutades kan vara lika värdefull som information om var den påbörjades. Mot bakgrund av ovanstående får det enligt regeringens mening anses stå klart att det finnas ett påtagligt behov av att lagra lokaliseringsuppgifter även vid kommunikationens slut.

De brottsbekämpande myndigheterna har därutöver framfört att det finns ett behov av lokaliseringsinformation för pågående kommunikation, eftersom en gärningsman mycket väl kan ha påbörjat och avslutat kommunikationen på andra platser än på själva brottsplatsen. Vill man som brottsling försvåra utredningsarbetet vore det enkelt att påbörja t.ex. 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 som lagras, t.ex. rörande rån och smugglingsresor med narkotika. Även dessa uppgifter är av värde i det brottsbekämpande arbetet.

Skydd för integriteten samt kostnads- och konkurrensaspekter

Ovan har konstaterats att de brottsbekämpande myndigheterna har behov av vissa uppgifter som inte omfattas av den lagringsskyldighet som direktivet föreskriver. Detta behov ska emellertid ställas mot andra intressen, dels skyddet för enskildas integritet, dels kostnads- och konkurrensaspekter. Flera remissinstanser har också invänt mot införande av en lagringsskyldighet som går utöver direktivet, bl.a. mot bakgrund av dessa sistnämnda intressen.

PTS, liksom *.SE,* har anfört att den omständigheten att direktivet i sig är en mycket kontroversiell lagstiftning, som föregicks av en omfattande debatt över hela Europa, talar för att genomförandet av direktivet i så stor utsträckning som möjligt bör hålla sig inom dess ramar. *Sveriges advokatsamfund*, *TeliaSonera AB* och *KLYS* har framfört liknande synpunkter.

Som bl.a. *JO* konstaterat är den avvägning som ska göras mellan brottsbekämpning och integritetsskydd i allt väsentligt given i direktivet. JO har vidare anfört att det är oundvikligt att lagstiftningen anpassas till de förändrade beteendemönster som är resultatet av att människor utnytt-

jar nya tekniker som förenklar och effektiviserar deras liv och att användarna i princip är medvetna om att data kring sådana aktiviteter skapas, avsätts och ibland registreras, men att den omständigheten i princip inte avhåller dem från att använda tekniken. Regeringen instämmer i JO:s konstaterande att människors allmänna obehag inför att information om dem lagras inte bör underskattas, men att det vore orealistiskt att utesluta detta växande informationsfält från de brottsbekämpande myndigheternas insyn. Som framgått ovan finns det goda skäl att för brottsbekämpande ändamål lagra uppgifter beträffande både misslyckad uppringning och lokaliseringsuppgifter vid kommunikationens slut beträffande mobil kommunikationsutrustning, vilket också bekräftas i remissyttranden från de brottsbekämpande myndigheterna. Sedan skälen för lagring väl bedömts motivera ett intrång i integritetsskyddet bör brottsbekämpningsintresset, som JO konstaterat, väga relativt tungt. Regeringen anser alltså, även med beaktande av integritetsskyddet, att det är motiverat att lagringsskyldigheten omfattar misslyckade uppringningar och lokaliseringsuppgifter vid kommunikationens slut beträffande mobil kommunikationsutrustning.

När det gäller lagring av lokaliseringsuppgifter beträffande pågående kommunikation bör följande beaktas. En sådan lagring skulle i princip innebära att t.ex. alla mobilanvändares rörelser under pågående samtal skulle lagras med jämna mellanrum, t.ex. varje minut eller en gång i timmen. Detta skulle föranleda lagring av en stor mängd uppgifter och skulle innebära en betydande utvidgning i förhållande till de skyldigheter som följer av direktivet. En lagringsskyldighet för lokaliseringsinformation under pågående kommunikation föreslås därför inte, främst på grund av integritetsskyddsskäl men även av kostnads- och konkurrensskäl.

Utredningen har vidare redovisat att de brottsbekämpande myndigheterna uttryckt behov av att få tillgång till uppgifter om besök på webbsidor (”surfning”), besök på ”chattsidor” (”chattrum”) och användning av File Transfer Protocol, FTP (t.ex. överföring eller nedladdning av filer). Även *Svenska Antipiratbyrån* anser att det är olyckligt att FTP-servrar utesluts ur lagringsskyldigheten med tanke på att de organiserade grupper som ägnar sig åt piratkopiering av film på nätet i stor utsträckning använder sig av sådana servrar. Enligt regeringens mening är det emellertid inte aktuellt att nu överväga en sådan väsentligt utökad lagringsskyldighet som föreslagits med hänsyn till vad det skulle innebära i förhållande till såväl integritetsskydd som kostnads- och konkurrensaspekter.

När det gäller kostnads- och konkurrensaspekterna för en lagringsskyldighet som går utöver direktivet har bl.a. *Stockholms handelskammare* menat att det förhållandet att den svenska regleringen omfattar mer än vad direktivet kräver höjer tröskeln för inträde på marknaden och leder till ökade kostnader och en mer svåröverskådlig marknad för aktörerna, vilket gör det svårare att agera internationellt och kan göra att vissa företag, till men för utvecklingen i Sverige, väljer att ha sina tjänster utomlands. Även *PTS* har anfört att det uppstår konkurrensnackdelar inom EU om direktivet genomförs på olika sätt i olika medlemsstater, vilket *Telia-Sonera AB* instämt i. Dessa har även föreslagit att regeringen inväntar hur tillämpningen av direktivet utvecklar sig på europeisk nivå innan tillämpningsområdet utvecklas till områden som inte uttryckligen berörs i

direktivet. *Telenor Sverige AB* har anfört att regeringen, både med hänsyn till proportionalitetsprincipen, men också av kostnads- och konkurrensskäl, inte bör ställa högre krav på vilka uppgifter som ska lagras än vad som är avsett i direktivet. *Tele 2 Sverige AB* har konstaterat att krav utöver de krav som ställs enligt direktivet skapar stora problem för operatörer med verksamhet i flera medlemsstater samt leder till kraftigt ökade anpassningskostnader av systemen, eftersom det då inte går att skräddarsy ett system som kan användas i samtliga medlemsstater. Vidare har Tele 2 Sverige AB anfört att de krav som ställs vid lagstiftning av förevarande slag i så stor utsträckning som möjligt bör vara lika för alla operatörer inom unionen för att konkurrenssituationen på framförallt den inre marknaden inte i onödan ska rubbas.

Utredningen har konstaterat att lagring av lokaliseringsinformation vid kommunikationens slut för mobil kommunikationsutrustning och av uppgifter rörande misslyckad uppringning kräver särskild anpassning av systemen, eftersom sådana uppgifter för närvarande inte lagras hos alla leverantörer, även om de i och för sig identifieras och sparas för en kort stund. Även volymen på lagrad datamängd kommer öka, främst med hänsyn till att även misslyckade uppringningar nu ska lagras. Avseende t.ex. fast telefoni utgör de misslyckade uppringningarna tre fjärdedelar av alla samtal. Utredningen bedömde emellertid att de totala kostnaderna för lagringsskyldigheten är begränsade i förhållande till marknadens totala omsättning, dvs. att marknaden som helhet torde påverkas endast marginellt av att en lagringsskyldighet införs. Regeringen ansluter sig till denna bedömning och menar att införandet av en lagringsskyldighet för dessa uppgifter inte i någon beaktansvärd grad kan förväntas påverka nya leverantörers möjligheter till marknadstillträde eller investeringsvilja.

Flera av de leverantörer som omfattas av lagringsskyldigheten har verksamhet i ett eller flera andra länder. Konkurrensförhållandena inom och mellan olika EU-länder torde, som flera remissinstanser påpekar, påverkas av hur enskilda länder reglerar lagringsskyldigheten. En fullständig harmonisering av reglerna inom EU skulle skapa de bästa förutsättningarna ur ett konkurrensperspektiv. Någon sådan fullständig enhetlighet i utformningen av de regler som genomför direktivet i de olika europeiska staterna finns dock inte. Direktivet medger viss variation i genomförandet för att tillgodose olika behov och skillnader mellan staterna, t.ex. beträffande lagringstid, men även beträffande vilka uppgifter som kan lagras. När det gäller lagringstiden har flertalet stater också valt en längre tid än Sverige (se nästa avsnitt), vilket borde innebära att svenska företag i den delen får en konkurrensmässig fördel. Det förekommer även krav på att trafikuppgifter vid ”surfning” lagras, något som det aktuella förslaget inte omfattar. Även detta torde medföra en fördel för svenska företag. Regeringen anser därför att det, även vid beaktande av konkurrens- och kostnadsaspekter, är motiverat att lagringsskyldigheten omfattar misslyckade uppringningar och lokaliseringsuppgifter vid kommunikationens slut för mobil kommunikationsutrustning.

Sammanfattning

Regeringen anser sammanfattningsvis att det ska införas en skyldighet att lagra uppgifter om misslyckad uppringning samt lokaliseringsuppgifter vid kommunikationens slut för mobil kommunikationsutrustning. Dessa uppgifter är av stort värde för de brottsbekämpande myndigheterna. Även med beaktande av intresset av enskildas integritetsskydd samt kostnads- och konkurrensaspekter bedöms en sådan lagringsskyldighet vara proportionerlig i förhållande till ändamålet att ge de brottsbekämpande myndigheterna tillgång till behövliga uppgifter för att avslöja, utreda och lagföra brott. Lagringsskyldigheten utgör enligt regeringens uppfattning inte heller något hot mot den fria åsiktsbildningen.

6.5 Lagringstiden

Regeringens förslag: Trafikuppgifterna ska lagras under sex månader från den dag kommunikationen avslutades.

Vid lagringstidens slut ska uppgifterna utplånas av den lagringsskyldige, om inte de brottsbekämpande myndigheterna vid den tiden har begärt tillgång till uppgifterna, men ännu inte fått ut dem. Vid en sådan situation ska uppgifterna utplånas av den lagringsskyldige efter att de har lämnats ut.

Utredningens förslag: Trafikuppgifterna ska lagras i ett år. I övrigt överensstämmer förslaget med regeringens.

Remissinstanserna: Ett antal remissinstanser, däribland *Riksdagens ombudsmän (JO), Tullverket* och *Juridiska fakultetsnämnden vid Stockholms universitet,* har inte haft någon invändning mot utredningens förslag om en lagringstid på ett år. *Telenor Sverige AB* har sagt sig kunna acceptera ett års lagringstid förutsatt att regeringen lyfter bort de andra extensiva lagringskraven. *Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, IFPI Svenska Gruppen* och *Svenska Antipiratbyrån* har, utifrån ett brottsbekämpningsintresse, förespråkat en lagringstid om två år. *Stockholms handelskammare, Juridiska fakultetsnämnden vid Lunds universitet, TeliaSonera AB, Amnesty International, Tele2 Sverige AB, .SE, KLYS* samt *Svenska Linuxföreningen* har förespråkat att lagringstiden inte går utöver direktivets minimikrav, dvs. sex månader. Hänvisning har då gjorts till såväl integritetsskyddet som kostnads-, säkerhets- och konkurrensaspekter.

Skälen för regeringens förslag: 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.

Regeringen delar utredningens bedömning att en och samma lagringstid ska gälla för alla typer av trafikuppgifter. Det går inte att generellt påstå att vissa av de trafikuppgifter som ska lagras är mer eller mindre viktiga än andra för utredning av brott.

Frågan är då hur lång lagringstiden ska vara. Direktivet ger, som nämnts inledningsvis, möjlighet till minst sex månaders och högst två års lagring.

Allvarliga brott orsakar stora skador för enskilda och samhället. Varje sådant brott som kan förhindras eller klaras upp, kanske redan på planeringsstadiet, är av stort värde. Både för medborgarna i allmänhet och för brottsoffren är det angeläget att förutsättningarna för att klara upp allvarliga brott är så bra som möjligt. 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. I betänkandet (s. 171 f.) lämnas en utförlig redovisning av behovet av trafikuppgifter i brottsbekämpningen. Av redogörelsen framgår att majoriteten av de grova brotten torde klaras upp inom ett år efter det att de har begåtts, men att även de trafikuppgifter som skulle finnas tillgängliga genom en lagringstid på två år skulle användas vid ett inte obetydligt antal utredningar som gäller grov brottslighet. Enligt utredningen skulle en lagringstid på sex månader innebära en stark tidspress för de brottsbekämpande myndigheterna. Åklagarmyndigheten har vidare anfört att ett stort antal åklagare omvittnat att de handlagt mål med misstankar om allvarlig brottslighet där samtalslistor med uppgifter som varit mer än ett år gamla varit av avgörande betydelse för utredningen och lagföringen av brotten. Säkerhetspolisen har, som exempel på situationer då behov av trafikuppgifter som är äldre än ett år uppstått, nämnt att det i samband med utredningen av bombdåden i Madrid i mars 2004 efterfrågades historiska trafikuppgifter från Sverige som var betydligt äldre än så. Det får således antas att upp till två år gamla trafikuppgifter i vissa situationer kan behövas för bekämpningen av allvarlig brottslighet. Sett endast utifrån ett brottsbekämpningsperspektiv skulle en lagringstid på två år därför väl kunna motiveras. Det finns emellertid andra aspekter som talar emot att välja en så lång lagringstid, vilka påtalats av flera remissinstanser.

En stor mängd trafikuppgifter kommer att lagras. Redan lagringen av trafikuppgifterna innebär ett intrång i enskildas integritet. Det är naturligt att enskilda individers upplevelse av intrånget har samband med lagringstidens längd och mängden uppgifter som lagras. Det måste också beaktas att risken för konkreta integritetsskador genom t.ex. läckage eller annan otillåten spridning torde öka ju längre tid uppgifterna lagras.

Även olika tekniska faktorer har betydelse när det gäller att bedöma hur lång lagringstiden bör vara. Lagringsvolymen ökar självfallet ju längre lagringstiden blir och det medför ökade krav på säkerhet. Det kan antas att kostnaderna för teknik och administrativa säkerhetsrutiner blir högre med en lagringstid på två år än med en lagringstid på sex månader.

Kraven på den kapacitet som leverantörerna måste ha för att fullgöra lagringsskyldigheten och kostnaderna för lagringen ökar med lagringstiden. Lagringstiden torde därmed vara 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, där en kortare lagringstid kan innebära vissa konkurrensmässiga fördelar för företag

etablerade i Sverige. Flertalet av de medlemsstater som har genomfört direktivet har också valt en längre lagringstid än sex månader.

Sammanfattningsvis finns det från brottsbekämpningssynpunkt således skäl att bestämma en så lång lagringstid som möjligt och som utredningen redovisat kommer en kortare lagringstid att innebära en ökad tidspress för de brottsbekämpande myndigheterna. Såväl skyddet för den personliga integriteten som kostnads-, säkerhets- och konkurrensaspekter talar emellertid för en kortare lagringstid. Enligt regeringens bedömning bör lagringstiden, främst med hänsyn till integritetsskyddet, bestämmas till den kortast möjliga, dvs. sex månader.

I detta sammanhang kan noteras att den lagringsskyldighet som nu införs inte innebär någon ändring av nuvarande regler om för vilka övriga ändamål leverantörerna kan spara trafikuppgifter (se avsnitt 5.1). De trafikuppgifter som har sparats av leverantörerna enligt befintliga regler, exempelvis för fakturering eller marknadsföring, kommer således alltjämt att vara tillgängliga. För sådana uppgifter kommer nuvarande regler om utplåning eller avidentifiering i 6 kap. 5 § lagen om elektronisk kommunikation alltjämt att gälla.

En annan fråga är 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. Vid telefoni och meddelandehantering blir kommunikationens slut utgångspunkten för lagringstidens beräkning. Utgångspunkten vid Internetåtkomst blir i stället avloggningen och vid anslutningsform när abonnemanget eller avtalet upphör.

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 § lagen om elektronisk kommunikation). Därför bör det införas ett uttryckligt 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. I en sådan situation ska uppgifterna i stället utplånas av leverantören så snart de har lämnats ut till den myndighet som har begärt dem.

7 Leverantörernas skyldigheter

7.1 Vem ska ansvara för lagringsskyldigheten?

Regeringens förslag: Det är leverantörerna som ska vara skyldiga att lagra trafikuppgifter. En leverantör ska dock kunna uppdra åt någon annan att utföra lagringen.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt eller inte framfört några invändningar mot förslaget. *Åklagarmyndigheten* har anfört att det ur de brottsbekämpande myndigheternas perspektiv skulle vara en fördel om en begäran om uppgifter som lagrats kunde lämnas till ett och samma ställe. *Amnesty International* har anfört att en lagring hos leverantörerna innebär att staten överlämnar ansvaret för skyddandet av integritetskänsliga uppgifter om enskilda till många olika privata aktörer, vilket innebär en risk för att uppgifterna sprids till obehöriga personer eller används för otillåtna ändamål samt innebär att det blir svårt att överblicka och utöva tillsyn över hanteringen av uppgifterna. *IT&Telekomföretagen, Banverket* och *Svenska Stadsnätsföreningen* har anfört att de extra kostnader som framför allt drabbar mindre operatörer skulle kunna reduceras om lagringen skedde centralt. IT&Telekomföretagen har vidare föreslagit en möjlighet för marknaden att arrangera en centraliserad lagring, vilket även skulle minska risken för problem med säkerhet och kvalitet. *Bahnhof AB* har ansett det orimligt att ansvaret för tvångsmedel landar på privatägda företag. *Riksdagens ombudsmän (JO)* har påtalat en motsägelse i att spridningen av lagring på flera leverantörer av utredningen beskrivs som en fördel från integritetssynpunkt samtidigt som möjligheten att anlita annan för lagringen framställs som något positivt. Enligt JO är det en fördel från integritetssynpunkt att den föreslagna lagringsskyldigheten åligger envar leverantör och att lagringen således sprids på flera håll. Ju fler uppgifter som kan sammanställas, desto större blir det potentiella integritetsintrånget. Om flera leverantörer sluter sig samman för att ordna lagringen gemensamt alternativt lejer ut den till någon som erbjuder denna tjänst, innebär det integritetsrisker som inte synes helt lätta att överblicka. *.SE* har betonat att möjligheten att anlita annan för att fullgöra lagringen i sig medför en risk för att en stor mängd information från olika källor samlas på samma plats och därmed kan komma att utgöra en måltavla för olika typer av attacker. *Stockholms handelskammare* och *Telenor Sverige AB* har ansett att en centraliserad lagring inte bör tillåtas av säkerhetsskäl.

Skälen för regeringens förslag: I avsnitt 6.1 föreslås att uppgifter som genereras eller behandlas av den enskilde nät- eller tjänsteleverantören ska lagras. En fråga som då uppstår är vem som ska ansvara för denna lagring. En utgångspunkt i direktivet är att lagringen bör ske på ett sådant sätt att man undviker att uppgifterna lagras mer än en gång (skäl 13).

