

Regeringens proposition till Riksdagen med förslag till lag om ändring av lagen om dataskydd vid elektronisk kommunikation

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås att lagen om dataskydd vid elektronisk kommunikation ska ändras. De tjänsteföretag som är skyldiga att göra en televerksamhetsanmälan ska åläggas att lagra kommunikationsuppgifter i tolv månaders tid. Lagringsskyldigheten ska gälla bl.a. uppgifter om vem som har ringt ett samtal eller skickat ett e-postmeddelande och när detta har skett. Lagringsskyldigheten utsträcker sig inte till innehållet i meddelandena. Uppgifterna ska lagras för myndigheternas behov och i synnerhet för behov i samband med utredning av brott. De föreslagna

ändringarna gäller enbart lagring av uppgifterna. Utnyttjandet av uppgifterna och myndigheternas rätt att få information bestäms alltså i enlighet med andra, gällande nationella bestämmelser. Det föreslås att den myndighet för vars behov uppgifterna lagras ska svara för de extra kostnader som lagringen medför för teleföretagen.

Dessutom föreslås vissa lagtekniska ändringar.

Lagen avses träda i kraft så snart som möjligt.

INNEHÅLL

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL	1
INNEHÅLL	2
ALLMÅN MOTIVERING	3
1 INLEDNING.....	3
2 NULÄGE	3
2.1 Lagstiftning och praxis.....	3
Myndigheternas rätt att få upplysningar.....	5
2.2 Den internationella utvecklingen samt lagstiftningen i utlandet	7
Irland	8
Storbritannien	8
Norge	8
Frankrike	9
Sverige.....	9
Tyskland.....	9
Danmark	9
Förenta staterna	10
Det huvudsakliga innehållet i direktivet om lagring av identifieringsuppgifter	11
2.3 Bedömning av nuläget	15
3 MÅLSÄTTNING OCH DE VIKTIGASTE FÖRSLAGEN	15
3.1 Målsättning.....	15
3.2 De viktigaste förslagen.....	15
4 PROPOSITIONENS KONSEKVENSER	16
4.1 Ekonomiska konsekvenser	16
4.2 Konsekvenser för myndigheternas verksamhet.....	16
4.3 Samhälleliga konsekvenser	16
5 BEREDNINGEN AV PROPOSITIONEN	17
5.1 Beredningsskeden och beredningsmaterial	17
5.2 Remissyttranden och hur de har beaktats.....	17
6 SAMBAND MED ANDRA PROPOSITIONER.....	18
DETALJMOTIVERING	19
1 LAGFÖRSLAG	19
1.1 Lagen om dataskydd vid elektronisk kommunikation	19
2 IKRAFTTRÄDANDE	30
3 FÖRHÅLLANDE TILL GRUNDLAGEN SAMT LAGSTIFTNINGSORDNING	30
LAGFÖRSLAG	35
Lag om ändring av lagen om dataskydd vid elektronisk kommunikation.....	35
BILAGA	39
PARALLELLTEXT	39
Lag om ändring av lagen om dataskydd vid elektronisk kommunikation.....	39

ALLMÄN MOTIVERING

1 Inledning

Uppgifter om elektronisk kommunikation är redan i dag viktiga för utredningen av olika slags brott. Det kan antas att dessa uppgifter får allt större betydelse i fortsättningen när informationssamhället utvecklas. Uppgifter om kommunikation har betydelse för utredningen av både brott som begåtts med kommunikationsmedel och helt traditionella brott. Behov av att få kommunikationsuppgifter av teleföretag kan uppkomma i och med uppdagade brott först flera månader efter en viss kommunikationshändelse. Med tanke på utredningen av brott är det därför viktigt att säkerställa att kommunikationsuppgifterna finns kvar tillräckligt länge. I sådana fall är det emellertid väsentligt att se till att de grundläggande fri- och rättigheterna för dem som idkar kommunikation görs gällande. Lagen om dataskydd vid elektronisk kommunikation (516/2004) trädde i kraft den 1 september 2004. Lagen reglerar bl.a. behandling och lagring av identifieringsuppgifter. Den baserar sig på rådets och parlamentets direktiv 2002/58/EG om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (nedan direktivet om integritet och elektronisk kommunikation).

I lagen om dataskydd vid elektronisk kommunikation ingår uttömmande bestämmelser om de ändamål för vilka de identifieringsuppgifter som nu ska regleras får behandlas. Efter behandlingen ska meddelandena och identifieringsuppgifterna i regel förstöras eller göras sådana att de inte kan förknippas med abonnenten eller användaren, om inte något annat bestäms i lag. I personuppgiftslagen (523/1999) bestäms om behandling av personuppgifter och förutsättningar för behandlingen.

Genom rådets och parlamentets direktiv 24/2006/EG, som gäller lagring av identifieringsuppgifter och som antogs i mars 2006, åläggs teleföretag att lagra vissa för dem tillgängliga identifieringsuppgifter om alla

abbonnenter eller användare som utövar kommunikation samt vissa andra uppgifter. Uppgifterna ska lagras i minst sex månader och högst två år. Inom denna tidsram får lagringstiden fastslås närmare på nationell nivå.

Syftet med lagringen är att säkerställa att teleföretagen förfogar över uppgifterna tillräckligt länge framför allt för polisens behov. Myndigheternas rätt att ta del av de lagrade uppgifterna bestäms särskilt i enlighet med gällande nationella bestämmelser.