En ganska självklar utgångspunkt kan tyckas vara att leverantörerna lagrar de uppgifter som genereras eller behandlas i den tjänst som leverantören tillhandahåller. En annan möjlig modell för lagring av trafikuppgifterna skulle kunna vara att leverantörerna skickar de uppgifter som ska lagras till ett centralt lager. Detta skulle innebära att antingen staten eller en utsedd aktör skulle lagra samtliga trafikuppgifter som alla leverantörer genererar eller behandlar. En fördel med ett sådant centrallager skulle, såsom *Amnesty International* påpekat, vara 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 enbart behöva vända sig till ett ställe när trafikuppgifter ska begäras ut, något som påpekats av *Åklagarmyndigheten*. Såsom anförts av *IT&Telekomföretagen, Banverket* och *Svenska Stadsnätsföreningen* skulle en central lagring också kunna innebära vissa fördelar ur kostnads-

synpunkt, främst för de mindre operatörerna. *Bahnhof AB* förespråkar en central lagring i statlig regi.

Regeringen anser, trots de beskrivna fördelarna, i likhet med utredningen att en central lagring skulle vara problematisk, framför allt ur integritetssynpunkt. Även andra skäl talar mot ett centrallager. En sådan lösning skulle 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. Om staten skulle ta ansvaret för en sådan central lagring skulle det innebära att staten behövde bygga upp en egen kompetens på områden där leverantörerna redan besitter en hög kompetens. En central lagring skulle också, oavsett vem som skulle ta ansvaret för denna, ställa mycket stora krav på lagringsvolym och säkra lösningar för överförande av uppgifterna från leverantörerna. Av säkerhetsskäl har också *Stockholms handelskammare* och *Telenor Sverige AB* avstyrkt en centraliserad lagring och *.SE* har pekat på att ansamlingar av uppgifter utgör en säkerhetsrisk. Regeringen anser på de angivna skälen att lagringen inte bör ske centralt.

Den modell som innebär att trafikuppgifterna lagras där de genereras eller behandlas, dvs. hos leverantörerna, framstår enligt regeringen som ett bättre alternativ. Denna lösning innebär stora fördelar ur främst integritetssynpunkt, då trafikuppgifterna oftast inte kommer att vara omedelbart läsbara eftersom den enskilde leverantören i många fall bara kommer att ha information som måste ställas samman med trafikuppgifter som lagrats av någon annan leverantör för att en enskild persons kommunikation ska kunna utläsas. Det förhållandet att trafikuppgifterna oftast inte finns samlade hos en enda nät- eller tjänsteleverantör, utan kan involvera flera olika leverantörer med delansvar för kommunikationen innebär visserligen, som utredningen konstaterat, att det är närmast omöjligt att skapa ett system som garanterar att uppgifterna inte lagras mer än en gång. För ett sådant system skulle leverantörerna behöva ha kontroll över vilka andra leverantörer som genererat eller behandlat uppgifter i samband med en kommunikation. Detta skulle vara kostsamt och tekniskt komplicerat och innebära nackdelar från integritetssynpunkt.

Den bästa lösningen är, enligt regeringens mening, att lagringen som utgångspunkt sker hos leverantörerna. Genom att de leverantörer som genererar och behandlar uppgifterna också lagrar dem säkerställs vidare att lagringen sker så enkelt och säkert som möjligt med utnyttjande av den kunskap om teknik som varje leverantör har.

Det som dock bör övervägas är om det, som utredningen funnit, ska vara tillåtet för leverantörerna att uppdra åt någon annan att utföra lagringen av uppgifterna. Som framhållits av *JO* är det ur integritetsskyddssynpunkt önskvärt att uppgifterna lagras på så spridda håll som möjligt. Som utredningen har redovisat finns det emellertid mycket stora skillnader mellan de leverantörer som kommer att omfattas av lagringsskyldigheten, både i fråga om verksamhet och volym. De små leverantörerna skulle, om de var skyldiga att anpassa sina system för att själva kunna lagra uppgifterna, kunna drabbas av betydande kostnads- och konkurrensmässiga nackdelar i förhållande till leverantörer som hanterar en väsentligt större mängd uppgifter. Om de däremot ges en möjlighet att uppdra åt annan att utföra lagringen kan kostnaderna sannolikt begränsas och möjligheten till konkurrens därmed förbättras. Enligt regeringens

bedömning överväger dessa fördelar de möjliga nackdelar som vissa remissinstanser pekat på.

Det bör framhållas att det inte är själva lagringsskyldigheten och de förpliktelser som följer med denna som kan uppdras åt annan. Behandling av personuppgifter när annan anlitas för lagringen regleras i 30 § första stycket personuppgiftslagen (1998:204). Den som anlitas benämns personuppgiftsbiträde. Av andra stycket samma bestämmelse framgår att det ska finnas ett personuppgiftsbiträdesavtal samt att detta ska innehålla bestämmelser dels om att biträdet endast får behandla uppgifterna enligt instruktioner från den ansvarige, och dels om att biträdet är skyldigt att vidta de säkerhetsåtgärder som anges i 31 § första stycket. Av detta följer att den lagringsskyldige leverantören aldrig genom ett avtal om att annan ska utföra lagringen kan frånhända sig någon skyldighet gentemot myndigheter eller enskilda. Exempelvis ska de brottsbekämpande myndigheterna alltid kunna vända sig till den som enligt bestämmelsen är skyldig att lagra uppgifterna med en begäran om utlämnande.

Visserligen kan en möjlighet att uppdra åt annan att fullgöra lagringen ge intryck av en motsägelse, som *JO* påpekat, om utgångspunkten är att lagringen av integritetsskäl ska ske hos respektive leverantör. Risken för att alla leverantörer kommer att använda sig av denna möjlighet eller att alla de som väljer att utnyttja möjligheten kommer att välja samma aktör måste dock betraktas som begränsad. Utvecklingen i denna fråga måste emellertid bevakas. Om det framöver skulle bildas mycket stora samlade lager, närmast liknande ett centrallager, kan frågan behöva ses över och bedömningen bli en annan.

7.2 Vilka leverantörer ska vara lagringsskyldiga?

Regeringens förslag: De leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation ska vara skyldiga att lagra trafikuppgifter. Tillsynsmyndigheten ska i enskilda fall få besluta om undantag från lagringskravet. Om ett undantagsbeslut har förenats med villkor och villkoren inte följts eller om det finns andra särskilda skäl ska beslutet kunna återkallas.

Utredningens förslag överensstämmer i huvudsak med regeringens förslag. Utredningen föreslog även att sekretess skulle gälla för uppgifter som hänför sig till tillsynsmyndighetens verksamhet för prövning av frågor om undantag.

Remissinstanserna: Flertalet remissinstanser har inte framfört några invändningar mot förslaget. *Rikspolisstyrelsen* har förespråkat en utvidgning av kretsen av lagringsskyldiga, med hänvisning till att det hos de brottsbekämpande myndigheterna finns ett behov av att fler leverantörer än de som följer av direktivet får skyldighet att lagra trafikuppgifter. *Åklagarmyndigheten, Ekobrottsmyndigheten, Telenor Sverige AB* och *Hi3G Access AB* har avstyrkt möjligheten till undantag från lagringsskyldigheten. Åklagarmyndigheten och Ekobrottsmyndigheten har ifrågasatt om direktivet tillåter att undantag medges samt påtalat den vikt det ur brottsutredande perspektiv är att så många trafikuppgifter som möjligt

lagras. De har pekat på risken att kriminella söker sig till operatörer som undantas från lagringsskyldigheten. Telenor Sverige AB har vidare anfört att en undantagsmöjlighet missgynnar konkurrensen, eftersom vissa operatörer då kan slippa kostnader och administration för lagringsskyldighet. *Teracom AB, .SE* och *SNUS* har efterlyst ett klargörande av förslaget om undantag från lagringsskyldigheten. Även Ekobrottsmyndigheten har efterlyst en tydligare reglering kring undantagsmöjligheten och framfört att en författningsreglering avseende tidsbegränsning och omprövning bör övervägas. Myndigheten har vidare framfört att det kan övervägas om en vandelsprövning bör införas om undantag ska kunna beviljas för vissa operatörer i likhet med 3 kap. 2 § andra stycket första punkten lagen (2004:297) om bank- och finansieringsrörelse samt har ifrågasatt om den sekretess som utredningen föreslagit får någon effekt så länge leverantörerna själva inte kan förhindras att offentliggöra undantagsbesluten. *IFPI Svenska Gruppen* och *Svenska Antipiratbyrån* har understrukit vikten av att en prövning av undantag från lagringsskyldigheten ska göras även med beaktande av information rörande vissa leverantörers verksamhet som kan finnas tillgänglig hos dem. *Rikspolisstyrelsen* och *Säkerhetspolisen* har anfört att det uttryckligen bör regleras att en konkursförvaltare eller likvidator som övertar en lagringsskyldig leverantörs verksamhet ser till att lagringen fullgörs under hela den återstående lagringstiden.

Skälen för regeringens förslag

Anmälningspliktiga leverantörer föreslås bli lagringsskyldiga

Direktivet om lagring av trafikuppgifter omfattar leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster *eller* allmänna kommunikationsnät. Det innebär att en leverantör av kommunikationstjänster inte samtidigt behöver leverera ett nät för att omfattas av skyldigheten att lagra trafikuppgifter (se t.ex. artikel 1 och 3).

Direktivets uttryck om vilka som omfattas av lagringsskyldigheten ansluter till formuleringarna i 2 kap. 1 § lagen om elektronisk kommunikation, där det anges att allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster endast får tillhandahållas efter anmälan till tillsynsmyndigheten (Post- och telestyrelsen). Av 2 kap. 2 § samma lag 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 samt att Post- och telestyrelsen får meddela föreskrifter om ytterligare undantag från anmälningsplikten. Undantaget för verksamhet som består i trådsändningar som omfattas av grundlagsskyddet i yttrandefrihetsgrundlagen har sin grund i att vissa av de krav som lagen om elektronisk kommunikation ställer för bedrivande av anmälningspliktig verksamhet annars skulle komma i konflikt med etableringsfriheten i 3 kap. 1 § yttrandefrihetsgrundlagen för sådan sändningsverksamhet.

Med den omfattning som direktivet anger blir inte alla leverantörer lagringsskyldiga. I de flesta fall då exempelvis en e-posttjänst tillhanda-

hålls ett slutet sällskap såsom anställda i företag 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 eller myndigheten omfattas då inte heller av skyldigheten att lagra enligt direktivet. *Rikspolisstyrelsen* har förespråkat att kretsen av lagringsskyldiga vidgas med hänvisning till att det hos de brottsbekämpande myndigheterna finns ett behov av att fler leverantörer än de som följer av direktivet får skyldighet att lagra trafikuppgifter. Ur ett brottsbekämpande perspektiv ligger det förvisso en begränsning i att direktivet om lagring av trafikuppgifter enbart omfattar leverantörer av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster. Regeringens ansluter sig dock till utredningens bedömning att ett system som innebär att andra än anmälningspliktiga leverantörer skulle omfattas av lagringsskyldigheten skulle bli svårt att överblicka och kontrollera. Skyldigheten att lagra trafikuppgifter bör därför ansluta till direktivet och till anmälningsplikten i 2 kap. 1 § lagen om elektronisk kommunikation. Det är till Post- och telestyrelsen (PTS) som anmälan ska göras och det blir PTS som genom sin tillämpning av bestämmelsen om anmälningsplikt avgör vilka leverantörer som också ska vara lagringsskyldiga. Att leverantörer som bedriver grundlagsskyddad verksamhet i form av trådsändningar inte kommer att omfattas av skyldigheten att lagra trafikuppgifter följer redan av att de inte är anmälningspliktiga enligt lagen om elektronisk kommunikation.

Undantag från lagringsskyldigheten

En annan fråga är om det, som utredningen föreslagit, med hänsyn till den stora variationen mellan leverantörerna i fråga om storlek och verksamhet, ska finnas en möjlighet till undantag från lagringsskyldigheten (även om anmälningsplikt enligt 2 kap. 1 § lagen om elektronisk kommunikation föreligger). Flera remissinstanser har avstyrkt en sådan undantagsmöjlighet. *Åklagarmyndigheten* och *Ekobrottsmyndigheten* har ifrågasatt om direktivet tillåter att undantag medges samt påtalat vikten, ur ett brottsutredande perspektiv, av att så många trafikuppgifter som möjligt lagras.

Regeringen delar Åklagarmyndighetens och Ekobrottsmyndighetens synpunkt att trafikuppgifter är mycket viktiga för utredandet av brott, vilket kommit till uttryck på många sätt i det aktuella förslaget. Det kan emellertid inte uteslutas att en del verksamheter, som i och för sig är anmälningspliktiga, är av så liten omfattning och har ett så begränsat intresse ur ett brottsbekämpande perspektiv att det skulle vara oproportionerligt att kräva att leverantören som bedriver verksamheten helt eller delvis ska lagra trafikuppgifter på det sätt som direktivet kräver. I direktivet framhålls att skyldigheterna för leverantörerna ska vara proportionerliga (exempelvis skäl 23). Flera medlemsstater som har genomfört direktivet har också infört undantag för de minsta leverantörerna. Det måste mot denna bakgrund anses finnas en möjlighet att meddela undantag från lagringsskyldigheten och regeringen anser i likhet med utredningen att en sådan undantagsmöjlighet är rimlig. Regeringens mening är, i motsats till

vad *Telenor Sverige AB* har anfört, att en sådan undantagsmöjlighet bidrar till att mildra de negativa effekter lagringskravet annars skulle kunna ha på konkurrensen. Det kan i detta sammanhang nämnas att även den anpassningsskyldighet som gäller enligt 6 kap. 19 § fjärde stycket lagen om elektronisk kommunikation för hemlig teleavlyssning och hemlig teleövervakning innehåller en liknande möjlighet till undantag.

En prövning av om undantag från lagringsskyldigheten ska medges bör, som utredningen föreslagit, göras av tillsynsmyndigheten efter en ansökan av en leverantör. Vid prövningen får en avvägning göras mellan nyttan för brottsbekämpningen av att leverantören lagrar trafikuppgifterna och kostnaden eller andra negativa effekter som lagringsskyldigheten innebär för leverantören. Undantagsmöjligheten bör tillämpas restriktivt. Tillsynsmyndigheten bör inför sitt beslut samråda med representanter för de brottsbekämpande myndigheterna. Bestämmelser om detta bör ges i förordning. I det samråd som ska föregå beslutet kommer naturligtvis leverantören och dennes verksamhet att granskas innan något undantag godtas. Regeringen ser inte något behov av att därutöver, som Ekobrottsmyndigheten föreslagit, införa en lagstadgad vandelsprövning av de leverantörer som ansöker om undantag. Regeringen delar *IFPI Svenska Gruppens* och *Svenska Antipiratbyråns* åsikt så till vida att det är av vikt att tillsynsmyndigheten vid sin bedömning har ett fullgott beslutsunderlag, men anser inte att någon skyldighet att samråda med andra än ovan nämnda myndigheter bör regleras.

För att minska den risk som *Ekobrottsmyndigheten*, *Telenor Sverige AB* och *Hi3G Access AB* pekat på, att personer som bedriver allvarlig brottslig verksamhet kommer att söka sig till de leverantörer som är undantagna från lagringsskyldigheten, föreslog utredningen att sekretess skulle gälla för uppgifter som hänför sig till tillsynsmyndighetens verksamhet för prövning av frågor om undantag. Regeringen delar redovisade remissinstansers åsikt att det är mycket viktigt att utvecklingen inte blir sådan att vissa leverantörer, i syfte att locka till sig kunder som bedriver kriminell verksamhet, anpassar sin verksamhet så att de ska medges undantag från lagringsskyldigheten. Regeringen delar dock Ekobrottsmyndighetens bedömning att en reglering som föreskriver sekretess för tillsynsmyndighetens verksamhet vad avser undantagsbeslut blir tämligen verkningslös eftersom det alltjämt står de leverantörer som medgivits undantag fritt att själva uppge att de inte omfattas av lagringskravet. Regeringen föreslår därför inte någon sådan sekretessreglering.

Ett par remissinstanser har efterlyst en tydligare reglering av undantagsmöjligheten. Enligt regeringens mening talar emellertid den snabba tekniska utvecklingen och variationen i leverantörernas verksamhet med styrka för att systemet bör utformas som en möjlighet för tillsynsmyndigheten att i enskilda fall meddela undantag från lagringsskyldigheten och inte som en generell föreskrift. En ordning där undantagsbeslut meddelas i enskilda fall torde också vara den som minimerar risken för att leverantörer anpassar sin verksamhet för att undgå lagringskravet. Här kan noteras att möjligheten till undantag från anpassningsskyldigheten enligt 6 kap. 19 § fjärde stycket lagen om elektronisk kommunikation också är utformad som en möjlighet till undantag efter beslut av PTS i enskilda fall. Inte heller för sådana beslut gäller sekretess.

Av stor vikt i detta sammanhang är att tillsynsmyndigheten övervakar de leverantörer som medgivits undantag. *Ekobrottsmyndigheten* har anfört att en författningsreglering avseende tidsbegränsning och omprövning av beslut om undantag bör övervägas. Som myndigheten påpekat följer det av allmänna förvaltningsrättsliga principer att det finns en möjlighet att tidsbegränsa och återkalla ett undantagsbeslut. Ett beslut om undantag från lagringsskyldigheten är dock ett för leverantören gynnande förvaltningsbeslut. Av hänsyn till den enskildes trygghet är huvudregeln beträffande dessa beslut att de inte kan återkallas. Återkallelse anses emellertid möjlig bl.a. med stöd av förbehåll i själva beslutet eller i den författning som ligger till grund för beslutet (se prop. 1985/86:80 s. 39 f.). Regeringen gör i likhet med Ekobrottsmyndigheten bedömningen att det i bestämmelsen som reglerar möjligheten att medge undantag från lagringsskyldigheten för tydlighets skull bör anges att ett beslut om undantag får förenas med villkor samt att ett sådant beslut får återkallas om villkoren i beslutet inte har följts. Enligt regeringens bedömning bör det även vara möjligt att återkalla ett beslut om undantag från lagringsskyldigheten när det finns andra särskilda skäl för det. Ett villkor som uppställs kan exempelvis vara kopplat till verksamhetens omfattning och en återkallelse skulle exempelvis kunna bli aktuell i en situation då en leverantör som medgivits undantag efter beslutet får ett stort antal kunder eller att de brottsbekämpande myndigheterna skulle uppmärksamma en tendens att kriminella personer söker sig till en viss leverantör som är undantagen från lagringsskyldigheten.

Tillsynsmyndighetens beslut i fråga om undantag bör kunna överklagas hos allmän förvaltningsdomstol. Vid överklagande till kammarrätten bör krävas prövningstillstånd (jämför 8 kap. 19 § lagen om elektronisk kommunikation).

Ansvaret vid verksamhetsövergång, konkurs och likvidation

I utredningen gjordes bedömningen att det följer av föreslagna regler att skyldigheten att lagra uppgifter, liksom de regler om exempelvis utplånande och skyddsåtgärder som följer med lagringsskyldigheten, övergår till den som övertar en verksamhet som träffas av lagringsskyldigheten (dvs. om leverantören är anmälningspliktig enligt 2 kap. 1 § lagen om elektronisk kommunikation). Enligt utredningens bedömning innebär en konkurs eller likvidation inte i sig att lagringsskyldigheten upphör, utan det följer av gällande regler att 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. Detta skulle enligt utredningen vara fallet både då verksamheten drivs vidare och då den upphör.

Rikspolisstyrelsen och *Säkerhetspolisen* har härvid anfört att de anser att det uttryckligen bör regleras att en konkursförvaltare eller likvidator som övertar en lagringsskyldig leverantörs verksamhet ska se till att lagringen fullgörs under hela den återstående lagringstiden.

Det följer av gällande regler att då en anmälningspliktig verksamhet drivs vidare har den som företräder verksamheten en skyldighet att se till att de förpliktelser som följer med verksamheten fortsätter att fullgöras

(exempelvis lagring, utplåning, kvalitet och säkerhet). Detta gäller oavsett om den som företräder verksamheten är en ny ägare eller en konkursförvaltare eller likvidator. Om verksamheten avvecklas torde dock inte någon sådan skyldighet föreligga.

Som huvudregel gäller att när en verksamhet upphör genom konkurs eller likvidation så upphör även de skyldigheter som var förknippade med verksamheten. Detta är enligt regeringens bedömning fallet också beträffande skyldigheterna kring lagring av trafikuppgifter. Motsatt ordning skulle innebära att t.ex. en konkursförvaltare skulle åläggas skyldigheter som i många fall skulle motverka det övergripande syftet med konkursen, nämligen att för borgenärernas räkning på bästa sätt förvalta boets tillgångar och avveckla verksamheten. För att en sådan skyldighet skulle gälla skulle det därför, såsom *Rikspolisstyrelsen* och *Säkerhetspolisen* föreslagit, krävas en uttrycklig reglering därom. Regeringen kan dock i nuläget inte förutse något behov av en specialreglering som tillser att lagringen fullgörs även efter ett beslut om konkurs eller likvidation. Det torde vara i ytterst sällsynta fall de brottsbekämpande myndigheterna har behov av att få tillgång till trafikuppgifter som finns just hos en leverantör som gått i konkurs eller trätt i likvidation och vars verksamhet hunnit upphöra innan behovet uppstod hos myndigheten.

7.3 För vilka ändamål ska leverantörerna få behandla trafikuppgifter?

Regeringens förslag: Trafikuppgifter som har lagrats för brottsbekämpande syften ska, utöver den behandling som utgörs av lagringen, få behandlas av leverantörerna endast för att lämnas ut enligt 6 kap. 22 § första stycket 2 eller 3 lagen om elektronisk kommunikation eller efter beslut om hemlig teleövervakning enligt 27 kap. 19 § rättegångsbalken.

Utredningens förslag överensstämmer i sak med regeringens.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt eller lämnat förslaget utan invändningar. *IFPI Svenska Gruppen* och *Svenska Antipiratbyrån* har dock anfört att uppgifter som lagrats enligt direktivet även bör kunna lämnas ut till innehavare av immateriella rättigheter. *Mälar-Energi AB* har efterlyst tydliga direktiv avseende vilka som har rätt att få ut lagrade trafikuppgifter.

Skälen för regeringens förslag: Enligt artikel 15.1 i direktiv 2002/58/EG om integritet och elektronisk kommunikation får trafikuppgifter lagras och lämnas ut för vissa närmare angivna syften, bl.a. för brottsbekämpning. Med stöd av denna bestämmelse har direktivet om lagring av trafikuppgifter tillkommit i syfte att harmonisera medlemsstaternas bestämmelser när det gäller skyldigheten att lagra trafikuppgifter för att säkerställa att uppgifterna finns tillgängliga för avslöjande, utredning och åtal av allvarliga brott. I artikel 4 i direktivet om lagring av trafikuppgifter stadgas vidare att medlemsstaterna ska anta åtgärder för att säkerställa att uppgifter som lagras i enlighet med direktivet om lagring av trafikuppgifter endast görs tillgängliga för behöriga nationella

myndigheter i närmare angivna fall och i enlighet med nationell lagstiftning. Direktivet om lagring av trafikuppgifter syftar alltså inte till att säkerställa tillgången till dessa uppgifter för andra syften. Mot den bakgrunden instämmer regeringen i utredningens bedömning att de trafikuppgifter som ska lagras med stöd av direktivet bör vara förbehållna brottsbekämpande syften och brottsbekämpande myndigheter. I de nya bestämmelserna bör därmed uttryckligen anges att dessa uppgifter får behandlas endast för att lämnas ut till brottsbekämpande myndigheter enligt reglerna i 6 kap. 22 § första stycket 2 eller 3 lagen om elektronisk kommunikation eller enligt 27 kap. 19 § rättegångsbalken. Det innebär bl.a. att varken rättegångsbalkens bestämmelser om vittnesförhör och edition eller de immaterialrättsliga bestämmelserna om s.k. informationsföreläggande kommer att kunna användas för att få ut de uppgifter som lagras med stöd av direktivet. Uppgifterna får alltså inte lämnas ut till någon annan eller för något annat syfte än vad som uttryckligen stadgas i de nya bestämmelserna. Det innebär också att uppgifter som lagras med stöd av direktivet inte får behandlas av leverantörerna för något internt intresse, såsom exempelvis fakturering och marknadsföring, eller för att förhindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst.

Med anledning av de synpunkter som *IFPI Svenska Gruppen* och *Svenska Antipiratbyrån* har framfört, om att det bör möjliggöras även för upphovsrättsinnehavare att få del av uppgifter som lagras med stöd av de nya bestämmelserna, vill regeringen tillägga följande. Visserligen möjliggör artikel 15.1 i direktivet om integritet och elektronisk kommunikation att trafikuppgifter får lagras och lämnas ut även för att t.ex. enskilda ska kunna tillvarata sina rättigheter i en civilrättslig process. Den lagringsskyldighet som nu föreslås ska dock endast omfatta användning för brottsbekämpande syften. Vid sidan av denna skyldighet kommer reglerna som möjliggör lagring av uppgifter för vissa andra ändamål att fortsätta att gälla (se vidare nedan). För att fullgöra förpliktelsen att se till att uppgifter som lagras enligt den nya lagringsskyldigheten inte ska kunna användas för andra ändamål, måste den som lagrar uppgifter redan från början se till att lagringen sker på ett sätt som gör att det står klart för vilket eller vilka syften uppgifterna lagras. Av detta följer att det måste vara möjligt för en utomstående, exempelvis tillsynsmyndigheten, att kunna avgöra för vilket eller vilka syften uppgifter finns lagrade. Det ska alltså inte vara möjligt för exempelvis en Internetleverantör att först när ett utlämnande blir aktuellt, eller när det upptäcks att uppgifterna även behövs för t.ex. fakturering, bestämma för vilket eller vilka syften uppgiften är lagrad. Om en uppgift endast finns lagrad för brottsbekämpande syften får uppgiften inte användas för några andra syften, inte ens för att leverantören själv ska kunna förhindra och avslöja obehörig användning. I övrigt kommer de regler om behandling av trafikuppgifter som redan gäller alltså att fortsätta gälla.

De allmänna bestämmelserna om behandling av trafikuppgifter finns främst i 6 kap. 5, 6 och 8 §§ lagen om elektronisk kommunikation. Enligt 6 kap. 5 § är huvudregeln att trafikuppgifter ska utplånas eller avidentifieras när de inte längre behövs för att överföra ett elektroniskt meddelande, men det finns flera undantag från denna huvudregel. Det kan t.ex. vara nödvändigt att spara denna typ av uppgifter för att kunna för-

hindra och avslöja obehörig användning av ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst. Vidare får trafikuppgifter sparas om de behövs för abonnentfakturering eller för betalning av avgifter för samtrafik. Sådana uppgifter får också behandlas för att marknadsföra elektroniska kommunikationstjänster, om den abonnent eller användare som uppgifterna avser har samtyckt till det. Dessa bestämmelser kommer att kvarstå oförändrade, vid sidan av den lagring som ska ske för brottsbekämpande syften. I den mån en leverantör har behov av att behandla de trafikuppgifter som enligt direktivet ska lagras för brottsbekämpande syften även för andra ändamål som anges i lagen om elektronisk kommunikation så får dessa uppgifter alltså även sparas med stöd av gällande regler.

Uppgifter som har sparats enligt nu gällande regler, dvs. uppgifter som inte enbart är lagrade på grund av den lagringsskyldighet som nu införs, ska precis som tidigare vara åtkomliga för vissa civilrättsliga ändamål, bl.a. enligt rättegångsbalkens regler om vittnesförhör och edition samt enligt de immaterialrättsliga bestämmelserna om s.k. informationsföreläggande (jfr prop. 2008/09:67 s. 124 f. och 143 samt skäl 12 i direktivets ingress, se dock även Högsta domstolens beslut den 16 september 2010 att inhämta förhandsavgörande i mål nr Ö 4817-09). När det gäller just bestämmelserna om informationsföreläggande kan dessutom tilläggas att regeringen genom beslut den 23 juli 2009 har tillsatt en särskild utredare som ska utvärdera hur regelverket påverkat rättighetshavare, Internetleverantörer och konsumenter (kommittédirektiv 2009:68). Utvärderingen ska bl.a. omfatta frågan om reglerna ger rättighetshavarna möjlighet att få tillgång till begärda uppgifter i befogad omfattning. Uppdraget ska redovisas senast den 1 augusti 2012.

7.4 Anpassning för utlämnande av uppgifter

Regeringens förslag: Leverantörerna ska bedriva verksamheten så att uppgifterna kan lämnas ut utan dröjsmål och informationen enkelt kan tas om hand samt så att verkställandet inte röjs.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt förslaget eller lämnat det utan invändningar. *Rikspolisstyrelsen* har framhållit att polisens behov av uppgifterna kan vara mycket akut och uppstå när som helst dygnet runt året om. *Stockholms handelskammare* har anfört att det är rimligt att anta att kravet på att uppgifterna enkelt kan tas om hand och lämnas ut utan dröjsmål delvis är i konflikt med kraven på säker lagring, hantering och överföring av uppgifterna. Användning av t.ex. kryptering och metoder för verifiering av dataintegritet kan ju innebära att processerna tar längre tid. Det påpekas också att detta inte bara gäller till skydd för personlig integritet utan också för att säkerställa uppgifternas riktighet, något som är avgörande för brottsbekämpningen. *IT&Telekomföretagen* och *Telenor Sverige AB* har kritiserat utredningens tolkning att ett ”utlämnande utan dröjsmål” innebär att aktivitet ska inledas inom någon timme räknat från när leverantören tar emot (blir medveten om) begäran

om att trafikuppgifter ska lämnas ut. IT&Telekomföretagen har anfört att ett sådant krav innebär stora kostnader som relativt sett drabbar små operatörer hårdare. Telenor Sverige AB har anfört att kravet i praktiken innebär att det måste finnas jourhavande personal för att serva myndigheterna med information, vilket kommer i konflikt med att det av säkerhetsskäl krävs att endast ett fåtal personer med speciell utbildning och behörighet inom ett företag får hantera dessa känsliga uppgifter.

Skälen för regeringens förslag: 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.

Enligt 6 kap. 19 § lagen om elektronisk kommunikation ska en verksamhet bedrivas så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas och så att verkställandet inte röjs. Detta är innebörden av den s.k. anpassningsskyldigheten. Denna skyldighet 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 endast gäller 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.

Som framgår av avsnitt 7.2 föreslår regeringen att skyldigheten att lagra trafikuppgifter ska omfatta samtliga de leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation. Denna skyldighet omfattar därmed fler leverantörer än de som är anpassningsskyldiga enligt 6 kap. 19 § lagen om elektronisk kommunikation. Skyldigheten att lagra trafikuppgifterna bör därför förenas med en anpassningsskyldighet som innebär att samtliga de lagringsskyldiga leverantörernas verksamhet ska bedrivas på ett sådant sätt att de lagrade uppgifterna enkelt kan överföras till och användas av de brottsbekämpande myndigheterna. Det innebär att myndigheterna utan ansträngning ska kunna ta del av informationen även om den skulle vara exempelvis krypterad eller komprimerad. Uppgifterna måste emellertid alltid överlämnas på ett sådant sätt att säkerheten och skyddet för uppgifterna inte eftersätts.

Därutöver bör det ställas krav i fråga om hur snabbt uppgifterna ska göras tillgängliga för myndigheterna. Som ovan nämnts krävs i direktivet om lagring av trafikuppgifter att uppgifterna lagras på ett sådant sätt att de tillsammans med annan nödvändig information kan överföras till

myndigheterna *utan dröjsmål*. En motsvarande lagbestämmelse bör införas avseende de uppgifter som lagras enligt direktivet.

När det gäller den praktiska tillämpningen av begreppet *utan dröjsmål* har det framgått av remissynpunkterna att det finns intressen som talar i olika riktningar. Å ena sidan kan det hos de brottsbekämpande myndigheterna i vissa situationer finnas ett akut behov av att få tillgång till trafikuppgifter och å andra sidan innebär en ständig beredskap hos leverantörerna ökade kostnader och i vissa fall eventuellt även ökade säkerhetsrisker. Enligt regeringens mening väger dock brottsbekämpningsintresset i denna fråga mycket tungt, då en snabb verkställighet i vissa fall kan vara absolut nödvändig för att skydda allmänheten eller föra en brådskande utredning framåt. Regeringen delar därför utredningens bedömning att begreppet *utan dröjsmål* i den nya bestämmelsen rimligen bör tillämpas så att behandling av en begäran som inkommer under kontorstid ska inledas inom mycket kort tid samt att leverantörerna kan komma att behöva arbeta med sådana förfrågningar även utanför kontorstid. Hur snabbt ett utlämnande ska ske i det enskilda fallet är en fråga som kommer att få avgöras av de brottsbekämpande myndigheterna och leverantörerna i varje situation. Därutöver omfattar tillsynsmyndighetens allmänna tillsynsverksamhet enligt 7 kap. lagen om elektronisk kommunikation även tillsyn av att leverantörerna lever upp till sina skyldigheter i denna del (se vidare avsnitt 8.2).

Slutligen ska, på samma sätt som gäller enligt 6 kap. 19 § lagen om elektronisk kommunikation, leverantörerna bedriva sin verksamhet på ett sådant sätt att verkställandet inte röjs.

Överföring ska ske så snart någon uppgift finns tillgänglig. Det kan innebära att det sker överföring vid flera tillfällen. Det kan för de brottsbekämpande myndigheterna t.ex. vara av stort värde 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.

8 Skyddet för de lagrade uppgifterna

För att lagringen av trafikuppgifter ska ha den säkerhet som krävs för att uppnå syftet med lagringen och för att skapa en hög tillit till systemet måste lagringen utföras så att både integritetsskyddet och effektiviteten tillgodoses. Det tekniska, såväl som det organisatoriska skyddet måste vara tillräckligt, samtidigt som de rättsliga regler som blir tillämpliga om trafikuppgifter ändå skulle komma att spridas i strid med lagen måste vara tydliga. Det fordrar också 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. En säker lagring av trafikuppgifter behöver med andra ord övervägas utifrån tekniska, administrativa, straffrättsliga, civilrättsliga och förvaltningsrättsliga utgångspunkter.

8.1 Kvalitet och säkerhet

Regeringens förslag: I lagen om elektronisk kommunikation ska det införas en särskild bestämmelse om leverantörernas skyldighet att vidta särskilda tekniska och organisatoriska åtgärder för att skydda de trafikuppgifter som lagrats för brottsbekämpande syften. Regeringen eller den myndighet regeringen bestämmer ska få meddela föreskrifter om leverantörens skyldighet att vidta dessa åtgärder.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: *Brottsoffermyndigheten* har framfört att lagring och hantering av trafikuppgifter kan utgöra en betydande säkerhetsrisk för enskilda brottsoffer. *Bahnhof AB* har anfört att inget elektroniskt system är så säkert att man kan garantera att obehöriga inte får tillgång till det och att risken för missbruk av de lagrade uppgifterna därför är stor. *Stockholms handelskammare* har anfört att det borde ställas motsvarande säkerhetskrav på de brottsbekämpande myndigheterna vad gäller överföringen och mottagandet av trafikuppgifter. *Kungliga tekniska högskolan (KTH)* har förordat att man, för att minimera riskerna vid ett eventuellt dataläckage, tittar på tekniska hjälpmedel, t.ex. kryptering, där endast brottsutredande myndighet har möjlighet att avkryptera. *Amnesty International* har uttryckt oro för att den föreslagna säkerhetsbestämmelsen är för vagt formulerad. *IT&Telekomföretagen, Juridiska fakultetsnämnden vid Stockholms universitet* och *.SE* har efterlyst mycket tydliga föreskrifter från tillsynsmyndigheten för vilket säkerhetsarbete som krävs av leverantörerna. *Försvarsmakten* har påtalat att det är angeläget att de operatörer som kommer att behandla uppgifter enligt förslaget görs uppmärksamma dels på att uppgifterna, i vart fall i sammanställd form, skulle kunna omfattas av försvarssekretess, dels att en behandling av sådana uppgifter kan medföra att föreskrifterna i bl.a. säkerhetsskyddslagen (1996:627) ska tillämpas. *TeliaSonera AB* har å sin sida anfört att en rätt avpassad kvalitet och säkerhet för operatörerna är en förutsättning för affärsverksamheten och det är hos operatörerna som den nödvändiga tekniska kunskapen finns. Eventuella föreskrifter bör därför utformas övergripande och främst inriktas på harmonisering mellan operatörer och tjänster. *Svenska Linuxföreningen* har anfört att sekretesskraven vad gäller lagrade trafikdata bör höjas och likställas med behandling av känsliga personuppgifter enligt personuppgiftslagen.

Skälen för regeringens förslag

En säker behandling av uppgifter

En grundförutsättning för att syftet med lagringen av trafikuppgifter ska uppnås är att trafikuppgifter lagras med hjälp av en teknik som håller hög kvalitet och säkerhet. En hög kvalitet och säkerhet är också avgörande för medborgarnas förtroende för systemet.

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).

Regler om teknisk säkerhet finns i 5 kap. 6 a § och 6 kap. 3 § lagen om elektronisk kommunikation. Bestämmelsen i 5 kap. 6 a § 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. Post- och telestyrelsen (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 bl.a. att leverantörerna ska ha en säkerhetspolicy och en säkerhetsorganisation som garanterar en tillräcklig säkerhetsnivå.

Bestämmelsen i 6 kap. 3 § lagen om elektronisk kommunikation 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. I artikel 4.1 i direktivet om integritet och elektronisk kommunikation, som genomförs i 6 kap. 3 § lagen om elektronisk kommunikation, anges att det är tekniska och organisatoriska åtgärder som avses.

Uttrycket ”tekniska och organisatoriska åtgärder” förekommer även i 31 § personuppgiftslagen. 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. Datainspektionen har utfärdat allmänna råd, Säkerhet för personuppgifter, som preciserar personuppgiftslagens krav på säkerhet vid behandling av personuppgifter.