2 Nuläge

2.1 Lagstiftning och praxis

I 10 § i grundlagen bestäms om skydd för privatlivet, dvs. integritetsskydd, som omfattar bl.a. skydd av hemfriden samt skydd av förtroliga (konfidentiella) meddelande- och personuppgifter. Inom elektronisk kommunikation är speciellt skyddet för personuppgifter och rätten till konfidentiell kommunikation viktiga delområden av integritetsskyddet. Till den elektroniska kommunikationen anknyter utöver dessa också behovet av integritetsskydd bl.a. inom delområden som omfattas av hemfriden. Vid elektronisk kommunikation gäller integritetsskyddet förutom skydd av innehållet i konfidentiella meddelanden också de identifieringsuppgifter som uppkommer genom allmän televerksamhet eller vid användning av informations-samhällets tjänster eller kommunikationsnätet och som kan användas för att identifiera antingen en fysisk person eller en juridisk person.

Med stöd av 10 § 2 mom. i grundlagen är skydd av konfidentiella meddelanden en grundläggande rättighet för medborgarna. Enligt bestämmelsen är brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden okränkbar. I grund och botten handlar det om att skydda den självbestämmanderätt som tillkommer varje medborgare. I 10 § 3 mom. i grundlagen sägs att genom lag kan bestämmas om

åtgärder som ingriper i hemfriden och som är nödvändiga för att de grundläggande fri- och rättigheterna ska kunna tryggas och för att brott ska kunna utredas. Genom lag kan också bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång och säkerhetskontroll samt under frihetsberövande. Kärnområdet för skyddet av förtroliga meddelanden omfattar i synnerhet meddelandets innehåll, men också identifieringsuppgifter som anknyter till meddelandet omfattas av skydd av konfidentialitet.

Skyddet av konfidentiella meddelanden innebär att ingen annan än avsändaren eller den av avsändaren avsedda rätta mottagaren av ett meddelande har rätt att ta del av meddelandets innehåll eller i övrigt göra ingrepp i meddelandets innehåll eller i identifieringsuppgifterna som anknyter till meddelandet, eller på något sätt förhindra att meddelandet förmedlas till mottagaren. Om meddelandet inte är avsett att bli föremål för allmän mottagning, får utomstående parter inte behandla eller lagra meddelandet eller överlåta det till någon annan utomstående part utan samtycke av kommunikationsparten.

Genom vanlig lag bestäms om skyddet av konfidentiella meddelanden i lagen om dataskydd vid elektronisk kommunikation. Enligt 4 § 1 mom. i lagen är meddelanden, identifieringsuppgifter och lokaliseringssuppgifter konfidentiella, om inte något annat bestäms i lagen eller i någon annan lag. I 9-14 § bestäms om situationer där någon annan än en kommunikationspart får behandla identifieringsuppgifter. Enligt 9 § får identifieringsuppgifter behandlas i den utsträckning det är nödvändigt för att utföra och använda nättjänster, kommunikationstjänster eller mervärdestjänster och för att sörja för dataskyddet för dessa tjänster. Det handlar om förmedling av meddelanden och om tjänsternas funktion. Dessutom får identifieringsuppgifter under vissa förutsättningar behandlas för fakturering, marknadsföringsändamål och teknisk utveckling, för att upptäcka missbruk som omfattar användning av tjänster och för att upptäcka fel och störningar.

Behandling är tillåten endast i den omfattning som behandlingens ändamål kräver och behandlingen får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt. Identifieringsuppgifter får lämnas ut endast till den som har rätt att behandla uppgifterna i förekommande fall. Efter behandlingen ska meddelandena och identifieringsuppgifterna förstöras eller göras sådana att de inte kan förknippas med abonnenten eller användaren, om inte något annat bestäms i lag.

I 19 § i lagen om dataskydd vid elektronisk kommunikation bestäms om skyldigheter när det gäller att sörja för dataskyddet.

Rätten att behandla och lagra identifieringsuppgifter om elektronisk kommunikation har reglerats med noggrann avgränsning i lagstiftningen i Finland och så att regleringen syftar till att säkra att integritetsskyddet och skyddet för förtroliga meddelanden görs gällande. För närvarande bestäms en längre tids förvaring av identifieringsuppgifter i praktiken enligt 10 § i lagen om dataskydd vid elektronisk kommunikation. Paragrafen gäller behandling av identifieringsuppgifter i faktureringssyfte. Enligt paragrafen ska uppgifterna lagras minst tre månader räknat från räkningens förfallodag eller från det att identifieringsuppgifterna registrerades, beroende på vilken av dessa tidpunkter som infaller senare. Uppgifterna får dock inte lagras efter det att fordran har preskriberats enligt lagen om preskription av skulder (728/2003). I 4 § i lagen om preskription av skulder bestäms om den allmänna preskriptionstiden så att en skuld preskriberas tre år efter en tidpunkt som bestäms i 5, 6 och 7 §, om inte preskriptionen har avbrutits före det. Med tanke på bestämmelsen i lagen om dataskydd vid elektronisk kommunikation räknas tidpunkten för när preskriptionstiden börjar i enlighet med 5 § i den nämnda lagen från den förfallodag som angetts på räkningen. I praktiken lagras teleföretagen i Finland uppgifter som hänförs sig till bestämmande av räkningar på ett något varierande sätt, men i lagen om preskription av skulder begränsas registreringen av faktureringsuppgifter till högst tre år.

Man har strävat efter att skydda konfidentiella meddelanden också genom att kriminalisera kränkningar av konfidentiell kommuni-

kation. Enligt 38 kap. 3 och 4 § i strafflagen (39/1889) är kränkning av kommunikationshemlighet en straffbar gärning. I 38 kap. 3 § föreskrivs straff för den som obehörigen öppnar ett brev eller ett annat tillslutet meddelande som är adresserat till någon annan eller genom att bryta ett säkerhetsarrangemang skaffar uppgifter om ett meddelande som har upptagits elektroniskt eller med någon annan sådan teknisk metod och som är skyddat mot utomstående, eller skaffar uppgifter om innehållet i samtal, telegram, text-, bild-, eller dataöverföring eller något annat motsvarande telemeddelande som förmedlas genom telenät eller om avsändande eller mottagande av ett sådant meddelande.

Skyddet av konfidentiella meddelanden garanteras också enligt internationella fördrag om de mänskliga rättigheterna, i synnerhet enligt konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (FördrS 19/1990) samt enligt de rättigheter som fastställts i Europeiska unionens stadga om de grundläggande rättigheterna. Artikel 8 i konventionen gäller respekt för privatlivet och familjelivet, vilket också omfattar respekt för korrespondensens integritet. Artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna gäller skydd av privatlivet och familjelivet, och artikel 8 gäller skydd av personuppgifter.

Myndigheternas rätt att få upplysningar

Med tanke på den föreslagna ändringen är det viktigt att granska på vilka grunder myndigheterna för närvarande kan få tillgång till uppgifter som teleföretagen förfogar över.

I personuppgiftslagen tillskrivs alla myndigheter rätt att få personuppgifter på vissa villkor. I personuppgiftslagen fastslås de allmänna förutsättningarna för att teleföretagen ska få lämna ut personuppgifter till myndigheterna. Personuppgiftslagen täcker inte sådana situationer som uttryckligen har reglerats särskilt i lag eller som föranleds av uppdrag eller skyldigheter som ålagts den registransvarige genom eller med stöd av lag.

I lagen om dataskydd vid elektronisk kommunikation anges de allmänna förutsättningarna för att teleföretag ska få lämna ut uppgifter om innehållet i meddelanden och

identifieringsuppgifter till myndigheterna. Uppgifter får lämnas ut endast till den som har rätt att behandla uppgifterna i förekommande fall.

Polisen är den myndighet som har de mest omfattande rättigheterna att ta del av uppgifter som teleföretagen förfogar över. Polisen har rätt att för att avvärja eller avslöja brott rikta teleövervakning eller teleavlyssning mot en person under vissa förutsättningar som anges i polislagen (493/1995) samt för att utreda brott med stöd av tvångsmedelslagen (450/1987). Polisen har dessutom rätt att av teleföretag få identifieringsuppgifter eller uppgifter om lokaliseringen av en mobiltelefon. Rättigheterna att få uppgifter i samband med teleövervakning och teleavlyssning inrymmer domstolskontroll. Utan hinder av företags-, bank- eller försäkringshemlighet har polisen också rätt att av privata sammanslutningar få uppgifter som behövs för avvärjande eller utredning av brott. Även övriga förundersökningsmyndigheter har motsvarande rättigheter i begränsad utsträckning.

Dessutom har polisen rätt att av ett teleföretag och av en sammanslutningsabonnent eller med en teknisk anordning få kontaktuppgifter om en sådan teleanslutning som inte är upptagen i en offentlig katalog, eller uppgifter som specificerar en teleanslutning, e-postadress, annan teledress eller teleterminalutrustning, om uppgifterna i ett enskilt fall behövs för utförandet av en uppgift som ankommer på polisen.

Med stöd av lagen om dataskydd vid elektronisk kommunikation har polisen rätt att med samtycke av målsäganden och den som innehar en anslutning få sådana identifieringsuppgifter av ett teleföretag om uppkoppling till anslutningen som behövs för utredning av brott mot besöksförbud enligt i 16 kap. 9 a § i strafflagen, av ofog enligt 17 kap. 13 § 2 punkten eller av hemfridsbrott enligt 24 kap. 1 § 2 punkten. Polisen har dessutom rätt att med abonnentens eller terminalutrustningsägarens samtycke få identifieringsuppgifter om de meddelanden som sänts från en mobiltelefon till den del detta är nödvändigt för att utreda brott där mobiltelefonen eller dess anslutning obehörigen har kommit i någon annans besittning.

Gränsbevakningslagen (578/2005) ger en gränsbevakningsman rätt att för förebyggande och utredning av brott få uppgifter om mobilteleapparater. I fråga om förutsättningarna hänvisas till 31 f § i polislagen och 5 a kap. 3 a § i tvångsmedelslagen, dvs. också denna rätt att få uppgifter är förenad med domstolskontroll. Bestämmelserna om teleavlyssning och teleövervakning i polislagen och tvångsmedelslagen medför inte direkt några rättigheter för gränsbevakningsmännen, utan rättigheterna kommer via hänvisningsbestämmelser. En gränsbevakningsman som deltar i en förundersökning som görs under ledning av en annan förundersökningsmyndighet har rätt att behandla uppgifter som har inhämtats med en sådan metod som inte står till buds för gränsbevakningsväsendet. I 18 § i lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005) föreskrivs om gränsbevakningsväsendets rätt att utan hinder av företagshemlighet eller bank- eller försäkringshemlighet av en privat sammanslutning eller en privatperson få uppgifter för förebyggande av eller utredning av ett brott. Bestämmelsen motsvarar den rätt att få uppgifter som ingår i 36 § i polislagen. I sjöräddningslagen (1145/2001) föreskrivs dessutom om rätt att i kritiska lägen av ett teleföretag få uppgifter om den anslutning som ett nödmeddelande hänför sig till.