Eftersom personuppgiftslagen är subsidiär till annan lagstiftning (2 §) och 6 kap. 3 § lagen om elektronisk kommunikation tar sikte på integritetsskyddet torde 31 § personuppgiftslagen inte vara direkt tillämplig för leverantörerna avseende hantering av trafikuppgifter (jfr 6 kap. 2 § lagen

om elektronisk kommunikation). Bestämmelsen kan dock ändå vara av intresse vid tolkning av det närmare innehållet i begreppet ”tekniska och organisatoriska åtgärder”.

Precisering av leverantörernas skyldigheter

Som närmare redovisats i avsnitt 7.1 föreslås leverantörerna få ansvaret för lagringen av trafikuppgifter. Det blir därmed även leverantörernas ansvar att lagringen 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 kvalitet 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 fall där de används för att bekämpa brott, behövs det regler som tar sikte på risken för otillåten eller obehörig åtkomst. Att bristande säkerhet skulle kunna få stora konsekvenser för enskilda påpekas bland andra av *Brottsoffermyndigheten*. Det innebär att de lagrade trafikuppgifterna måste skyddas inte bara genom tekniska lösningar utan också genom organisatoriska och administrativa åtgärder som begränsar tillgången till uppgifterna.

Den nuvarande bestämmelsen i 6 kap. 3 § lagen om elektronisk kommunikation 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 huvudsak de trafikuppgifter som behövs för att säkerställa att avtalsförhållandet mellan leverantör och kund fullgörs. Den lagringsskyldighet som nu föreslås har emellertid ett helt annat syfte och kommer dessutom att säkerställa att en mycket stor mängd trafikuppgifter finns bevarade. Detta medför att kravet på säkerhet bör höjas och att säkerhetsnivån bör preciseras i lagen om elektronisk kommunikation.

Trafikuppgifter är ofta också personuppgifter. Regeringen delar därför utredningens bedömning att det är lämpligt att ta det skydd för personuppgifter som gäller enligt personuppgiftslagen som utgångspunkt för fastställandet av den skyddsnivå som bör gälla även för lagrade trafikuppgifter. Med denna utgångspunkt bör kravet på säkerhet för trafikuppgifterna formuleras på så sätt att leverantörerna ska vidta de särskilda tekniska och organisatoriska åtgärder som krävs för att säkerställa att behandlade uppgifter skyddas. I detta ligger att behandlingen ska vara sådan att uppgifterna bibehåller en hög kvalité, är tillförlitliga och att det finns ett tillräckligt skydd mot intrång och annan otillåten behandling.

Amnesty International har uttryckt oro över att en bestämmelse som den föreslagna är för vagt formulerad. Regeringens mening är dock att en detaljerad bestämmelse riskerar att alltför snabbt bli föråldrad. Med hänsyn till den snabba teknikutvecklingen och leverantörernas fortlöpande säkerhetsarbete är det lämpligare att tillsynsmyndigheten närmare fastställer nivån på säkerheten genom föreskrifter. Det är då upp

till tillsynsmyndigheten att närmare överväga exempelvis de tekniska hjälpmedel som föreslås av *KTH*. Som ett antal remissinstanser påpekat är det av stor vikt att föreskrifterna är tydliga. Föreskrifterna bör tas fram efter samråd med Rikspolisstyrelsen och Datainspektionen. Den slutliga bedömningen av om de vidtagna åtgärderna är tillräckliga ska ske genom tillsynsåtgärder i enskilda fall (se närmare om tillsynsmyndighetens befogenheter i avsnitt 8.2).

Stockholms handelskammare har anfört att motsvarande säkerhetskrav som ställs på leverantörerna även bör ställas på de brottsbekämpande myndigheterna vad gäller överföringen och mottagandet av trafikuppgifter. Regeringen delar åsikten att det är av stor vikt att säkerhetsnivån är hög hos alla inblandande aktörer som behandlar trafikuppgifter. Hos de brottsbekämpande myndigheterna regleras skyddet för inhämtade trafikuppgifter i första hand genom 31 § personuppgiftslagen, som är tillämplig på myndigheternas verksamhet. Det kan också konstateras att de mängder information som ska hanteras kommer att skilja sig väsentligt mellan leverantörerna och de brottsbekämpande myndigheterna, där de senare endast kommer att hantera en bråkdel av alla de uppgifter som totalt sett har lagrats.

Regeringen anser sammanfattningsvis att säkerhetsnivån, genom den beskrivna skärpningen av kravet på leverantörernas säkerhetsarbete tillgodoser kravet på säker behandling av uppgifterna.

8.2 Tillsyn

Regeringens bedömning: Post- och telestyrelsen bör ha att utöva tillsyn över leverantörernas lagring av trafikuppgifter. Myndighetens nuvarande tillsynsbefogenheter är ändamålsenliga och tillräckliga.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser har delat eller inte framfört några invändningar mot utredningens bedömning. *Riksdagens ombudsmän (JO)* har dock förespråkat att Säkerhets- och integritetsskyddsnämnden ges en roll i sammanhanget, antingen som direkt tillsynsmyndighet eller på annat sätt. Enligt JO skulle det främja den tillit till systemet som utredningen eftersträvat. *Säkerhets- och integritetsskyddsnämnden* har anfört att det vore naturligt att nämndens tillsyn i framtiden får omfatta all tillgång till trafikuppgifter som brottsbekämpande myndigheter har, inte bara som nu är fallet vid hemlig teleövervakning. *TeliaSonera AB* har uttryckt farhågor över att Post- och telestyrelsens (PTS) utökade roll enligt förslaget riskerar att leda till alltför detaljerade föreskrifter från myndigheten. *Swedish Network Users' Society (SNUS)* har anfört att tillsynsverksamhetens bedömningar och resultat regelbundet bör rapporteras publikt för att förtroendet för systemet ska kunna upprätthållas.

Skälen för regeringens bedömning

Post- och telestyrelsens nuvarande verksamhet

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).

Enligt gällande regler utövar PTS 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. Myndigheten 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). Vidare ska PTS utöva tillsyn när det gäller leverantörernas anpassning av systemen så att hemlig teleavlyssning och hemlig teleövervakning kan verkställas (6 kap. 19 § lagen om elektronisk kommunikation) samt utöva tillsyn enligt säkerhetsskyddslagen. 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 (7 kap. 2 §). Den som bedriver sådan verksamhet kan också föreläggas att tillhandahålla myndigheten upplysningar och handlingar som behövs för utövandet av kontrollen bl.a. av efterlevnaden av de allmänna skyldigheter som gäller enligt lagen om elektronisk kommunikation (7 kap. 3 § första stycket 2). Myndigheten 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 (7 kap. 5 §). 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 tillstånd eller ändra tillståndsvillkoren samt besluta att en verksamhet helt eller delvis ska upphöra (7 kap. 8 §).

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 [2003:396] om elektronisk kommunikation). Utredningen har dock redovisat att myndigheten hittills inte har 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 § lagen om elektronisk kommunikation). Vid överklagande till kammarrätten krävs prövningstillstånd.

När det gäller behandlingen av personuppgifter utövas tillsynen av Datainspektionen. De båda myndigheternas tillsynsverksamheter överlappar således varandra i de fall de trafikuppgifter som operatörerna hanterar även utgör personuppgifter.

Post- och telestyrelsen bör utses till tillsynsmyndighet för lagringen

Inledningsvis kan det konstateras att direktivet om lagring av trafikuppgifter kräver att en eller flera behöriga, oberoende tillsynsmyndigheter utses för övervakning av att bestämmelserna om säkerhet för lagrade trafikuppgifter efterlevs.

Som framgått av redovisningen ovan är det i dag PTS som utövar tillsyn över leverantörernas verksamhet enligt lagen om elektronisk kommunikation, bl.a. i fråga om hur trafikuppgifter behandlas. Utredningen har föreslagit att PTS ska tilldelas tillsynsuppgiften även rörande den nu föreslagna lagringsskyldigheten. Förslaget grundas främst på det förhållande att PTS är den myndighet som besitter kunskap om de leverantörer som kommer att omfattas av skyldigheten att lagra trafikuppgifter och den verksamhet de annars bedriver.

JO och *Säkerhets- och integritetsskyddsnämnden* har i detta sammanhang förespråkat att Säkerhets- och integritetsskyddsnämnden ges en utökad tillsynsfunktion. JO har anfört att nämnden exempelvis skulle kunna utses till direkt tillsynsmyndighet avseende lagringen av trafikdata alternativt ges någon annan tillsynsfunktion. Säkerhets- och integritetsskyddsnämnden har föreslagit att nämndens tillsyn i framtiden ska omfatta all tillgång till trafikuppgifter som brottsbekämpande myndigheter har, inte bara som nu är fallet vid hemlig teleövervakning.

Säkerhets- och integritetsskyddsnämnden har i uppdrag att utöva tillsyn över brottsbekämpande myndigheters användning av bl.a. hemliga tvångsmedel. Nämnden inrättades som ett led i att stärka rättssäkerheten för enskilda i samband med att de brottsbekämpande myndigheterna fick möjlighet till bl.a. hemlig rumsavlyssning och preventiv tvångsmedelsanvändning. Att, så som JO föreslagit, även ge nämnden i uppdrag att bevaka att privata leverantörer sköter sin lagringsuppgift enligt direktivet om lagring av trafikdata på ett korrekt sätt skulle, enligt regeringens mening, i dagsläget vara verksamhetsfrämmande.

Vad avser påpekandet att Säkerhets- och integritetsskyddsnämnden ska ges en utökad tillsynsfunktion i fråga om de brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation, så har en sådan ordning föreslagits av Polismetodutredningen i delbetänkandet En mer rättssäker inhämtning av uppgifter om elektronisk kommunikation i brottsbekämpningen (se vidare avsnitt 5.1). Förslaget avses behandlas i en lagrådsremiss inom kort.

De lagändringar som krävs för att genomföra direktivet om lagring av trafikuppgifter föreslås införas i lagen om elektronisk kommunikation. Av den redogörelse som ovan lämnats framgår att det är PTS som enligt

7 kap. 1 § lagen om elektronisk kommunikation har tillsyn över efterlevnaden av lagen och de beslut, skyldigheter eller villkor samt de föreskrifter som har meddelats med stöd av lagen. Regeringen anser det lämpligt att PTS utövar denna tillsyn även fortsättningsvis och anser inte att det finns anledning att utse någon annan myndighet till tillsynsmyndighet över efterlevnaden av de bestämmelser som nu införs.

PTS:s tillsynsverksamhet kommer således att omfatta exempelvis att leverantörerna lagrar rätt uppgifter, att uppgifterna utplånas efter den föreskrivna tiden, att leverantörerna vidtar de särskilda tekniska och organisatoriska åtgärder som föreskrivits till skydd för de lagrade uppgifterna och att uppgifterna lämnas ut till de brottsbekämpande myndigheterna utan dröjsmål och på ett sätt som gör att de enkelt kan tas om hand samt att ett utlämnande av uppgifter inte röjs.

Ovan har redogjorts för de åtgärder PTS har tillgång till för utövandet av sin tillsyn. Där framgår att PTS, för det fall myndigheten skulle finna att en leverantör inte uppfyller sina skyldigheter, har möjlighet att vidta ett antal olika åtgärder, varav vissa får anses mycket långtgående. Såsom utredningen funnit får de befogenheter PTS har därmed anses tillräckliga för att myndigheten ska kunna utöva en aktiv och ändamålsenlig tillsynsverksamhet.

Regeringen delar inte *TeliaSonera AB:s* farhågor om risk för att PTS meddelar allt för detaljerade föreskrifter. Som redovisats i avsnitt 8.1 har ett antal remissinstanser efterlyst mycket tydliga föreskrifter från tillsynsmyndigheten. Det är även regeringens mening att detta bör vara myndighetens ambition. *SNUS* har anfört att tillsynsverksamhetens bedömningar och resultat regelbundet bör rapporteras publikt. PTS publicerar sina föreskrifter, allmänna råd, rapporter och beslut. Detta främjar allmänhetens insyn och kan därför sägas möta de synpunkter som SNUS framfört.

8.3 Överföring av personuppgifter till ett annat land

Regeringens bedömning: Trafikuppgifter bör kunna lagras i ett annat land under förutsättning att den lagringsskyldige lever upp till de krav och skyldigheter som följer av personuppgiftslagens regler och de bestämmelser som föreslås gälla vid genomförandet av direktivet om lagring av trafikuppgifter.

Utredningens bedömning överensstämmer i huvudsak med regeringens.

Remissinstanserna: Flertalet remissinstanser delar eller har inte haft några invändningar mot utredningens bedömning. *Säkerhetspolisen, Krisberedskapsmyndigheten, Sveriges advokatsamfund* och *.SE* har emellertid ifrågasatt utredningens bedömning att lagring av trafikuppgifter med tillräcklig grad av säkerhet kan ske även utomlands.

Skälen för regeringens bedömning: Inledningsvis kan konstateras att det i direktivet om lagring av trafikuppgifter inte finns några uttryckliga regler om var trafikuppgifter får eller inte får lagras. 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. En leverantör som har sådan verksamhet i Sverige som medför anmälningsskyldighet enligt 2 kap. 1 § lagen om elektronisk kommunikation föreslås vara lagringsskyldig (se avsnitt 7.2). Om en utländsk leverantör inte är anmälningspliktig för verksamhet i Sverige utan enbart förlägger sitt lager av trafikuppgifter här i landet gäller däremot inte den svenska regleringen för lagring av trafikuppgifter. Leverantörens hantering av uppgifterna i lagret kan dock komma att omfattas av t.ex. bestämmelserna i personuppgiftslagen, om hanteringen innebär behandling av sådana trafikuppgifter som är personuppgifter.

Ett antal remissinstanser har ifrågasatt utredningens bedömning att lagring av svenska trafikuppgifter med tillräcklig grad av säkerhet kan ske även utomlands.

Regeringen har förståelse för den oro som framförts. I de länder där direktivet redan har införts har det, såvitt känt, emellertid inte införts några uttryckliga begränsningar som gör att trafikuppgifter inte får lagras i ett annat medlemsland. När det gäller övriga EU-länder kan också konstateras att det i samtliga medlemsländer finns rättsregler för dataskydd som grundar sig på EU:s dataskyddsdirektiv (95/46/EG) och på direktiv 2002/58/EG om integritet och elektronisk kommunikation. Regeringen delar därför utredningens bedömning att direktivet inte ger något utrymme för att begränsa leverantörernas möjligheter att förlägga lagret av trafikuppgifter till ett annat EU-land.

Vad gäller lagring av trafikuppgifter som också är personuppgifter i ett tredjeland (dvs. ett land som varken ingår i EU eller är anslutet till EES) innehåller personuppgiftslagen bestämmelser som begränsar sådana möjligheter. Enligt 33 § personuppgiftslagen är det förbjudet att till tredjeland 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 tredjelandet. Trots förbudet är det enligt 34 § samma lag tillåtet att föra över personuppgifter till tredjeland, 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 § personuppgiftslagen meddela undantag från förbudet att föra över personuppgifter till tredjeland. Regeringen har föreskrivit att personuppgifter får föras över till tredjeland om och i den utsträckning kommissionen har konstaterat att landet har en adekvat nivå för skyddet av personuppgifter. Vilka de länderna är anges i en bilaga till personuppgiftsförordningen. Datainspektionen får också meddela beslut om

undantag i enskilda fall om det finns tillträckliga garantier till skydd för de registrerades rättigheter (13 och 14 §§ personuppgiftsförordningen [1998:1191]).

Som inledningsvis nämnts finns det i direktivet om lagring av trafikuppgifter inga uttryckliga regler som stadgar var lagringen av trafikuppgifter får eller inte får ske. Om lagringen sker inom EU eller i ett land som är anslutet till EES tillämpas ett gemensamt regelverk som innebär ett starkt skydd för personuppgifterna. Möjligheterna att lagra i ett land utanför denna krets begränsas av bestämmelserna i personuppgiftslagen. Även om lagringen förläggs utomlands gäller dock leverantörens alla skyldigheter enligt de bestämmelser som anger hur lagringsskyldigheten ska fullgöras, t.ex. de krav som rör säkerheten för de lagrade trafikuppgifterna. Detta måste särskilt beaktas av leverantörerna om de överväger att lagra trafikuppgifter utomlands. Leverantörernas skyldigheter inkluderar också bestämmelserna om tystnadsplikt. Tystnadsplikten för de uppgifter som ska lagras med stöd av de bestämmelser som genomför direktivet om lagring av trafikuppgifter föreslås endast kunna brytas med stöd av bestämmelserna i 6 kap. 22 § första stycket 2 eller 3 lagen om elektronisk kommunikation eller enligt 27 kap. 19 § rättegångsbalken, dvs. för att under vissa förutsättningar lämnas ut till åklagarmyndighet, polismyndighet eller annan myndighet. Med dessa angivna myndigheter åsyftas endast svenska – inte utländska – brottsbekämpande myndigheter. Av skäl 25 i ingressen till direktivet om lagring av trafikuppgifter framgår också att direktivet inte påverkar medlemsstaternas möjligheter att använda sig av lagstiftning som reglerar nationella myndigheters rätt till tillgång till och användning av de lagrade uppgifterna.

Sammanfattningsvis anser regeringen att befintliga regler får anses ge ett tillfredsställande skydd och att det således inte finns behov av kompletterande lagbestämmelser.

8.4 Det straff- och skadeståndsrättsliga skyddet

Regeringens bedömning: De nya reglerna om lagring av trafikuppgifter ger inte anledning att förändra någon straff- eller skadeståndsrättslig bestämmelse.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser har delat eller inte haft några invändningar mot utredningens bedömning. *Kammarrätten i Göteborg* och *.SE* har dock anfört att det bör övervägas att införa en bestämmelse om grovt dataintrång med en strängare straffskala. *Datainspektionen* har påpekat att straffbestämmelserna i personuppgiftslagen inte torde omfatta en situation där trafikuppgifterna lagras under längre tid än vad som är tillåtet eftersom straffbestämmelserna i 49 § b) personuppgiftslagen endast gäller sådan behandling i strid med personuppgiftslagen som avser s.k. känsliga uppgifter och dit hör inte trafikuppgifter.

Skälen för regeringens bedömning

Gällande regler om ansvar

Av artikel 13 i direktivet om lagring av trafikuppgifter följer 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 sanktioner, inbegripet administrativa eller straffrättsliga sanktioner, som är effektiva, proportionerliga och avskräckande.

I utredningen redogörs för befintliga straff- och skadeståndsrättsliga bestämmelser till skydd för lagrade trafikuppgifter (se sid. 202 f.). Sammanfattningsvis redovisas följande bestämmelser.

En anställd hos en leverantör som olovligen bereder sig tillgång till trafikuppgifter eller behandlar dem för ett otillåtet ändamål kan göra sig skyldig till dataintrång enligt 4 kap. 9 c § brottsbalken. Straffskalan för brottet är böter eller fängelse i högst två år. Bestämmelsen kan också bli tillämplig om någon utomstående olovligen bereder sig tillgång till de lagrade trafikuppgifterna. För dataintrång kan också dömas om någon ändrar, förstör eller blockerar en trafikuppgift. Förfarandet kan dessutom 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.