Tullagen (1466/1994) ger en tullman rätt att få identifieringsuppgifter om telemeddelanden. Rätten att få uppgifter gäller i syfte att förebygga eller avslöja brott och på vissa villkor som anges i tullagen. I fråga om utredning av brott hänvisas till tvångsmedelslagen. En tullman har dessutom rätt att utan hinder av företags-, bank- eller försäkringshemlighet av privata sammanslutningar och enskilda personer få sådana uppgifter som behövs för förebyggande och utredning av tullbrott. En tullman har också rätt att för förhindrande och utredning av tullbrott av samfund som idkar televerksamhet erhålla kontaktuppgifter om en sådan teleanslutning som inte är upptagen i offentlig katalog.

De myndigheter som tar emot nödmeddelanden, t.ex. en nödcentral, sjöräddningscentral, sjöräddningsundercentral och polisens alarmeringscentral, har enligt lagen om data-

skydd vid elektronisk kommunikation rätt att få identifierings- och lokaliseringssuppgifter om den anslutning och den terminalutrustning från vilken nödmeddelandet har sänts samt uppgifter om anslutningens abonnent, användare och installeringsadress. Dessa aktörer har dessutom rätt att få identifierings- och lokaliseringssuppgifter som anger lokaliseringen av den terminalutrustning och anslutning som innehas av den användare som är föremål för nödmeddelandet, om den myndighet som mottagit nödmeddelandet har grundad anledning att anta att användaren befinner sig i uppenbar nöd eller omedelbar fara.

I lagen om kontroll av export av produkter med dubbel användning (562/1996) ges tullmyndigheten rätt att få sådana uppgifter som behövs för exportkontroll. Även utrikesministeriet och skattemyndigheterna har samma rätt. Bestämmelsen lämpar sig på bred front för alla som förfogar över uppgifter som behövs för kontroll av export av produkter med dubbel användning. Bestämmelsen är tillämplig på teleföretag, om de exporterar produkter med dubbel användning eller förfogar över uppgifter som behövs för exportkontroll. Enligt lagen om förvaltningen av utrikeshandeln samt om kontroll- och skyddsåtgärder i vissa fall (1521/1994) gäller dessutom att utrikesministeriet, handels- och industriministeriet, jord- och skogsbruksministeriet, tullstyrelsen samt skattemyndigheterna har rätt att av varandra få sådana uppgifter om export och import som myndigheterna behöver i sin övervakningsuppgift. Bestämmelsen lämpar sig på bred front för alla som förfogar över uppgifter som behövs för exportkontroll. Bestämmelsen är tillämplig också på teleföretag när de bedriver utrikeshandel som omfattas av kontroll eller skyddsåtgärder eller om de förfogar över uppgifter som behövs för exportkontroll.

Enligt lagen om yttrandefrihet i masskommunikation (460/2003) har dessutom en tjänsteman som är anhållningsberättigad, en allmän åklagare eller en målsägande rätt att få uppgifter med tillstånd av en domstol. De har rätt att få identifieringsuppgifter som behövs för utredande av vem som är avsändare av ett nätmeddelande, om det föreligger sannolika skäl att misstänka att innehållet i

meddelandet är sådant att det är straffbart att göra det tillgängligt för allmänheten. Det får dock förordnas att identifieringsuppgifterna ska lämnas ut till målsäganden först när målsäganden själv väcker åtal för brottet.

I lagen om dataskydd vid elektronisk kommunikation bestäms särskilt om rätt för Kommunikationsverket att få identifierings- och lokaliseringssuppgifter, om de behövs för att utreda vissa i lagen nämnda fel, störningar och andra oklarheter. Dessutom har Kommunikationsverket och dataombudsmannen rätt att under vissa i lagen angivna förutsättningar få identifierings- och lokaliseringssuppgifter samt i 20 § 3 mom. avsedda meddelanden. Enligt lagen om statens televisions- och radiofond (745/1998) har Kommunikationsverket dessutom rätt att enligt avtal få telefonnummer och annan motsvarande kontaktinformation, om uppgifterna behövs för indrivningen av televisionsavgifter och övervakningen av att lagen följs. Det föreslås inte någon ändring av tillsynsmyndigheternas rätt att ta del av uppgifterna och följaktligen har t.ex. Kommunikationsverket rätt att få uppgifter på samma villkor som hittills.

Enligt utsköningslagen (37/1895) har en utmätningsman rätt att få identifierings- och personuppgifter, dvs. gäldenärens adress- och telefonuppgifter liksom övriga kontaktuppgifter som denne har i egenskap av utövare av tele- eller postverksamhet. Enligt konkurslagen (120/2004) och lagen om företagsreanering (47/1993) har konkursboets förvaltare och utredningsman rätt att få uppgifter om gäldenärens ekonomiska ställning eller om gäldenärens ekonomiska verksamhet. Bo-förvaltarens rätt att få uppgifter gäller inte känsliga uppgifter som avses i personuppgiftslagen och som omfattas av integritetsskydd. En gäldenär har motsvarande rätt att få uppgifter med stöd av båda lagarna.

Också i fängelselagen (767/2005) och häktningsslagen (768/2005) finns bestämmelser om rätt att få uppgifter. Enligt lagberedningsmaterialet används likväl egen utrustning för avlyssning enligt fängelselagen, t.ex. en annan telefon, en högtalartelefon eller så att någon är närvarande i samma rum. Bestämmelserna medför därmed inte rätt att ta del av uppgifter som teleföretagen förfogar över.

En intressebevakare som avses i lagen om förmyndarverksamhet (442/1999) är berättigad att få de uppgifter som huvudmannen själv skulle ha rätt att få. Rätten att få uppgifterna gäller endast i fråga om ärenden som hör till intressebevakarens uppdrag. Dessutom har intressebevakaren utan huvudmannens samtycke rätt att öppna endast sådana till huvudmannen anlända brev eller därmed jämförbara tillslutna meddelanden som på basis av avsändarens namn eller någon annan särskild omständighet kan antas gälla ärenden som intressebevakaren ska sköta. Enligt ärvdabalken (40/1965) har dödsbodelägare, boutredningsmannen och testamentsexekutorn rätt att få sådana uppgifter som arvlåtaren också själv skulle ha haft rätt att få. Uppgifterna ska vara nödvändiga för utredning av boet.