Anställda hos en leverantör som bryter mot reglerna om tystnadsplikt i lagen om elektronisk kommunikation kan också göra sig skyldiga till brott mot tystnadsplikten enligt 20 kap. 3 § brottsbalken. Straffskalan för uppsåtliga brott mot tystnadsplikten är böter eller fängelse i högst ett år. För brott som begåtts av oaktsamhet döms till böter. I ringa fall ska dock inte dömas till ansvar.

Av 49 § personuppgiftslagen följer vidare bl.a. att det är straffbart att uppsåtligen eller av grov oaktsamhet behandla personuppgifter som utgör s.k. känsliga personuppgifter enligt 13 § samma lag i strid med lagen eller att föra över personuppgifter till ett tredjeland som inte har en adekvat skyddsnivå för behandling av uppgifterna i strid med 33–35 §§ samma lag. Straffskalan är böter eller fängelse i högst sex månader eller, om brottet är grovt, fängelse i högst två år.

Skadeståndsrättslig reglering till skydd för enskilda som lidit skada till följd av felaktig behandling av trafikuppgifter återfinns, i de fall trafikuppgifterna även utgör personuppgifter, främst i personuppgiftslagen (48 §). I denna lag ges rätt till skadestånd för såväl kränkning som annan skada. Vidare återfinns andra regler om skadestånd i skadeståndslagen (1972:207). Slutligen finns regler om rätt till skadestånd även i lagen (1990:409) om skydd för företagshemligheter.

Finns behov av att överväga ändring av de straff- eller skadeståndsrättsliga reglerna?

Utredningen har gjort bedömningen att de nuvarande straff- och skadeståndsrättsliga bestämmelserna inte behöver förändras med anledning av de nya reglerna om lagring av trafikuppgifter.

Kammarrätten i Göteborg och *.SE* har anfört att införande av en bestämmelse om grovt dataintrång med en strängare straffskala bör övervägas. .SE har påtalat detta behov i anledning av att trafikuppgifter inte är ”känsliga uppgifter” i personuppgiftslagens mening och således inte skyddas av 49 § b) personuppgiftslagen. Denna begränsning i personuppgiftslagens räckvidd har även påtalats av *Datainspektionen*.

Vad gäller tillämpligheten av 49 § b) personuppgiftslagen, som avser behandling av personuppgifter i strid med 13–21 §§ samma lag (dvs. känsliga personuppgifter) instämmer regeringen i redovisade remissinstansers bedömning. Trafikuppgifter torde alltså inte utgöra känsliga personuppgifter, såsom de definieras i personuppgiftslagen. Regeringens mening är dock att övriga redovisade straff- och skadeståndsrättsliga regler, sammantaget med den tillsynsreglering som redovisats, ger ett skydd mot kränkningar av den personliga integriteten vid otillåten och oaktsam behandling av trafikuppgifter som väl svarar mot direktivets krav på sanktioner som är effektiva, proportionerliga och avskräckande.

Härutöver bör nämnas att utredningen i fråga om ett eventuellt införande av en bestämmelse om grovt dataintrång har anfört att ett sådant övervägande inte kan göras enbart utifrån ett eventuellt behov av ytterligare straffrättsligt skydd för lagrade trafikuppgifter, utan kräver att hänsyn tas till betydligt fler omständigheter. Regeringen delar den bedömningen. Förslaget väcker frågor av såväl systematisk som lagteknisk karaktär och förutsätter en analys som det saknas beredningsunderlag för och som inte är möjlig att göra inom ramen för detta lagstiftningsärende.

Regeringen gör sammanfattningsvis bedömningen att det inte finns skäl att förändra befintliga straff- eller skadeståndsrättsliga bestämmelser i anledning av de nya reglerna om lagring av trafikuppgifter.

9 Fördelning av kostnaderna

9.1 Beräkning av kostnaderna

Regeringens bedömning: Kostnaderna för att genomföra lagringsskyldigheten och anpassningsskyldigheten kan beräknas uppgå till ca 200 miljoner kronor. Kostnaden för att lämna ut uppgifterna kan beräknas uppgå till ca 20 miljoner kronor årligen.

Utredningens bedömning överensstämmer med regeringens.

Remissinstanserna: Remissinstanserna har, med ett fåtal undantag, uppgett att de delar utredningens kostnadsbedömning eller lämnat den utan invändningar. *Rikspolisstyrelsen* har anfört att utredningen i sina beräkningar inte synes ha tagit med kostnaderna för en bemanning dygnet runt hos leverantörerna, en fråga som är mycket viktig för polisen. *Post- och telestyrelsen (PTS)* har uppgett att de i allt väsentligt håller med om utredningens redovisning av de kostnader som uppstår. De har dock velat lyfta fram att kostnaderna kommer att slå olika hårt mot olika leverantörer. *Stockholms handelskammare* har framfört att de anser att kostnadsfrågan bör utredas ytterligare. *Bahnhof AB* har anfört att

utredningen genomgående undervärderat förslagets ekonomiska implikationer och drar slutsatsen att förslaget i sin helhet är ekonomisk omöjligt att genomföra.

Skälen för regeringens bedömning: Utredningen har för beräkning av vilka kostnader förslaget kommer att leda till inhämtat uppgifter från ett stort antal aktörer. I utredningen påtalas dock svårigheterna att, bl.a. från leverantörerna, få tillgång till några mer precisa kostnadsberäkningar. Ett antal osäkerhetsmoment har också förelegat om den framtida utvecklingen, exempelvis har det varit svårt att uppskatta i vilken utsträckning leverantörerna kommer att välja att lagra sina uppgifter själva alternativt uppdra åt annan att utföra lagringen. Med dessa förbehåll har utredningen presenterat följande beräkningar.

När det inledningsvis gäller kostnaderna för att *identifiera och spara* de uppgifter som ska lagras kan dessa 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 är i förhållande till de nya kraven och storleken på leverantörens verksamhet. Enligt den analys av kostnaderna som utredningen 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 där de nya systemen har anpassats till de krav som gäller för lagring av trafikuppgifter. Utredningen har sammanfattningsvis bedömt att de totala kostnaderna för att identifiera och spara uppgifterna kan beräknas till omkring 100 miljoner kronor.

När det gäller kostnaderna för att *lagra* trafikuppgifterna har det beaktats 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 kraven på tillräckliga tekniska och organisatoriska säkerhetsåtgärder. För de leverantörer som har ett väl utbyggt och fungerande säkerhetssystem kommer kostnaderna troligen inte att bli särskilt betungande medan andra leverantörer kan behöva införa nya rutiner och system som medför kostnader. Det aktuella förslaget bygger på att varje enskild leverantör har det ansvar för lagringen som följer av lagringsskyldigheten. Förslaget öppnar även för en möjlighet för den enskilde leverantören att anlita någon annan att lagra uppgifterna. Utredningen har bedömt att kostnaderna för lagringen med en kostnadseffektiv lagring hos varje leverantör kan beräknas uppgå till sammanlagt omkring 100 miljoner kronor för hela branschen.

Vidare uppges, beträffande kostnaderna för att *lämna ut* trafikuppgifter, att dessa i stor utsträckning beror på verksamhetens omfattning, dvs. antalet kunder och antalet förfrågningar från brottsbekämpande myndigheter. Utredningen har, mot bakgrund av att fler uppgifter kommer att finnas lagrade, vid sin beräkning utgått ifrån en viss ökning av antalet fall där trafikuppgifter kommer att begäras ut och bedömt 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 har utredningen bedömt att kostnaderna för utlämnande av trafikuppgifter kommer att uppgå till omkring 20 miljoner kronor per år.

Sammanfattningsvis har utredningen gjort bedömningen att förslaget innebär att kostnaderna 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 bedömningar 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, uttryckt som intäkter från slutkund, som uppgick till drygt 50 miljarder kronor år 2009.

Remissinstanserna har med ett fåtal undantag inte haft några invändningar mot utredningens kostnadsberäkningar. *PTS* har exempelvis uppgett att de i allt väsentligt håller med om utredningens redovisning av de kostnader som uppstår. IT&Telekomföretagen presenterade emellertid i samband med utredningen en kostnadsuppskattning som, med utgångspunkten att förslaget avser lagring enligt direktivets minimikrav samt bemanning under kontorstid, uppgick till 760 miljoner kronor i engångskostnader (anpassning av systemen) samt 133 miljoner kronor i årliga kostnader (varav lagring 76 miljoner kronor och utlämnande 57 miljoner kronor). För det fall förslaget skulle innebära mer omfattande lagringskrav och/eller bemanning utanför kontorstid uppgavs kostnaderna öka väsentligt. Den uppskattade nivån 1 500 kr i ersättning för ett enskilt utlämnande ansåg IT&Telekomföretagen dock vara väl avvägd.

Regeringens bedömning är, med förbehåll för de osäkerhetsmoment som inledningsvis presenterats, att utredningens beräkningar är väl underbyggda och därmed bör kunna tas som utgångspunkt för ungefärligen vilka kostnader förslaget kommer att generera. Det bör i detta sammanhang noteras att utredningen vid sin bedömning utgick ifrån att uppgifterna skulle lagras under ett år, vilket innebär att det bör finnas viss marginal i kostnadsberäkningen då lagringstiden nu föreslås vara begränsad till sex månader.

Rikspolisstyrelsen har påtalat att utredningen i sina beräkningar inte verkar ha tagit hänsyn till kostnader för bemanning dygnet runt hos leverantörerna. Något sådant bemanningskrav ställs heller inte upp i regeringens förslag. Frågan behandlas närmare i avsnitt 7.4, där det anges att leverantörerna kan komma att behöva arbeta med verkställigheten även utanför kontorstid. Som utredningen konstaterat torde de större leverantörerna redan ha denna kapacitet. Vissa ökade kostnader kan uppstå för de mindre leverantörerna. Dessa bedöms dock rymmas inom de kostnadsramar utredningen angivit.

9.2 Kostnadsfördelningen

9.2.1 Hur ska kostnaderna för lagringsskyldigheten fördelas?

Regeringens förslag: Leverantörerna ska stå för kostnaderna för lagring, säkerhet och anpassning av systemen. Det allmänna ska ersätta leverantörerna för de kostnader som hänför sig till utlämnande av uppgifter i enskilda ärenden.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt eller har inte haft några invändningar mot utredningens förslag. *Riksdagens ombudsmän (JO), Stockholms handelskammare, Post- och telestyrelsen (PTS), Banverket, TeliaSonera AB, Teracom AB, IT&Telekomföretagen, Svenska Stadsnätsföreningen, Tele2 Sverige AB, Telenor Sverige AB* samt *Svenska Linuxföreningen* har avstyrkt förslaget att leverantörerna ska stå för delar av kostnaderna och anfört att samtliga kostnader bör läggas på staten. Det skäl som i första hand har framhållits är att de uppgifter som åläggs leverantörerna enbart är motiverade av rättsväsendets intresse och inte är till någon nytta för leverantörerna själva, varför det är orimligt att leverantörerna ska betala merparten av kostnaderna. Det anförs även att förslaget riskerar att medföra en tröskel för marknadsinträden samt i större utsträckning drabbar de mindre operatörerna, vilket har en negativ påverkan på såväl konkurrenssituationen som den tekniska utvecklingen. Även *Sveriges advokatsamfund* har ställt sig frågande till om det är rimligt att låta operatörerna bära kostnaden för lagringen och om denna kan anses stå i rimlig proportion till de eventuella effektivitetsvinster som genomförandet av direktivet kommer att medföra för de brottsutredande myndigheterna. .*SE* har uttryckt farhågor för att den föreslagna kostnadsmodellen kommer att fördyra tjänsterna för Internetanvändare, vilket kan komma att påverka utvecklingen av Internets användning. *JO* har efterlyst lagstiftarens syn på den princip som synes ha utvecklats att de som hanterar information som är potentiellt intressant för de brottsbekämpande myndigheterna åläggs att på egen bekostnad lagra informationen och dessutom göra det på ett sätt så att polisen enkelt och snabbt kan få tillgång till den. JO har vidare framfört att det är en nackdel från integritetssynpunkt att kostnaderna för användandet av trafikuppgifter på det föreslagna sättet ”osynliggörs” när dessa för de brottsbekämpande myndigheterna görs till en ekonomiskt så attraktiv metod.

Som alternativ till utredningens förslag har *PTS* föreslagit att aktörerna ersätts med en klumpsumma beräknad utifrån storleken på leverantören och typen av teknik leverantören har. *Tele2 Sverige AB* har som en medelväg föreslagit att det allmänna står för en schabloniserad kostnad att anpassa nätet i initialfasen och att operatörerna därefter får ta kostnaden för ny infrastruktur i samband med nyanläggning av nät eller tjänster. *Telenor Sverige AB* har föreslagit att staten ersätter operatörerna per kund och per tjänst för de investeringar som bedöms nödvändiga för lagringen samt inför ett kostnadsbaserat belopp för utlämnande av uppgifter.

Skälen för regeringens förslag

Tidigare överväganden när det gäller kostnadsfördelningen

Direktivet om lagring av trafikuppgifter reglerar inte frågan om hur kostnaderna som uppstår till följd av direktivets krav ska fördelas, utan lämnar denna fråga åt medlemsstaterna att besluta.

Enligt 6 kap. 19 § lagen om elektronisk kommunikation har vissa leverantörer redan i dag en skyldighet att anpassa sin verksamhet så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas.

När anpassningsskyldigheten infördes år 1996 i dåvarande telelagen begränsades den till att endast omfatta tillståndspliktiga leverantörer. Dessa skulle då 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. 29 f.) uttalades bl.a. att det finns en rad verksamhetsområden där samhället som förutsättning för att få idka näring kräver att vissa samhälleliga intressen beaktas. 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 förelåg någon avgörande principiell skillnad mellan dessa förpliktelser och en förpliktelse att på egen bekostnad anpassa telesystemen så att möjligheterna till hemlig teleavlyssning och hemlig teleövervakning bibehålls. Regeringen anförde vidare att hemlig teleavlyssning och hemlig teleövervakning inte kunde sägas inta någon särställning i detta hänseende endast på den grunden att det rörde sig om brottsbekämpande verksamhet. Istället framhölls att televerksamhet är så speciell att det är oundvikligt att ett relativt stort samhällsansvar måste följa med verksamheten. Regeringen uttryckte också att det redan fanns lagstadgade skyldigheter för företag att vidta vissa åtgärder för att underlätta den brottsbekämpande verksamheten. Som exempel nämndes bankernas uppgiftsskyldighet enligt dåvarande lagen 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.

Beredningen för rättsväsendets utveckling har därefter föreslagit en utvidgad anpassningsskyldighet för leverantörerna (SOU 2005:38 s. 278 f.). I det sammanhanget behandlade utredningen även frågan om hur kostnaderna för anpassningen skulle fördelas och föreslog att leverantörerna även i fortsättningen skulle stå för dessa kostnader. De skäl som angavs var huvudsakligen desamma som de regeringen anförde när anpassningsskyldigheten infördes.

Fördelning av kostnaderna

Som utredningen redovisat finns det tre möjliga sätt att fördela kostnaderna; att det allmänna står för samtliga kostnader, att leverantörerna står

för samtliga kostnader eller att kostnaderna fördelas mellan det allmänna och leverantörerna. Av dessa har utredningen föreslagit den sist nämnda modellen.

Som framgått av redovisade remissyttranden har kritik riktats mot utredningens förslag avseende fördelning av kostnaderna mellan leverantörerna och de brottsbekämpande myndigheterna. Kritiken har handlat främst om principfrågan om leverantörerna bör åläggas att bidra till finansieringen av en verksamhet som är till enbart för att tillgodose de brottsbekämpande myndigheternas intresse, men även behandlat frågor framför allt kring konkurrens. De konkurrensmässiga utgångspunkterna för genomförandet av direktivet har presenterats i avsnitt 5.2.

Vad avser nämnda principfråga gör regeringen följande bedömning. Som redogjorts för ovan bygger den nuvarande anpassningsskyldigheten i 6 kap. 19 § lagen om elektronisk kommunikation 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. Till grund för den ordningen har legat principiella överväganden om fördelningen av kostnaderna mellan det allmänna och leverantörerna när det gäller tillgång till viss del av leverantörernas verksamhet i brottsbekämpningen. Dessa överväganden, som har haft sin utgångspunkt i ställningstagandet att det finns verksamhetsområden där samhället som förutsättning för att få idka näring kräver att vissa samhälleliga intressen beaktas, har enligt regeringens mening giltighet även för bedömningen av hur kostnaderna för genomförandet av nuvarande förslag bör fördelas.

PTS, Tele2 Sverige AB och *Telenor Sverige AB* har lämnat olika förslag på hur leverantörerna skulle kunna ersättas för sina anpassningskostnader. Regeringen anser emellertid att den modell som redan gäller, där leverantörerna bekostar anpassning och drift av systemen, medan de brottsbekämpande myndigheterna ersätter leverantörerna när uppgifter lämnas ut, har stora fördelar. Med denna modell har den part som har möjlighet att påverka kostnaden också ansvar för den. Leverantörernas tekniska och administrativa kompetens på området utnyttjas, samtidigt som de har ett tydligt incitament att hålla kostnaderna för anpassning och drift nere. Med denna modell får de brottsbekämpande myndigheterna dessutom ett incitament att inhämta trafikuppgifter bara då man anser det vara en effektiv metod som kan förväntas föra utredningsarbetet framåt. En sådan modell blir således enligt regeringens mening mest samhällsekonomiskt kostnadseffektiv. Regeringen har förståelse för den synpunkt som framförts av *JO*, att den föreslagna fördelningen skulle vara olämplig eftersom kostnaderna ”osynliggörs”. Samtidigt bör understrykas att de brottsbekämpande myndigheterna enligt förslaget ska betala för de kostnader som uppstår vid varje enskilt utlämnande. Det innebär att kostnaderna för att inhämta uppgifterna blir tydliga och gör att myndigheterna i varje fall måste ta ställning till om inhämtande av trafikuppgifter utgör en effektiv utredningsmetod.

Regeringen anser sammanfattningsvis att kostnaderna för den lagringsskyldighet som nu är aktuell bör fördelas på samma sätt som enligt gällande ordning, dvs. att leverantörerna står för kostnaderna beträffande lagring, säkerhet och anpassning medan det allmänna ersätter leveran-

törerna när uppgifter lämnas ut. Detta inte minst mot bakgrund av att den lagrings- och anpassningsskyldighet som nu föreslås blir en del av det system som redan gäller enligt rättegångsbalken och lagen om elektronisk kommunikation.

9.2.2 Ersättningsnivån för utlämnande av trafikuppgifter

Regeringens förslag: Det informeras om att regeringen eller den myndighet regeringen bestämmer meddelar föreskrifter om ersättningen.

Utredningens förslag överensstämmer med regeringens.