2.2 Den internationella utvecklingen samt lagstiftningen i utlandet

Europeiska rådet bekräftade i sitt uttalande om terrorismbekämpning av den 25 mars 2004 att det är nödvändigt med regler på EU-nivå för att säkerställa att trafikuppgifter finns tillgängliga för terrorismbekämpning. Efter bombattackerna i Madrid fick rådet i uppdrag av Europeiska rådet att undersöka ”förslag för att fastställa regler för lagring av trafikuppgifter från kommunikation hos tjänsteoperatörer” med avsikten att sådana regler skulle antas under 2005. Att antagandet av ett lämpligt rättsligt instrument på detta område är en prioritet bekräftades i slutsatserna från Europeiska rådets möte den 16-17 juni 2005 samt vid det särskilda mötet med rådet (rättsliga och inrikes frågor) den 13 juli 2005 efter terroristattacker i London.

Det ärende som ligger i bakgrunden till det direktiv som nu ska genomföras initierades ursprungligen som ett rambeslutsförslag av fyra medlemsländer, Frankrike, Irland, Sverige och Storbritannien. Förslaget till rambeslut behandlades flera gånger i rådet (rättsliga och inrikes frågor) med början i juli 2004, men enighet nåddes inte. Den 27 juli 2005 lade kommissionen fram ett direktivförslag som till sitt innehåll motsvarade rambesluts-

förslaget. Direktivet om lagring av identifieringsuppgifter antogs den 15 mars 2006.

Irland

Irland har väckt talan i EG-domstolen mot Europeiska gemenskapernas kommission (ECJ – Luxemburg) med anledning av den rättsliga grunden för direktivet om lagring av identifieringsuppgifter. Enligt Irlands ståndpunkt har direktivet antagits utifrån fel rättslig grund. Enligt den gällande terroristlagstiftningen i Irland kan Irlands nationella poliskommissionär (Garda Commissioner) kräva att tjänsteleverantörerna ska lagra identifieringsuppgifterna i särskilda fall i tre år. Teleföretagen svarar själva för alla kostnader för lagringen av uppgifterna.

Storbritannien

I antiterrorismlagen i Storbritannien (*Anti-terrorism, Crime and Security Act 2001*) behandlas insamling och lagring av identifieringsuppgifter i syfte att trygga den nationella säkerheten samt förebygga brott när de antingen direkt eller indirekt hänför sig till den nationella säkerheten. I Storbritannien regleras identifieringsuppgifter förutom i den ovan nämnda lagen också i personuppgiftslagen (*Data Protection Act 1998*) samt i lagen om dataskydd vid elektronisk kommunikation (*The Privacy and Electronic Communications (EC Directive) Regulations 2003*). Enligt de två sistnämnda författningarna ska identifieringsuppgifterna förstöras när de inte längre behövs för kommersiella ändamål, bl.a. för utredning av faktureringsfrågor. Enligt antiterrorismlagen från 2001 har teleföretag rätt att lagra identifieringsuppgifter. Enligt lagen baserar lagringen av identifieringsuppgifter sig på frivilliga avtal mellan Storbritanniens inrikesministerium (Home Office) samt teleföretagen och Internettjänsteleverantörerna. I praktiken har det avtalats om att uppgifterna ska lagras som följer: abonnentuppgifter lagras i tolv månader, identifieringsuppgifter som gäller uppkopplingar i tolv månader, identifieringsuppgifter för SMS-, EMS- och MMS-tjänster i sex månader, identifieringsuppgifter för e-

postmeddelanden i sex månader, ISP-data i sex månader och logguppgifter om webb-funktioner i fyra dagar. I fråga om övriga tjänster avtalas om lagringstiden från fall till fall.

De myndigheter som har rätt att få identifieringsuppgifter och förutsättningarna för erhållande av uppgifterna har fastställts i lag (*Regulation of Investigatory Powers Act 2000*).

De myndigheter för vilkas verksamhet uppgifterna lagras ska betala teleföretagen ersättning för de kostnader som registreringen av identifieringsuppgifterna medför.

Norge

I Norge regleras identifieringsuppgifter genom lagen om elektronisk kommunikation (*Lov om elektronisk kommunikasjon, ekomloven, nr. 83, 4.7.2003*). Med stöd av lagen har det utfärdats en föreskrift om elektroniska kommunikationsnät (*Forskrift om elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste (ekomforskriften) For 401, 16.2.2004*), där bestämmelserna i 7 kap. reglerar behandlingen av identifieringsuppgifter. Genom författningarna har direktivet om integritet och elektronisk kommunikation genomförts.

I Norge bereds som bäst ny lagstiftning. Enligt erhållna uppgifter är det sannolikt att registreringen av identifieringsuppgifter genomförs i två steg: först i fråga om det fasta telefonnätet, mobiltelenäten och Internetförbindelserna, senare i fråga om IP-samtalen och e-postkommunikationen. Det är sannolikt att identifieringsuppgifter kommer att hållas registrerade ett år i Norge och att uppgifterna registreras av respektive tjänsteleverantör.

Frågan om ersättning för kostnaderna har ännu inte avgjorts. Enligt nuvarande praxis fördelas kostnaderna så att lagtillsynsmyndigheten ansvarar för de grundläggande kostnaderna och programvarulicenserna medan operatörerna ansvarar för uppdateringarna av programvaran. Lagtillsynsmyndigheten ansvarar för driftskostnaderna.