Remissinstanserna: Flertalet remissinstanser har tillstyrkt eller har inte haft några invändningar mot utredningens förslag. *Teracom AB* har uppgett att de stödjer förslaget att en schablonavgift för varje förfrågan utgår och *Tele2 Sverige AB* har anfört att de anser det föreslagna sättet att bestämma ersättning för verkställighet vara väl avvägt. *Post- och telestyrelsen (PTS)* har emellertid invänt mot utredningens förslag och uppgett att den föreslagna uträkningen av en schablonavgift kommer att bli mycket komplicerad att utföra och att utsikten att kunna göra en rimlig beräkning som uppfyller de rättssäkerhetskrav som bör ställas är små. Myndigheten anser mot den bakgrunden att schablonersättningen inte bör ske i föreskriftsform. I stället förordas i första hand att ersättningsnivån förhandlas fram mellan de polisiära myndigheterna och leverantörerna. Även *Telenor Sverige AB* har anfört att det kan bli svårt att införa ett rättvist schablonbelopp och att nivån på ersättningen därför bör lösas direkt mellan operatörerna och de myndigheter som begär ut informationen, förslagsvis som en ersättning relaterad till antal kunder per tjänst. *IFPI Svenska Gruppen* och *Svenska Antipiratbyrån* har anfört att det är nödvändigt att schablonersättningen fastställs inom en rimlig tid så att inte ovissheten får en hämmande effekt på polisens utredningsarbete.

Skälen för regeringens förslag: Regeringen anser, i likhet med utredningen, att principerna för den ersättning som myndigheterna ska betala för utlämnande av trafikuppgifter bör vara att leverantörerna ska få sina kostnader för att lämna ut trafikuppgifter i enskilda ärenden ersatta. Det torde dock vara närmast ogörligt att exakt beräkna vad varje enskilt utlämnande av trafikuppgifter från leverantörerna till de brottsbekämpande myndigheterna kostar. Det rör sig om ett förhållandevis stort antal utlämnanden (se avsnitt 10) och kostnaderna varierar mycket mellan olika leverantörer, bl.a. beroende på vilka uppgifter som begärs ut och när verkställigheten ska ske. Om ersättningen skulle bestämmas för varje enskilt ärende skulle det också leda till stora administrativa kostnader för båda parter som riskerade 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.

Frågan är då hur dessa schabloner ska fastställas. Utredningen har föreslagit att tillsynsmyndigheten ska fastställa schablonerna och ge riktlinjer för vad som ska gälla i de situationer där det finns anledning att avvika från schablonerna genom föreskrifter. Detta förslag har fått stöd av ett

antal remissinstanser. *PTS* och *Telenor Sverige AB* har dock invänt mot förslaget och i stället föreslagit att ersättningsnivån ska förhandlas fram mellan de myndigheter som begär ut trafikuppgifter och leverantörerna. Deras förslag är i linje med den ordning som hittills har gällt, där ersättningen vid utlämnande av uppgifter har 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.

Utredningen har emellertid redovisat att det hittills har varit mycket svårt för Säkerhetspolisen och de största leverantörerna att komma överens, varför förhandlingarna har varit både resurskrävande och tidsödande. Säkerhetspolisen har generella avtal med mindre än en handfull leverantörer och det tog enligt uppgift mellan två och tre år av förhandlingar innan överenskommelserna nåddes. Mot denna bakgrund framstår alternativet att de brottsutredande myndigheterna och leverantörerna själva ska förhandla fram ersättningsnivån inte som en lämplig lösning. Regeringen delar utredningens bedömning att det skulle vara olyckligt med en ordning som innebar att mycket stora resurser såväl hos leverantörerna som hos de brottsbekämpande myndigheterna skulle behöva läggas ned för att bestämma ersättningsnivåer för olika typer av utlämnanden gentemot olika leverantörer. Ett system med schablonersättningar fastställda av tillsynsmyndigheten ger däremot en enkel och snabb handläggning för både leverantörer och de brottsbekämpande myndigheterna.

Även om fastställandet av ersättningsnivåerna, som PTS anfört, kommer att innebära svårigheter för myndigheten så ger schablonersättningar med förutbestämda nivåer över lag minskade administrationskostnader och möjliggör en effektiv handläggning. Det kan vidare noteras att såväl leverantörerna som de brottsbekämpande myndigheterna under utredningen ansåg att kostnaden i ett normalt ärende uppgick till 1 500–2 000 kr, en uppskattning i stort sett samtliga remissinstanser anslutit sig till.

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 motiverar och att de ibland får en lägre ersättning än vad som motsvarar deras kostnader. Om avvikelserna blir för stora bör dock kunna föreskrivas att schablonersättningen inte ska tillämpas, utan att en ersättning i stället ska bestämmas till ett belopp som motsvarar kostnaderna i det enskilda fallet.

För att ge de brottsbekämpande myndigheterna möjlighet att påverka hur schablonbeloppen bestäms 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.

10 Förslagets konsekvenser

10.1 Ekonomiska konsekvenser

Regeringens förslag innebär att ansvaret för de kostnader som uppstår 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 Post- och telestyrelsen (PTS) efter samråd med de brottsbekämpande myndigheterna samt med leverantörerna.

I dag fattar domstol beslut om hemlig teleövervakning i drygt 1 000 fall om året och polisen begär ut uppgifter med stöd av lagen om elektronisk kommunikation i omkring 9 500 fall. Eftersom förslaget innebär att trafikuppgifterna i viss ökad utsträckning kommer att vara tillgängliga vid begäran kan det förväntas att de brottsbekämpande myndigheterna kommer att begära ut trafikuppgifter i något ökad utsträckning i förhållande till vad som gäller, vilket kommer att leda till marginellt ökade handläggningskostnader.

I bedömningen av rättsväsendets kostnader måste emellertid också vägas in att vissa effektivitetsvinster för rättsväsendet torde uppstå i och med att allvarliga brott kan utredas och lagföras snabbare. Regeringen bedömer att 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. Utredningen har bedömt kostnaden för ersättning till leverantörerna vid utlämnande till 20 miljoner kronor, vilket väl överensstämmer med nivån på den ersättning som betalas till leverantörerna i dag. Ingen remissinstans har invänt mot utredningens bedömning i denna del.

Regeringen bedömer sammanfattningsvis att förslaget inte medför behov av att tillföra rättsväsendet ytterligare resurser.

Den myndighet som utöver rättsväsendet kommer att få ökade kostnader till följd av förslaget är PTS. Myndigheten har redan i uppdrag att utöva tillsyn enligt lagen om elektronisk kommunikation. I det uppdraget ingår att ha tillsyn över hur leverantörerna sparar, utplånar och avidentifierar trafikuppgifter enligt 6 kap. lagen om elektronisk kommunikation. PTS har dock hittills inte bedrivit någon särskilt omfattande verksamhet på det området. Myndigheten kommer med den nya regleringen att behöva lägga ner ytterligare 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 kommer bl. a. att behöva utfärda säkerhetsföreskrifter och föreskrifter om ersättning, pröva om det ska medges 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. Myndigheten har bedömt att verksamheten behöver tillföras ca 3 miljoner kronor det första året, ca 2 miljoner kronor det andra året och därefter knappt en miljon kronor årligen.

PTS:s verksamhet inom verksamhetsgrenen elektronisk kommunikation som bedrivs med stöd av lagen om elektronisk kommunikation finansieras med avgifter. Detta följer av 8 kap. 17 § samt förordningen (2003:767) om finansiering av PTS:s verksamhet. Ingen ändring föreslås för denna ordning. Det kan noteras att lagen om elektronisk kommunikation och den tillsynsverksamhet som PTS bedriver därutöver har inslag som avser nyttan av leverantörernas verksamhet för brottsbekämpningen (leverantörerna är bl.a. skyldiga att anpassa sina verksamheter så att beslut om hemlig teleavlyssning och hemlig teleövervakning kan verkställas). Vid varje åtgärd som kan resultera i högre avgifter för leverantörer måste den samlade avgiftsbördan beaktas. Regeringen bedömer dock att PTS:s utökade verksamhet på detta område i det här fallet ska finansieras genom ökade avgifter. Sammanfattningsvis kommer det alltså att ankomma på PTS att täcka de ökade kostnaderna genom avgifter.

10.2 Övriga konsekvenser

Utöver de ekonomiska konsekvenser som har presenterats ovan kommer ett genomförande av direktivet om lagring av trafikuppgifter att få konsekvenser för leverantörerna, bl.a. beträffande möjligheterna att konkurrera med de tjänster som de tillhandahåller. En redogörelse för dessa övriga konsekvenser har lämnats i de föregående avsnitten under respektive frågeställning. En särskild utredning beträffande förslagets samtliga konsekvenser har också sammanställts i en konsekvensutredning. För den sammantagna bilden av förslagets alla konsekvenser finns denna konsekvensutredning intagen som *bilaga 6*.

11 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag: Lagändringarna ska träda i kraft den 1 juli 2011.

Regeringens bedömning: Några övergångsbestämmelser bör inte införas.

Utredningens förslag och bedömning: Utredningen har föreslagit att lagändringarna ska träda i kraft den 1 januari 2009. Även utredningen har gjort bedömningen att några övergångsbestämmelser inte ska finnas.

Remissinstanserna: *Stockholms handelskammare, TeliaSonera AB, Teracom AB, IT&Telekomföretagen, Hi3G Access AB, Telenor Sverige AB* och *Swedish Network Users' Society (SNUS)* har anfört att den genomförandetid utredningen föreslagit är alltför kort. De anger att betydande förändringar kommer att behöva göras i de tekniska systemen, inte minst om en lösning väljs där leverantörerna åläggs lagringsskyldigheter som går utöver direktivets minimikrav. Det anförs av flera av de redovisade remissinstanserna att en övergångsperiod om minst ett år efter riksdagsbeslut behövs innan lagringskraven kan vara fullt genomförda, något som internationella erfarenheter visar. Det bör i detta

sammanhang också tas hänsyn till att en aktör som tror sig ha möjlighet att få dispens från lagringskravet rimligen inte ska behöva genomföra de ändringar som krävs innan en dispensansökan har handlagts.

Skälen för regeringens förslag och bedömning: Regeringens förslag går ut på att direktivet om lagring av trafikuppgifter nu genomförs i svensk rätt. Europeiska unionens domstol har i dom den 4 februari 2010 konstaterat att Sverige inte i rätt tid genomfört den del av direktivet som skulle ha varit genomförd senast den 15 september 2007. Mot denna bakgrund, samt då lagrade trafikuppgifter utgör ett mycket viktigt verktyg vid avslöjande, utredning och lagföring av allvarlig brottslighet är det angeläget att de nya reglerna träder i kraft snarast möjligt.

Regeringen delar de remissynpunkter som framförts om att det är rimligt att leverantörerna får viss tid på sig att anpassa sin verksamhet till de nya kraven. I detta sammanhang bör dock beaktas att direktivet har funnits på plats sedan mars 2006 och utredningen sedan november 2007. Därigenom har grundförutsättningarna för vilka krav leverantörerna kommer att åläggas varit kända under lång tid. Regeringens förslag följer också till allra största del direktivets minimikrav. Eftersom Sverige är bland de sista länderna inom EU att genomföra direktivet har leverantörerna även haft möjlighet att studera och dra nytta av erfarenheter från leverantörer i andra medlemsstater och av den teknik som utvecklats där. Mot denna bakgrund anser regeringen att det är rimligt att lagändringarna träder i kraft den 1 juli 2011.

Regeringen bedömer inte heller att några särskilda övergångsbestämmelser bör införas. Lagringskravet kommer att införas samtidigt som möjligheten kommer att finnas att söka dispens från denna skyldighet hos tillsynsmyndigheten. Det är en konsekvens som följer av föreslagna regler och tillsynsmyndigheten får ta ställning till om sådana synnerliga skäl föreligger att dispens ska ges.

12 Författningskommentar

12.1 Förslaget till lag om ändring i rättegångsbalken

27 kap.

25 §

Har rätten lämnat tillstånd till hemlig teleavlyssning eller hemlig teleövervakning, får de tekniska hjälpmedel som behövs för avlyssningen eller övervakningen användas.

I *6 kap.* lagen (2003:389) om elektronisk kommunikation finns bestämmelser om hemlig teleavlyssning och hemlig teleövervakning som gäller för den som driver verksamhet som avses i den lagen.

Paragrafen innehåller bestämmelser som ger den som har fått tillstånd till hemlig teleavlyssning eller hemlig teleövervakning befogenheter att kunna verkställa åtgärderna och en hänvisning till lagen om elektronisk kommunikation.

I *andra stycket* görs en hänvisning till nät- och tjänsteleverantörers skyldigheter enligt lagen om elektronisk kommunikation att driva

verksamheten på visst sätt. Genom de nya paragrafer som föreslås i 6 kap. lagen om elektronisk kommunikation, 16 a–16 f §§, införs ytterligare bestämmelser om hur verksamheten ska drivas för att hemlig teleövervakning ska kunna verkställas. Hänvisningen justeras därför till att omfatta hela 6 kap.

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

6 kap. ***Behandling av trafikuppgifter samt*** **integritetsskydd**

1 §

I detta kapitel avses med

elektroniskt meddelande: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst, utom information som överförs som del av sändningar av ljudradio- och TV-program som är riktade till allmänheten via ett elektroniskt kommunikationsnät om denna information inte kan sättas i samband med den enskilde abonnenten eller användaren av informationen,

Internetåtkomst: möjlighet till överföring av ip-paket som ger användaren tillgång till Internet,

meddelandehantering: utbyte eller överföring av elektroniskt meddelande som inte är samtal och inte heller är information som överförs som del av sändningar av ljudradio- och TV-program,

misslyckad uppringning: uppringning som kopplas fram utan att nå en mottagare,

telefoni: elektronisk kommunikationstjänst som innebär möjlighet att ringa upp eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan,

trafikuppgift: uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande.

Begreppen *behandling, personuppgiftsansvarig* och *samtycke* har i kapitlet samma innebörd som i personuppgiftslagen (1998:204).

Ändringarna, som innebär införande av definitioner av särskilda begrepp som används i 6 kap., har behandlats i avsnitt 6. I paragrafens *första stycke* införs de nya definitionerna *Internetåtkomst, meddelandehantering, misslyckad uppringning* och *telefoni.*

Med *Internetåtkomst* avses möjligheten att överföra s.k. ip-paket med hjälp av olika tekniker. Med ip-paket avses ett telekommunikationspaket med data som ska överföras, vilket bland annat innehåller uppgifter om vilken eller vilka ip-adresser som används. Själva tekniken eller kapaciteten som tillhandahålls för att få Internetåtkomst utgörs av anslutningsformen, som faller utanför definitionen av Internetåtkomst (se vidare kommentaren till 16 a §).

Definitionen av *meddelandehantering* omfattar utbyte eller överföring av samtliga elektroniska meddelanden som inte är samtal eller information som överförs som del av sändningar av ljudradio- och TV-program. Med detta avses exempelvis elektronisk post, sms (Short Message Service) och mms (Multimedia Messaging Service). Vad som i lagen avses med begreppet *samtal* framgår av 1 kap. 7 §.

Misslyckad uppringning omfattar enligt den givna definitionen såväl den situationen att någon ringer och kopplas fram men ingen svarar på uppringningen som den situationen att det har skett ett ingrepp i driften i kommunikationsnätet så att en uppringning kopplas fram utan att nå mottagaren. I det sistnämnda fallet kan den som försöker ringa få ett meddelande om att abonnenten för tillfället inte kan nås. Ett uppringning som når fram till en röstbrevlåda anses däremot inte som en misslyckad uppringning utan som en fullbordad sådan. Vidare omfattar definitionen inte den situationen att en uppringning, exempelvis på grund av tekniskt fel, över huvud taget inte kopplas fram. Misslyckad uppringning innebär enligt den givna definitionen således att information överförs. Begreppet omfattas därmed av den definition av *elektroniskt meddelande* som återfinns i paragrafen, förutsatt att även övriga kriterier som ställs upp i denna definition är uppfyllda.

Definitionen av *telefoni* ansluter till hur telefonitjänst definieras i 1 kap. 7 §. Definitionen telefonitjänst är generell för hela lagens tillämpning. Enligt den definitionen måste det emellertid även kunna gå att genomföra nödsamtal för att kommunikationstjänsten ska anses vara telefoni. Kravet på möjlighet till nödsamtal finns inte med i den definition av telefoni som här ges. Anledningen till detta är att vissa Internettelefonitjänster inte alltid medger att nödsamtal genomförs. Även sådana telefonitjänster som inte ger möjlighet till nödsamtal omfattas således av den här givna definitionen. Det ska påpekas att denna definition av telefoni endast är avsedd att tillämpas när det gäller den skyldighet att lagra uppgifter som följer av 16 a §. I vissa bestämmelser i 6 kap. används begreppet telefonitjänst (14 §, 19 § första stycket 2 a och 24 § 2). Innebörden av det begreppet följer definitionen av telefonitjänst som ges i 1 kap. 7 §.

I begreppet telefoni ingår såväl fast som mobil telefoni och Internettelefoni. Mobil telefoni innebär att telefonitjänsten använder en mobil nätanslutningspunkt. Internettelefoni använder ytterligare en annan teknik för överföring av uppgifter, nämligen överföring av uppgifter via Internet med användande av s.k. ip-paket.

3 a §

Den som är skyldig att lagra uppgifter enligt 16 a § ska vidta särskilda tekniska och organisatoriska åtgärder för att skydda de lagrade uppgifterna vid behandling.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om säkerhetsåtgärder enligt första stycket.

Paragrafen, som är ny, har behandlats i avsnitt 8.1.

I bestämmelsen regleras skyldigheten för nät- och tjänsteleverantörer att vidta åtgärder för att säkerställa att behandlade uppgifter skyddas mot integritetsintrång. Det kan t.ex. röra sig om skydd mot obehörig avlyssning.

I *första stycket* föreskrivs ett strängare krav för skyddet av de uppgifter som lagras för brottsbekämpande syften enligt 16 a § än vad som enligt 3 § gäller för uppgifter som sparats för andra ändamål. Skillnaden i den säkerhetsnivå som leverantörerna ska ha jämfört med de skyldigheter som följer av 3 § anges genom uttrycket ”särskilda åtgärder för att

skydda de lagrade uppgifterna", i stället för uttrycket "lämpliga åtgärder", som används i 3 §. Den nya bestämmelsen lämnar således inte något utrymme att bestämma säkerhetsnivån genom en avvägning mellan teknik, kostnader och risken för integritetsintrång. Istället måste tekniska och organisatoriska åtgärder vidtas av leverantörerna som säkerställer att uppgifterna skyddas vid behandling. Innebörden av det utökade kravet på skyddsåtgärder är bl.a. att leverantörerna ska säkerställa att de uppgifter som lagras bibehåller en hög kvalitet då de behandlas och att det finns ett skydd mot integritetsintrång.

I *andra stycket* bemyndigas regeringen eller den myndighet som regeringen bestämmer att komplettera bestämmelsen med ytterligare föreskrifter om säkerheten.

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, 13*, 16 a eller 16 c §.*

I bestämmelsen återfinns huvudregeln om behandling av trafikuppgifter. Den innebär att när en sådan uppgift inte längre behövs för att överföra ett elektroniskt meddelande måste uppgiften utplånas eller avidentifieras. Paragrafen har kompletterats med en hänvisning till 16 a och 16 c §§ om lagringsskyldighet för brottsbekämpande syften och behandling av dessa trafikuppgifter. Dessa bestämmelser utgör undantag från huvudregeln. Enligt 16 d § ska trafikuppgifter som lagras för brottsbekämpande syften utplånas vid utgången av lagringstiden. I det fallet räcker det således inte med att uppgifterna avidentifieras. Frågan om lagringstid och utplåning av uppgifter har behandlats i avsnitt 6.5.