Frankrike

I Frankrike regleras identifieringsuppgifter genom en separat lag (*LOI no 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne*). I artikel 29 bestäms om bemyndigande att lagra identifieringsuppgifter i ärenden som hänför sig till utredning av brott. Identifieringsuppgifterna ska förvaras högst ett år. Identifieringsuppgifter regleras mera detaljerat i en särskild förordning (*Décret no 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques*).

Staten ersätter de extra kostnader som lagringsskyldigheten medför för företagen. I praktiken ersätts utgifterna i enskilda fall i enlighet med en viss ersättningstabell.

Sverige

I Sverige kan myndigheterna få identifieringsuppgifter av teleföretag i särskilda fall, när de utreder brott där straffet är fängelse i minst två år. Tjänsteleverantörerna registrerar identifieringsuppgifter allmänt för att förhindra illegal användning av nätet. Enligt den gällande lagstiftningen behöver identifieringsuppgifter inte förstöras när de kan användas för att förhindra illegal användning av nätet.

Bestämmelserna i direktivet om integritet och elektronisk kommunikation har införlivats i *lagen om elektronisk kommunikation (2003:389)*. I 6 kap. 5-8 § finns bestämmelser om användning av identifieringsuppgifter. Genomförandet av direktivet om lagring av identifieringsuppgifter medför ändringar i 6 kap. i lag 2003:389 och 27 kap. i svenska *rättegångsbalken (1998:605)*. Enligt justitiedepartementet håller Sverige på att gå in för en lagringstid på ett år och registreringsskyldigheterna åläggs varje teleföretag särskilt.

Den svenska lagen fastställer ersättningar för kostnaderna endast när det gäller situationer för utlämnande av uppgifter i anslutning till larmkommunikation (6 kap. 22 §). Ersättningarna begränsas till rimliga kostnader. För övrigt regleras inte ersättningar för kostnaderna i telelagen. I praktiken ansvarar operatörerna för kostnaderna för utrustningen me-

dan lagtillsynsmyndigheten ansvarar för driftskostnaderna.

Tyskland

Enligt den gällande lagstiftningen i Tyskland regleras teletjänster genom två lagar (TDG (*Teledienstegesetz*) och TKG (*Telekommunikationsgesetz*)). Tillhandahållare av teletjänster har rätt, men inte skyldighet, att lagra identifieringsuppgifter i sex månader. Genom författningarna har skyldigheterna enligt direktivet om integritet och elektronisk kommunikation införlivats. I den lag som gäller straffprocesser (*Code of Criminal Procedure, Strafprozeßordnung*) och i dess 100 g- och 100 h-punkt regleras myndigheternas rättigheter att få identifieringsuppgifter.

Ett nytt lagförslag (*Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, Berlin 27.11.2006*) gäller genomförande av direktivet om lagring av identifieringsuppgifter. Lagen avses träda i kraft den 15 september 2007 och dess skyldigheter avseende Internet- och e-posttjänster den 15 mars 2009.

Enligt artikel 2 i förslaget till lagändring ska en ny 110 a § (*Speicherungspflichten für Verkehrsdaten*) fogas till TKG. I den nya paragrafen åläggs teleföretagen att lagra identifieringsuppgifter så som förutsätts i direktivet. Det föreslås att identifieringsuppgifterna ska lagras i sex månader.

I syfte att sänka kostnaderna för operatörerna tillämpas lagen om rättsersättning, gottgörelse och skadestånd, vilken allmänt reglerar ersättningen för kostnader i anslutning till rättsmål och förundersökning. Varje operatör debiterar myndigheterna från fall till fall för de kostnader som anlitaendet av personal och användningen av utrustningen har medfört. För närvarande bereds likväl en ny lag som avses innehålla bindande bestämmelser om ersättningar för åtgärderna.

Danmark

I Danmark regleras identifieringsuppgifter i en lag som gäller telemarknaden (*Lov om konkurrence- og forbrugerforhold på tele-*

markedet LOV nr 418 af 31/05/2000) jämte ändringar samt i en särskild författning som utfärdats med stöd av lagen (*Bekendtgørelse om udbud af elektroniske kommunikationsnet og -tjenester, nr. 1031 af 13. Oktober 2006*). I Danmark har teleföretagen eller tillhandahållarna av tjänster på Internet inte några skyldigheter att lagra identifieringsuppgifter utöver det som behövs för att debitera slutanvändarna och ta ut samtrafikutgifter (sammankopplingsavgifter). Genom de nuvarande författningarna har skyldigheterna enligt direktivet om integritet och elektronisk kommunikation genomförts.

Det danska parlamentet har antagit en anti-terrorismlag (378, 6.6.2002), genom vilken det föreskrivs om merskyldigheter avseende förvaltningslagen (*Lov om rettens pleje*). Genom lagändringen åläggs teleföretag och tillhandahållare av tjänster på Internet att registrera och lagra identifieringsuppgifter i ett års tid. Ikraftträdandet förutsätter att det danska justitieministeriet utfärdar detaljerade bestämmelser om verkställandet. Med stöd av 786 § 4 och 7 mom. i förvaltningslagen (*Lov om rettens pleje*) och med stöd av en separat författning (*Lovbekendtgørelse nr. 910 af 27. september 2005*) utfärdade justitieministeriet den 28 september 2006 författningen *Bekendtgørelse om udbydere af elektroniske kommunikationsnets og elektroniske kommunikationstjenesters registrering og opbevaring af oplysninger om teletrafik (logningsbekendtgørelsen)*, (eng. "Executive Order on the retention and storage of traffic data by providers of electronic communications networks and electronic communications services (the Logging Executive Order). I 4–6 § fastställs de uppgifter som företag som tillhandahåller telenättjänster och teletjänster ska införa i sina register. Enligt 9 § ska uppgifterna enligt 4–6 § förvaras i ett års tid. Författningen träder i kraft den 15 september 2007, och det har meddelats anvisningar för hur den ska tillämpas (*Guidelines for the Executive Order on the retention and storage of traffic data by providers of electronic communications networks and electronic communications services (the Logging Executive Order)*).