Lagring och annan behandling av trafikuppgifter m.m. för brottsbekämpande syften

16 a §

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

Skyldigheten att lagra uppgifter enligt första stycket omfattar uppgifter som genereras eller behandlas vid telefoni, meddelandehantering, Internetåtkomst och tillhandahållande av kapacitet för att få Internetåtkomst (anslutningsform). Även vid misslyckad uppringning gäller skyldigheten att lagra uppgifter som genereras eller behandlas.

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

Regeringen eller den myndighet som regeringen bestämmer meddelar närmare föreskrifter om vilka uppgifter som ska lagras enligt denna bestämmelse.

Rubriken och paragrafen är nya.

Rubriken omfattar de nya bestämmelserna i 16 a–16 f §§. Begreppet *trafikuppgift* definieras i 1 § som en 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 omfattas av skyldigheten att lagra uppgifter enligt 16 a §, t.ex. uppgifter om Internetanslutning och om typ av kapacitet för överföring, varför ett ”m.m.” lagts till efter ”trafikuppgifter”.

I *första stycket* regleras vilka leverantörer som ska vara lagringsskyldiga. Frågan har behandlats i avsnitt 7.2. Lagringsskyldigheten ansluter till anmälningsplikten som regleras i 2 kap. 1 §. Det innebär att den som bedriver en anmälningspliktig verksamhet enligt 2 kap. 1 § också är skyldig att lagra sådana uppgifter som anges i bestämmelsen. Lagringsskyldigheten gäller därmed leverantörer av allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning och av allmänt tillgängliga elektroniska kommunikationstjänster. I 16 b § ges en möjlighet för tillsynsmyndigheten att i enskilda fall medge undantag från skyldigheten att lagra uppgifter enligt denna bestämmelse. Att leverantörer som bedriver enligt yttrandefrihetsgrundlagen skyddad verksamhet i form av trådsändningar inte kommer att omfattas av skyldigheten att lagra trafikuppgifter följer redan av att de enligt 2 kap. 2 § inte är anmälningspliktiga.

I första stycket regleras också lagringsskyldighetens omfattning. Frågan har behandlats i avsnitt 6.1 och 6.2. Sådana uppgifter som anges i 20 § första stycket 1 och 3 ska lagras, dvs. dels uppgifter om abonnemang, dels andra uppgifter som angår ett särskilt elektroniskt meddelande. Som anförts i kommentaren till 1 § första stycket omfattas även misslyckad uppringning av begreppet elektroniskt meddelande, eftersom viss information överförs trots att samtalet inte når någon mottagare. Uppgifter om sådan information ska alltså också lagras i enlighet med bestämmelsen. Däremot ska uppgifter om innehållet i ett elektroniskt meddelande inte lagras (20 § första stycket 2). Sådana uppgifter som är nödvändiga för att spåra och identifiera kommunikationskällan, slutmålet för kommunikationen, datum, tidpunkt och varaktighet för kommunikationen, typen av kommunikation, kommunikationsutrustningen samt lokaliseringen av mobil kommunikationsutrustning vid kommunikationens början och slut ska lagras.

Genom *andra stycket* preciseras lagringsskyldighetens omfattning. Lagringsskyldigheten förutsätter att den enskilde leverantören genererar eller behandlar uppgiften. Övervägandena i denna del har redovisats i avsnitt 6.1. 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 § personuppgiftslagen, 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 en uppgift någon gång finns hos leverantören, även om det bara rör sig om en ytterst kort tid, ska den lagras.

I andra stycket anges också för vilka kategorier lagringsskyldigheten gäller, närmare bestämt telefoni, meddelandehantering, Internetåtkomst och anslutningsform. Med *anslutningsform* avses själva tekniken eller kapaciteten som tillhandahålls för att få Internetåtkomst. Exempel på anslutningsform är DSL (Digital Subscriber Line), fiberoptiska anslutningar, 3G (UMTS), GSM (GPRS), vanliga traditionella telefonmodem och WLAN (trådlöst nät). Denna fråga har behandlats i avsnitt 6.3. I andra stycket regleras vidare att lagringsskyldigheten avseende uppgifter som genererats eller behandlats även omfattar misslyckad uppringning. Övervägandena i den frågan finns i avsnitt 6.4. Frågan berörs även i kommentaren till första stycket. Besök på webbsidor (”surfning”), besök på ”chattsidor” (”chattrum”) och användning av File Transfer Protocol (FTP, t.ex. överföring eller nedladdning av filer), är exempel på tjänster som faller utanför lagringsskyldighetens räckvidd.

Enligt *tredje stycket* ges den som är skyldig att lagra uppgifter enligt bestämmelsen en möjlighet att uppdra åt annan att fullgöra lagringen. Denna fråga har behandlats i avsnitt 7.1. Behandling av personuppgifter när annan anlitas för lagringen regleras i 30 § första stycket personuppgiftslagen. Den som anlitas benämns personuppgiftsbiträde. Av bestämmelsen följer att behandlingen av uppgifterna ska ske enligt instruktioner från den ansvarige. Även om lagringen således kan uppdras åt någon annan har den som är skyldig att lagra uppgifterna alltid kvar alla de skyldigheter gentemot myndigheter och enskilda som gäller för lagringen och behandlingen. De brottsbekämpande myndigheterna ska alltid kunna vända sig till den som enligt bestämmelsen är skyldig att lagra uppgifterna med en begäran om utlämnande. Ett utlämnande får inte fördröjas på grund av ett avtal med annan om lagringen (se även kommentaren till 16 f §).

I *fjärde stycket* lämnas en upplysning om att verkställighetsföreskrifter, som preciserar vilka uppgifter som ska lagras enligt bestämmelsen, meddelas av regeringen eller den myndighet som regeringen bestämmer.

16 b §

Tillsynsmyndigheten får i enskilda fall besluta om undantag från skyldigheten att lagra uppgifter enligt 16 a §, om det finns synnerliga skäl. Beslutet får förenas med villkor.

Beslutet om undantag får återkallas om villkoren i beslutet inte har följts eller det finns andra särskilda skäl.

Paragrafen, som är ny, har behandlats i avsnitt 7.2.

I *första stycket* ges tillsynsmyndigheten (Post- och telestyrelsen) en möjlighet att i enskilda fall medge undantag från lagringsskyldigheten som följer av 16 a §, om det finns synnerliga skäl. Vid prövningen av om undantag ska medges får en avvägning göras mellan nyttan för brottsbekämpningen av att leverantören lagrar trafikuppgifterna och kostnaderna eller andra negativa effekter som lagringsskyldigheten innebär för leverantören. Möjligheten att medge undantag från lagringsskyldigheten ska tillämpas restriktivt. Ett beslut om undantag får förenas med

villkor. Exempelvis kan ett villkor vara kopplat till verksamhetens omfattning.

Av *andra* stycket följer att ett beslut om undantag får återkallas om villkoren i beslutet inte har följts eller det finns andra särskilda skäl. Det kan exempelvis handla om en situation då leverantören efter beslutet erhåller ett stort antal kunder eller att de brottsbekämpande myndigheterna uppmärksammar en tendens att kriminella personer söker sig till en viss leverantör som är undantagen från lagringsskyldigheten.

Post- och telestyrelsens beslut i fråga om undantag får enligt 8 kap. 19 § överklagas hos allmän förvaltningsdomstol. Vid överklagande till kammarrätten krävs prövningstillstånd.

16 c §

Uppgifter som lagrats enligt 16 a § får behandlas endast för att lämnas ut enligt 22 § första stycket 2 eller 3 eller enligt 27 kap. 19 § rättegångsbalken.

Paragrafen, som är ny, har behandlats i avsnitt 7.3. I bestämmelsen regleras för vilka ändamål uppgifter som har lagrats enligt 16 a § får behandlas.

Uppgifter som har lagrats med stöd av 16 a § får, utöver den behandling som utgörs av lagringen hos leverantören eller hos någon som fått i uppdrag av leverantören att lagra uppgifterna, behandlas endast i två situationer; för att lämnas ut till brottsbekämpande myndigheter enligt 22 § första stycket 2 eller 3 eller för att lämnas ut enligt ett beslut om hemlig teleövervakning enligt 27 kap. 19 § rättegångsbalken. Ingen annan behandling av uppgifterna är tillåten innan de ska utplånas enligt 16 d §, inte ens behandling som syftar till att förhindra och avslöja obehörig användning av ett nät eller en tjänst. Vad som avses med begreppet behandling utvecklas närmare i kommentaren till 16 a §.

Bestämmelsens reglering hindrar inte att uppgifter som lagras enligt 16 a § även lagras enligt de allmänna bestämmelserna i 5, 6 och 8 §§. Den begränsar inte heller hur uppgifter som har lagrats enligt de allmänna bestämmelserna får behandlas. Av bestämmelsen följer däremot att den lagringsskyldige måste se till att lagringen redan från början sker på ett sätt som gör att det står klart för vilket eller vilka syften en viss uppgift lagras. Det måste alltså redan från början vara möjligt för en utomstående, exempelvis tillsynsmyndigheten, att avgöra för vilket eller vilka syften en uppgift är lagrad.

16 d §

Lagring enligt 16 a § ska pågå under sex månader från den dag kommunikationen avslutades. Därefter ska den som är skyldig att lagra uppgifterna utplåna dem.

Om uppgifterna har begärts utlämnade inom den i första stycket angivna tidsfristen, men ännu inte har lämnats ut, ska uppgifterna lagras till dess att ett utlämnande har skett. Därefter ska uppgifterna utplånas av den som är skyldig att lagra dem.

Paragrafen, som är ny, har behandlats i avsnitt 6.5. I bestämmelsen regleras lagringstidens längd och de åtgärder som ska vidtas från leverantörens sida vid lagringstidens slut.

Lagringstidens längd är enligt paragrafens *första stycke* sex månader från det datum kommunikationen avslutades. Vid telefoni och meddelandehantering blir kommunikationens slut utgångspunkten för lagringstidens beräkning. Utgångspunkten vid Internetåtkomst blir i stället avloggningen och vid anslutningsform när abonnemanget eller avtalet upphör. Vid lagringstidens slut ska uppgifterna utplånas. Oavsett om lagringen sker hos den lagringsskyldige leverantören själv eller denne har uppdragit åt annan att utföra lagringen i enlighet med 16 a § tredje stycket, ligger ansvaret för att utplåna uppgifterna alltid hos den som är lagringsskyldig (se kommentaren till 16 a §).

Av paragrafens *andra stycke* följer att om en uppgift har begärts ut från leverantören under de sex månader lagringen pågår, men ännu inte hunnit lämnas ut till myndigheten innan lagringstidens utgång, ska leverantören inte utplåna uppgiften förrän efter att ett utlämnande har skett. Därefter ska uppgiften på samma sätt som anges i första stycket utplånas hos den lagringsskyldige leverantören eller hos den som på dennes uppdrag lagrar uppgifterna.

16 e §

Den som är skyldig att lagra uppgifter enligt 16 a § har rätt till ersättning när lagrade uppgifter lämnas ut. Ersättningen ska betalas av den myndighet som har begärt uppgifterna.

Regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om ersättningen som avses i första stycket.

Paragrafen, som är ny, har behandlats i avsnitt 9.2.

I paragrafen ges enligt *första stycket* de som är skyldiga att lagra uppgifter enligt 16 a § rätt till ersättning för kostnader som uppstår vid utlämnande av de lagrade uppgifterna enligt 22 § första stycket 2 och 3 samt 27 kap. 19 § rättegångsbalken.

Det är den myndighet som har begärt uppgifterna som ska betala ersättningen. Det är inte meningen att ersättning ska utgå för varje utlämnad uppgift utan bestämmelsen innebär att ersättning ska betalas för varje begäran, alltså först när de uppgifter som hänför sig till en viss begäran har lämnats ut.

I *andra stycket* lämnas en upplysning om att regeringen eller den myndighet som regeringen bestämmer meddelar föreskrifter om ersättningen.

16 f §

Den som är skyldig att lagra uppgifter enligt 16 a § ska bedriva verksamheten så att uppgifterna kan lämnas ut utan dröjsmål och informationen enkelt kan tas om hand samt så att verkställandet inte röjs.

Paragrafen, som är ny, har behandlats i avsnitt 7.4.

I bestämmelsen anges vilka krav som ställs på leverantörerna vid verkställandet av en begäran om utlämnande. Det anges att uppgifterna ska lämnas ut utan dröjsmål. Utgångspunkten är att arbetet med att överföra information med anledning av en begäran som inkommer under kontorstid ska inledas inom mycket kort tid. Leverantören kan också komma att behöva arbeta med verkställigheten utanför kontorstid. Om det tar olika lång tid att få fram uppgifterna ur leverantörens system, bör

utlämnandet ske successivt så snart uppgifterna blir tillgängliga för leverantören. Hur snabbt ett utlämnande ska ske i det enskilda fallet är en fråga som får avgöras av den aktuella brottsbekämpande myndigheten och leverantören i varje situation.

I bestämmelsen anges också att de som är lagringsskyldiga enligt 16 a § ska bedriva verksamheten så att informationen enkelt kan tas om hand. Det innebär att de brottsbekämpande myndigheterna utan ansträngning ska kunna ta del av uppgifterna även om de skulle vara exempelvis krypterade eller komprimerade. Uppgifterna måste dock alltid överlämnas på ett sådant sätt att säkerheten och skyddet för uppgifterna inte eftersätts. Verksamheten måste också bedrivas på ett sådant sätt att verkställandet inte röjs.

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) 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, 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.

---

[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.

[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.

(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.

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

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

(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,

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

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

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.

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.

(*) EUT L 105, 13.4.2006, s. 54."

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.

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 kommissionen 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 samband 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 Internetåtkomst, 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.

Sammanfattning av betänkandet Lagring av trafikuppgifter för brottsbekämpning (SOU 2007:76)

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 brottsbekämpningen.

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 Internet-tjänsten,
- 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 Internet-telefoni 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 lagrings-skyldigheten 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 tillsyns-myndigheten 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 integritetskänsliga 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 föreläggganden 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.

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.

Betänkandets lagförslag

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	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 §.

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.

Förteckning över remissinstanserna

Följande remissinstanser har inkommit med yttranden över betänkandet: Riksdagens ombudsmän, Svea hovrätt, Stockholms tingsrätt, Sundsvalls tingsrätt, Kammarrätten i Göteborg, Länsrätten i Skåne län, Justitiekanslern, Domstolsverket, Åklagarmyndigheten, Ekobrottsmyndigheten, Rikspolisstyrelsen, Säkerhetspolisen, Registernämnden, Kriminalvårdsstyrelsen, Brottsförebyggande rådet, Brottsoffermyndigheten, Stockholms handelskammare, Försvarsmakten, Försvarets radioanstalt, Krisberedskapsmyndigheten, Kustbevakningen, Försvarets underrättelsenämnd, Tullverket, Skatteverket, Datainspektionen, Statskontoret, Juridiska fakultetsnämnden vid Stockholms universitet, Kungliga Tekniska högskolan, Juridiska fakultetsnämnden vid Lunds universitet, Konsumentverket, Post- och Telestyrelsen, Banverkets Telenät, Konkurrensverket, TeliaSonera AB, Teracom AB, Sveriges advokatsamfund, Svenskt Näringsliv, Svenska journalistförbundet, Svenska Bankföreningen, Svenska polisförbundet, Amnesty International, VINNOVA, Mälarenergi AB, IT&Telekomföretagen, Svenska Stadsnätsföreningen, Hi3G Access AB, Tele2 i Sverige AB, Telenor AB, Bahnhof AB, SNUS (Swedish Network Users' Society), .SE, Net Insight AB, IFPI Svenska Gruppen, Svenska Antipiratbyrån, Konstnärliga och Litterära Yrkesutövares Samarbetsnämnd (KLYS) och Svenska Linuxföreningen.

Följande remissinstanser har avstått från att yttra sig: SOS Alarm Sverige AB, Vattenfall, Sveriges Kommuner och Landsting, Svenska Avdelningen av Internationella Juristkommissionen, Svenska Helsingforskommittén för Mänskliga rättigheter, Näringslivets Telekomförening, Sveriges Internetoperatörers Forum, Stokab AB, TDC Song AB, IPOnly, Lidén Data Gruppen AB, Com hem AB, Cisco Sverige AB, Packetfront Systems AB, Netnod, ISOC-SE, BSA Sverige, Svenska Artisters och Musikers Intresseorganisation (SAMI) och Svenska Tonsättares Internationella Musikbyrå (STIM).

Utöver de som uttryckligen anmodats eller beretts tillfälle till det har ett yttrande även inkommit från tre privatpersoner.

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

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.

Konsekvensutredning

Bakgrund

Uppgifter om användningen av elektronisk kommunikation är värdefulla för att utreda, avslöja och åtala brott. Lagring av trafikuppgifter för viss typ av kommunikation har i många av Europeiska unionens (EU) medlemsstater visat sig vara ett nödvändigt och effektivt redskap för de brottsbekämpande myndigheterna, framför allt när det gäller utredningen av allvarliga brott som organiserad brottslighet och terrorism. Både praktisk erfarenhet och forskning har visat på vikten av trafikuppgifter för utredande av brott.

I betänkandet Tillgång till elektronisk kommunikation i brottsutredningar m.m. (SOU 2005:38), redogörs ingående för i vilken omfattning trafikuppgifter används (se s. 322–325). Av denna redogörelse kan följande framhållas. Uppgifterna inhämtas i stort sett i varje utredning om allvarlig brottslighet som mord, våldtäkt, grovt narkotikabrott eller terroristbrott. I ett inledande skede av utredningen inhämtas trafikuppgifter som genererats i anslutning till en brottsplats. Uppgifterna tillsammans med annan information gör det möjligt för polisen att ”lägga pussel” och på så sätt ringa in personer som kan misstänkas. Genom trafikuppgifter, t.ex. från mobiltelefoner, kan polisen kartlägga hur ett brott planerats och genomförts, men även hur de misstänkta agerat efter att de genomfört ett brott, t.ex. vilka flyktvägar som använts. Uppgifterna kan också många gånger resultera i att personer helt avförs från en utredning. Beträffande Internetrelaterad brottslighet är utgångsläget ofta att ingen misstänkt person finns och att tillgången till trafikuppgifter är det enda sätt polisen kan komma en misstänkt på spåren. Sammanfattningsvis anges i betänkandet att tillgången till trafikuppgifter är av helt avgörande betydelse för att utreda viss typ av brottslighet. I Trafikuppgiftsutredningens betänkande (SOU 2007:76) har myndigheterna också lämnat exempel på konkreta fall där trafikuppgifter varit av stort värde för utredningen; t.ex. i utredningar om allvarliga vålds-, sexual- och tillgreppsbrott (se s. 33 f.).

Efter bombattentaten i Madrid den 11 mars 2004 fick rådet för rättsliga och inrikes frågor (RIF) i uppdrag av Europeiska rådet att snarast anta gemensamma åtgärder i fråga om lagring av trafikuppgifter.