Utöver det som krävs enligt direktivet ska tjänsteleverantörer som tillhandahåller tråd-

lösa Internetanslutningar dessutom registrera uppgifter om lokalnätens exakta geografiska eller fysiska lokalisering och om den utrustning som använts. Registreringsskyldigheten avseende paketen för start och avslutning av en Internetsession gäller dock inte när den ovan nämnda skyldigheten inte kan fullgöras tekniskt i tjänsteleverantörens system. Också då ska uppgifterna registreras för varje paket om 500 per uppkoppling. Tidpunkten för registrering av datapaketet ska också registreras.

I Danmark kan lagringsskyldigheten enligt direktivet komma att gälla inte bara teleföretag, utan också företag och andra sammanslutningar med mer än 100 användare, vilket är en mycket väsentlig utvidgning i jämförelse med direktivet. Data ska registreras i en nätanslutningspunkt där tillhandahållarens nät löper samman med en eller flera andra tillhandahållares nät.

Teleföretagen ansvarar för investeringskostnaderna i anslutning till utlämnande av identifieringsuppgifter och lagtillsynsmyndigheten ansvarar för driftskostnaderna.

Förenta staterna

I Förenta staterna regleras insamling och lagring av identifieringsuppgifter i en lag från 1996 (*Electronic Communication Transactional Records Act*), i dess 121 kap. 2703 § (f) mom. Enligt lagen ska tillhandahållare av teletjänster på begäran av myndigheterna förvara registreringsuppgifterna i 90 dagar. Om myndigheten begär det kan tidsgränsen förlängas med ytterligare 90 dagar. En revidering av lagringen av identifieringsuppgifter har diskuterats i Förenta staterna redan i ett par års tid. Enligt uppgifter i januari 2007 är avsikten sannolikt att kongressen under 2007 ska föreläggas planer på ny lagstiftning som ålägger tillhandahållare av tjänster på Internet att lagra identifieringsuppgifterna en viss tid. Än så länge har man inte enats om längden på denna tid. Ärendet är också förenat med flera andra öppna frågor, såsom definitionen av tjänsteleverantör, vilka skyldigheter bl.a. tillhandahållare av WiFi-tjänster har och vilka uppgifter som ska lagras.

I 121 kap. 2706 § (Cost reimbursement) i telelagen (*Electronic Communication Tran-*

sactional Records Act) fastställs ersättningarna i sådana fall där myndigheten kräver att för skaffande av information få uppgifter med stöd av 2702 § (*Voluntary disclosure of customer communications of records*), 2703 § (*Required disclosure of customer communications of records*) eller 2704 § (*Back up preservation*). Det betalas ersättning för direkta, rimliga kostnader och teleföretaget och myndigheten kommer överens om ersättningsbeloppet. Om något avtal inte har ingåtts, beslutar domstolen om ersättningen. Ersättningarna gäller dock inte teleidentifieringsuppgifter enligt 2703 §. Domstolen kan likväl besluta om ersättning också när det gäller teleidentifieringsuppgifter, om den information som yrkas är ovanligt stor till sin volym eller om kravet annars medför betydande svårigheter för teleföretaget.

Det huvudsakliga innehållet i direktivet om lagring av identifieringsuppgifter

Artikel 1. Syfte och tillämpningsområde. Enligt artikeln är syftet med direktivet 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.

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

Artikel 2. Definitioner. I direktivet ska enligt artikeln 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) [7] samt direktivet om

integritet och elektronisk kommunikation gälla. Enligt artikel 2.1 avses i direktivet med

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

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

c) telefonitjänst: uppringning (inbegripet rösttelefoni, röstmeddelanden, konferenssamtal och datatelefoni), tilläggstjänster (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 Internets kommunikationstjänst,

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. I artikel 3.1 sägs att genom avvikelser från artiklarna 5, 6 och 9 i direktivet om integritet och elektronisk kommunikation ska 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. Enligt artikel 3.2 ska den lagringsskyldighet som anges i punkt 1 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. Direktivet ska inte innebära krav på lagring av uppgifter rörande samtal som inte kopplats fram.

Artikel 4. Tillgång till uppgifter. Enligt artikeln ska medlemsstaterna anta åtgärder för att säkerställa att uppgifter som lagras i enlighet med direktivet endast görs tillgängliga för behöriga nationella myndigheter, i närmarre angivna fall och i enlighet med nationell lagstiftning. De förfaranden som ska följas och de villkor som ska uppfyllas för att erhålla tillgång till lagrade uppgifter i enlighet med nödvändighets- och proportionalitetskraven ska 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 ska lagras. Enligt artikeln ska medlemsstaterna 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) Abonentens 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 telefonätet.

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 (abbonenternas) 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 Internettelefonisamtal.

ii) Namn på och adress till abonnenten (abbonenterna) 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 Internettelefontjänsten 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. Enligt artikeln ska medlemsstaterna 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. I artikeln sägs att utan att det påverkar tillämpningen av de bestämmelser som antagits i enlighet med direktiv 95/46/EG och direktiv 2002/58/EG ska 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 ska vara av samma kvalitet och vara föremål för samma säkerhet och skydd som uppgifterna i nätverket.

b) Uppgifterna ska omfattas av lämpliga tekniska och organisatoriska åtgärder för att skyddas mot oavsiktlig eller olaglig

förstöring, oavsiktlig förlust eller oavsiktlig ändring, eller otillåten eller olaglig lagring av, behandling av, tillgång till eller avslöjande av uppgifterna.