Europaparlamentet och rådet antog den 15 mars 2006 direktivet 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.

Direktivet syftar till att harmonisera medlemsstaternas regler om vissa skyldigheter för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster och allmänna kommunikationsnät att lagra vissa uppgifter som genereras eller behandlas i samband med att en kommunikation sker med fast eller mobil telefoni, eller i viss omfattning på Internet. De uppgifter som avses i direktivet är trafik- och lokaliseringsuppgifter samt de uppgifter som behövs för att identifiera en abonnent eller användare. Direktivet gäller uppgifter om såväl fysiska som juridiska personer samt uppgifter som är nödvändiga för att kunna identifiera

abonnenten eller den registrerade användaren. Däremot är direktivet inte tillämpligt på innehållet i kommunikationen.

Flera av EU:s medlemsstater har sedan tidigare lagstiftning om skyldighet för leverantörer av kommunikationstjänster att lagra trafikuppgifter. Lagstiftningen skiljer sig dock åt mellan medlemsstaterna. Skillnader i rättsliga och tekniska bestämmelser om lagring av trafikuppgifter utgör hinder för den inre marknaden för elektronisk kommunikation. Tjänsteleverantörerna ställs inför olika krav när det gäller vilken typ av uppgifter som ska lagras och vilka villkor som gäller för lagringen. Målet med direktivet är följaktligen att harmonisera leverantörernas skyldighet att lagra uppgifter och säkerställa att de är tillgängliga för utredning av brott. Direktivet syftar dock inte till att harmonisera tekniken för lagring av uppgifter. Det är en fråga som får lösas på nationell nivå.

Alternativ till lagreglering

Möjligheterna för brottsbekämpande myndigheter att få tillgång till trafikuppgifter är i dag beroende av vilka uppgifter som leverantörerna har lagrat för andra syften, t.ex. för fakturering och marknadsföring. Vilka uppgifter som lagras och den tid de lagras styrs alltså av helt andra faktorer än de brottsbekämpande myndigheternas behov. Utvecklingen inom området elektronisk kommunikation innebär också att nät- och tjänsteleverantörer i framtiden inte kan förväntas behöva lagra uppgifter för sin egen verksamhet i lika stor utsträckning som tidigare. Det medför att möjligheterna för brottsbekämpande myndigheter att få tillgång till dessa uppgifter kan komma att minska om någon lagringsskyldighet inte införs.

Sveriges medlemskap i EU innebär att det finns en skyldighet att genomföra direktiv i nationell rätt. Enligt direktivet skulle medlemsstaterna senast den 15 september 2007 ha genomfört bestämmelserna i nationell rätt. När det gäller Internetåtkomst, e-post och Internettelefoni fanns en möjlighet att skjuta upp genomförandet av direktivet till och med den 15 mars 2009. Den möjligheten har Sverige utnyttjat.

I maj 2006 gavs en utredare i uppdrag att lämna förslag till hur direktivet om lagring av trafikuppgifter ska genomföras i svensk rätt. Trafikuppgiftsutredningens förslag överlämnades till regeringen i november 2007. Förslaget har remissbehandlats.

Ett genomförande av direktivet om lagring av trafikuppgifter innebär att olika intressen ställs mot varandra; de brottsbekämpande myndigheternas behov av effektiva verktyg för att kunna utreda brott ställs mot intresset av att skydda enskildas integritet. Vid utformningen av direktivet har hänsyn tagits till dessa intressen och en avvägning mellan dem har gjorts, men även genomförandet av direktivet föranleder att dessa aspekter beaktas. Detsamma gäller den inverkan direktivet har på möjligheterna att konkurrera på lika villkor. Direktivet innebär inga förändringar när det gäller under vilka förutsättningar trafikuppgifter får lämnas ut i respektive medlemsstat, men vissa utgångspunkter anges i direktivet.

De som berörs av regleringen

Lagringsskyldigheten åläggs samtliga leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät. Post- och telestyrelsen (PTS) ska dock i enskilda fall få besluta om undantag från lagringskravet. Undantagsmöjligheten är avsedd för verksamheter som är av så liten omfattning och har ett så begränsat intresse ur ett brottsbekämpande perspektiv att det skulle vara oproportionerligt att kräva att leverantören som bedriver verksamheten helt eller delvis ska lagra trafikuppgifter på det sätt som direktivet kräver.

Trafikuppgifter är uppgifter om korrespondens och ett genomförande av direktivet berör därför alla som kommunicerar via telefoni och Internet. Direktivet gäller trafikuppgifter om såväl fysiska som juridiska personer samt uppgifter som är nödvändiga för att kunna identifiera abonnenten eller den registrerade användaren. De brottsbekämpande myndigheterna berörs i sin brottsutredande verksamhet av i hur stor utsträckning trafikuppgifter finns lagrade. Därutöver berörs PTS i egenskap av tillsynsmyndighet med föreskriftsrätt.

Kostnader och andra konsekvenser utifrån alternativa regleringsförslag

Kostnader

Kostnaderna för att genomföra lagringsskyldigheten och anpassningsskyldigheten har av Trafikuppgiftsutredningen beräknats uppgå till cirka 200 miljoner kronor. Med hänsyn till att lagringstiden föreslås begränsas till sex månader och kostnadsuppskattningen utgår från en lagringstid på ett år bör det dock finnas viss marginal i kostnadsberäkningen. Kostnaden för att lämna ut uppgifterna kan beräknas uppgå till cirka 20 miljoner kronor årligen. En utförligare redogörelse för kostnadsberäkningen återfinns i betänkandet, SOU 2007:76.

Ekonomiska konsekvenser

Det finns tre möjliga sätt att fördela kostnaderna; att det allmänna står för alla kostnader, att leverantörerna står för alla kostnader eller att kostnaderna fördelas mellan det allmänna och leverantörerna. Enligt förslaget ska leverantörerna stå för kostnaderna för lagring, säkerhet och anpassning av systemen. Det allmänna ska ersätta leverantörerna för de kostnader som uppstår i samband med utlämnande av uppgifter i enskilda ärenden. Förslaget innebär att regeringen eller den myndighet regeringen bestämmer meddelar närmare föreskrifter om ersättningen. I avsnitt 9.2.2 i lagrådsremissen redovisas bedömningen att tillsynsmyndigheten genom föreskrifter bör fastställa schabloner för ersättningsnivån och ge riktlinjer för vad som ska gälla i de situationer där det finns anledning att avvika från schablonerna. Den ordning som hittills har gällt innebär att ersättningen har bestämts generellt efter förhandlingar mellan de brottsbekämpande myndigheterna och leverantörerna.

Den modell som föreslås, och som gäller sedan tidigare, där leverantörerna bekostar anpassning och drift av systemen, medan de brottsbekäm-

pande myndigheterna ersätter leverantörerna när uppgifter lämnas ut har stora fördelar. Med denna modell har den part som har möjlighet att påverka kostnaden också ansvar för den. Leverantörernas tekniska och administrativa kompetens på området utnyttjas, samtidigt som de har ett tydligt incitament att hålla kostnaderna för anpassning och drift nere. Med denna modell får de brottsbekämpande myndigheterna dessutom ett incitament att inhämta trafikuppgifter bara då man anser det vara en effektiv metod som kan förväntas föra utredningsarbetet framåt. En sådan modell blir således mest samhällsekonomiskt kostnadseffektiv.

I dag fattar domstol beslut om hemlig teleövervakning i drygt 1 000 fall om året och polisen begär ut uppgifter med stöd av lagen om elektronisk kommunikation i omkring 9 500 fall. Eftersom förslaget innebär att trafikuppgifterna i viss ökad utsträckning kommer att vara tillgängliga vid begäran kan det förväntas att de brottsbekämpande myndigheterna kommer att begära ut trafikuppgifter i något ökad utsträckning i förhållande till vad som redan gäller, vilket kommer att leda till marginellt ökade handläggningskostnader. I bedömningen av rättsväsendets kostnader måste emellertid också vägas in att vissa effektivitetsvinster för rättsväsendet torde uppstå i och med att allvarliga brott kan utredas och lagföras snabbare. Den uppskattade kostnaden för ersättning till leverantörerna vid utlämnande av uppgifter överensstämmer väl med nivån på den ersättning som betalas till leverantörerna i dag. Sammanfattningsvis görs bedömningen att förslaget inte medför behov av att tillföra rättsväsendet ytterligare resurser.

Den myndighet som utöver rättsväsendet kommer att få ökade kostnader till följd av förslaget är PTS. Myndigheten har redan i uppdrag att utöva tillsyn enligt lagen om elektronisk kommunikation. I det uppdraget ingår att ha tillsyn över hur leverantörerna sparar, utplånar och avidentifierar trafikuppgifter enligt 6 kap. lagen om elektronisk kommunikation. PTS har dock hittills inte bedrivit någon särskilt omfattande verksamhet på det området.

Myndigheten kommer med den nya regleringen att behöva lägga ner mer 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 kommer bl. a. att behöva utfärda säkerhetsföreskrifter och föreskrifter om ersättning, pröva om det ska medges 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.

Myndigheten har bedömt att verksamheten behöver tillföras cirka tre miljoner kronor under det första året, cirka två miljoner kronor under det andra året och därefter knappt en miljon kronor årligen. PTS:s verksamhet inom verksamhetsgrenen elektronisk kommunikation, som bedrivs med stöd av lagen om elektronisk kommunikation, finansieras till största del med avgifter. Ingen ändring föreslås för denna ordning. Det kommer alltså även fortsättningsvis ankomma på PTS att disponera avgifterna så att de ökade kostnaderna får täckning.

Det är sannolikt att leverantörernas ökade kostnader för lagring, säkerhet och anpassning av systemen, liksom ökade avgifter för PTS:s tillsyn,

leder till att priserna på kommunikationstjänster höjs och att slutkonsumenterna därmed i viss utsträckning får bära dessa kostnader. Av de skäl som anförts ovan bedöms dock den valda modellen för kostnadsfördelning vara den mest kostnadseffektiva från en samhällsekonomisk utgångspunkt.

Förslagens utformning med anledning av Sveriges medlemskap i Europeiska unionen samt nationell särreglering

Sveriges medlemskap i EU innebär att det finns en skyldighet att genomföra EG-direktiv i nationell rätt. Utöver vad som följer av direktivet om lagring av trafikuppgifter föreslås att lagringsskyldigheten ska gälla även vid misslyckad uppringning och för uppgifter om lokalisering av mobil kommunikationsutrustning vid kommunikationens slut.

De brottsbekämpande myndigheterna har, utöver uppgifter om samtal som gått fram, ett stort behov av uppgifter om misslyckad uppringning. Den begränsning som ligger i direktivet, att uppgifterna inte bara ska vara behandlade utan även lagrade eller loggade av leverantören, skulle vidare kunna leda till att de brottsbekämpande myndigheterna inte får tillgång till uppgifter som de i dag får, dvs. om dessa uppgifter inte framöver lagras av leverantörerna. Utifrån ett brottsbekämpande perspektiv finns således stort värde i att lagringsskyldigheten gäller även vid misslyckad uppringning, utan den begränsning som ligger i direktivet.

Av direktivet följer att lokaliseringsinformation för kommunikationens början ska lagras. Enligt de brottsbekämpande myndigheterna bör lagringsskyldigheten för lokaliseringsuppgifter omfatta även kommunikationens slut samt pågående kommunikation, exempelvis en gång per minut. Det kan konstateras att lokaliseringsinformation för kommunikationens början många gånger inte alls är tillräckligt för de brottsbekämpande syftena. Om lokaliseringsinformation för kommunikationens slut inte lagras skulle det vara enkelt att i en kriminell verksamhet vilseleda myndigheterna med negativa följder för utredningsarbetet. Detta har också beaktats i exempelvis den danska regleringen, som föreskriver lagringsskyldighet för lokaliseringsuppgifter även rörande kommunikationens slut. Information om var en kommunikation avslutades kan vara lika värdefull som information om var den påbörjades. Mot bakgrund av ovanstående får det anses finnas ett behov av att lagra lokaliseringsuppgifter även vid kommunikationens slut.

Om intresset av att bekämpa brott motiverar att en lagringsskyldighet införs, trots att det innebär ett intrång i integritetsskyddet, bör också brottsbekämpningsintresset väga relativt tungt vid utformningen av lagringsskyldigheten. Även med beaktande av integritetsskyddet är det alltså motiverat att lagringsskyldigheten omfattar misslyckade samtal och lokaliseringsuppgifter för mobil kommunikationsutrustning vid kommunikationens slut. Däremot föreslås inte lagringsskyldighet för lokaliseringsinformation under pågående kommunikation.

Ikraftträdande och övergångsbestämmelser

Lagändringarna föreslås träda i kraft den 1 juli 2011. Några övergångsbestämmelser föreslås inte. Förslaget går ut på att direktivet om lagring av trafikuppgifter nu genomförs i svensk rätt. Europeiska unionens domstol har i dom den 4 februari 2010 konstaterat att Sverige inte i rätt tid genomfört den del av direktivet som skulle ha varit genomförd senast den 15 september 2007. Mot denna bakgrund, samt då lagrade trafikuppgifter utgör ett mycket viktigt verktyg vid avslöjande, utredning och lagföring av allvarlig brottslighet är det angeläget att de nya reglerna träder i kraft snarast möjligt.

Det är rimligt att leverantörerna får viss tid på sig att anpassa sin verksamhet till de nya kraven. Det bör dock beaktas att direktivet har funnits på plats sedan mars 2006 och utredningen sedan november 2007. Därigenom har grundförutsättningarna för vilka krav leverantörerna kommer att åläggas varit kända under lång tid. Förslaget följer också till allra största del direktivets minimikrav. Eftersom Sverige är bland de sista länderna inom EU att genomföra direktivet har leverantörerna även haft möjlighet att studera och dra nytta av erfarenheter från leverantörer i andra medlemsstater och av den teknik som utvecklats där. Mot denna bakgrund anser regeringen att det är rimligt att lagändringarna träder i kraft den 1 juli 2011. Några särskilda övergångsbestämmelser bedöms inte heller behöva införas.

De företag som berörs av regleringen

Direktivet om lagring av trafikuppgifter omfattar leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster och allmänna kommunikationsnät. Direktivets uttryck om vilka som omfattas av lagringsskyldigheten ansluter till formuleringarna i 2 kap. 1 § lagen (2003:389) om elektronisk kommunikation, där det anges att allmänna kommunikationsnät av sådant slag som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster endast får tillhandahållas efter anmälan till tillsynsmyndigheten (Post- och telestyrelsen). Av 2 kap. 2 § lagen om elektronisk kommunikation 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 samt att Post- och telestyrelsen får meddela föreskrifter om ytterligare undantag från anmälningsplikten.

Förslaget innebär att de leverantörer som är anmälningspliktiga enligt lagen om elektronisk kommunikation ska vara skyldiga att lagra trafikuppgifter. Enligt en uppskattning gjord av branschorganisationen IT&Telekomföretagen rör det sig om 460–470 operatörer.

Post- och telestyrelsen (PTS) ska i enskilda fall få besluta om undantag från lagringskravet. En sådan undantagsmöjlighet avser verksamheter, som i och för sig är anmälningspliktiga men är av så liten omfattning och har ett så begränsat intresse ur ett brottsbekämpande perspektiv att det skulle vara oproportionerligt att kräva att leverantören som bedriver

verksamheten helt eller delvis ska lagra trafikuppgifter på det sätt som direktivet kräver.

Påverkan på konkurrensförhållanden

Genomförandet av direktivet om lagring av trafikuppgifter kommer att få konsekvenser för leverantörerna, bl.a. beträffande deras möjligheter att konkurrera med de tjänster som de tillhandahåller. Skyldigheten att lagra uppgifter kan exempelvis medföra ökade inträdeshinder för nya operatörer. Lagringsskyldigheten kan också förväntas få olika konsekvenser beroende på om den leverantör som blir skyldig att lagra trafikuppgifter ska anpassa ett nyare eller äldre system eller om det rör sig om ett litet eller stort företag. Det kan antas att mindre företag relativt sett får högre kostnader än större företag till följd av att lagringsskyldigheten är förenad med vissa fasta kostnader. Därigenom kan konkurrensen påverkas. En annan aspekt som kan påverka möjligheten att konkurrera är vad för typ av tjänst som kommer att omfattas av lagringsskyldigheten.

Direktivet om lagring av trafikuppgifter syftar bl.a. till att främja den inre marknaden och förbättra konkurrensmöjligheterna bland leverantörerna inom den europeiska gemenskapen. I direktivet konstateras att de stora skillnaderna mellan medlemsstaterna vad gäller lagring av trafikuppgifter utgör ett hinder för den inre marknaden, varför ett direktiv med en minimiharmonisering av lagringsskyldigheten kommer att förbättra möjligheterna att konkurrera på lika villkor. Utgångspunkten är således att leverantörerna ställs inför huvudsakligen samma krav inom den europeiska gemenskapen, vilket får anses främja konkurrensen. De flesta medlemsstaterna i EU har valt en längre lagringstid än sex månader, vilket borde innebära att svenska företag får en konkurrensmässig fördel, i den utsträckning lagringstiden påverkar de totala kostnaderna för företagen.

Enligt förslaget införs ett nationellt särkrav i Sverige, av innebörd att även uppgifter rörande misslyckad uppringning och lokaliseringsinformation för kommunikationens slut, vid mobil kommunikationsutrustning, ska lagras. Trafikuppgiftsutredningen har konstaterat att det nationella särkravet kräver särskild anpassning av operatörernas system, eftersom sådana uppgifter för närvarande inte lagras hos alla leverantörer, även om de i och för sig identifieras och sparas för en kort stund. Även volymen på lagrad datamängd kommer att öka, främst med hänsyn till att även misslyckade samtal nu ska lagras. Utredningen bedömde emellertid att de totala kostnaderna för lagringsskyldigheten är begränsade i förhållande till marknadens totala omsättning, dvs. att marknaden som helhet torde påverkas endast marginellt av att en lagringsskyldighet införs. Införandet av en lagringsskyldighet för dessa uppgifter förväntas därför i princip inte påverka nya leverantörers möjligheter till marknadstillträde eller investeringsvilja, men detta särkrav kan påverka svenska företags konkurrenssituation negativt i förhållande till aktörer verksamma i medlemsstater där motsvarande krav inte införs.

Många verksamheter som bedrivs i privat regi är förknippade med olika samhälleliga krav. Det är således inget nytt att andra intressen än

rent företagsekonomiska, t.ex. att få in skatteintäkter, mildra påverkan på miljön eller brottsbekämpningsintressen, måste beaktas även om detta påverkar de privata aktörernas verksamhet.

För att så långt det är rimligt och möjligt mildra de negativa konkurrensmässiga effekterna som ett genomförande av direktivet innebär har följande föreslagits. PTS har en möjlighet att medge undantag från lagringsskyldigheten, helt eller delvis, när leverantören bedriver en verksamhet av liten omfattning. De som är skyldiga att lagra uppgifter får också uppdra åt någon annan att utföra lagringen, om de inte själva har förmåga att göra det. De myndigheter som begär ut trafikuppgifter ska vidare ersätta leverantörerna för de kostnader som uppstår.