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

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

Artikel 8. Krav för lagring av uppgifter. Enligt artikeln ska medlemsstaterna 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. Enligt artikeln ska varje medlemsstat utse en eller flera offentliga myndigheter som ska 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. Enligt artikel 9.2 ska de myndigheter som avses i punkt 1 vara helt oberoende när de utövar de övervakningsuppgifter som avses i den punkten.

Artikel 10. Statistik. Enligt artikeln ska medlemsstaterna säkerställa att kommissionen varje år får statistik om lagring av de uppgifter som genereras eller behandlas i samband med allmänt tillgängliga elektroniska kommunikationstjänster eller ett allmänt kommunikationsnät. Denna statistik ska 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. Enligt artikel 10.2 ska sådan statistik inte omfatta personuppgifter.

Artikel 11. Ändring av direktiv 2002/58/EG. Enligt artikeln ska följande

punkt införs i artikel 15 i direktivet om integritet och elektronisk kommunikation:

”1a. Punkt 1 ska inte tillämpas på uppgifter som specifikt ska lagras enligt Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät för de ändamål som avses i artikel 1.1 i det direktivet.

Artikel 12. Framtida åtgärder. Enligt artikeln får en medlemsstat som står inför särskilda omständigheter som föranleder en tidsbegränsad förlängning av den högsta tillåtna lagringstid som avses i artikel 6 vidta nödvändiga åtgärder. Medlemsstaten ska 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. Kommissionen ska 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 ska de nationella åtgärderna anses vara godkända. 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. Enligt artikeln ska varje medlemsstat 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. Varje medlemsstat ska särskilt vidta nödvändiga åtgärder för att säkerställa att sådan avsiktlig tillgång till eller överföring av uppgifter som lagras i enlighet med direktivet 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. Enligt artikeln ska kommissionen senast den 15 september 2010 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 ska offentliggöras. För detta ändamål ska kommissionen utreda alla synpunkter som inkommer från medlemsstaterna eller den arbetsgrupp som inrättats genom artikel 29 i direktiv 95/46/EG.

Artikel 15. Införlivande. Enligt artikeln ska medlemsstaterna sätta i kraft de bestämmelser i lagar och andra författningar som är nödvändiga för att följa detta direktiv senast den 15 september 2007. De ska genast underrätta kommissionen om detta. När en medlemsstat antar dessa bestämmelser, ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda. Medlemsstaterna ska till kommissionen överlämna texten till de centrala bestämmelser i nationell lagstiftning som de antar inom det område som omfattas av detta direktiv. Varje medlemsstat får till och med den 15 mars 2009 skjuta upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefoni och Internetbaserad e-post. Alla medlemsstater som önskar utnyttja denna bestämmelse ska underrätta rådet och kommissionen om detta i form av en förklaring när direktivet antas. Förteckningen ska offentliggöras i Europeiska unionens officiella tidning.

Artikel 16. Ikraftträdande. Enligt artikeln träder direktivet i kraft den tjugonde dagen efter det att det har offentliggjorts i Europeiska unionens officiella tidning.

Artikel 17. Adressater. Enligt artikeln riktar direktivet sig till medlemsstaterna.

2.3 Bedömning av nuläget

Det bör utfärdas uttömmande bestämmelser på lagnivå när det gäller behandling och lagring av identifieringsuppgifter som omfattas av skyddet av konfidentiella meddelanden. Enligt den gällande lagstiftningen får identifieringsuppgifter behandlas och lagras endast för vissa behov som hänför sig till teleföretagens affärsverksamhet. I praktiken förvaras identifieringsuppgifter en längre tid i första hand för faktureringsändamål. På grundval av den reglering som nu föreslås ska motsvarande uppgifter lagras för myndigheternas behov. Det handlar därmed om en betydande principiell förändring.

När elektronisk kommunikation blir allt vanligare kommer uppgifterna om kommunikationen att få en allt större betydelse i fortsättningen också med tanke på utredning av brott. För utredningen av brott är det nödvändigt att genom en måttfull skyldighet avseende lagring av uppgifter säkerställa att uppgifter som är tillgängliga för teleföretagen lagras i enlighet med förslaget tillräckligt länge på ett sätt som svarar mot myndigheternas behov.

3 Målsättning och de viktigaste förslagen

3.1 Målsättning

Förslaget syftar till att förenhetliga teleföretagens förfaranden vid lagring av identifieringsuppgifter och vissa andra uppgifter så att uppgifterna finns bevarade tillräckligt länge för myndigheternas behov. Målet är att beakta informationssamhällets behov av att skydda sig mot brottslighet samt på så vis skydda rättigheterna för såväl dem som använder och dem som tillhandahåller elektroniska kommunikationstjänster i en föränderlig nätmiljö. Regleringen syftar till att främja möjligheterna att utreda brott och därigenom tryggheten i samhället. Förenhetligandet gäller framför allt lagringstiden för uppgifterna. Syftet med direktivet bakom förslaget är dessutom att trygga överföringen av såda-

na uppgifter mellan medlemsstaterna som är nödvändiga för utredning av brott och åtalsprövning.

Målet med regleringen är också att säkerställa att skyddet för konfidentiella meddelanden och integritetsskyddet görs gällande i samband med lagringen av uppgifter.

Avsikten är att lagringsskyldigheten ska vara sådan att den kan fullgöras med skäligen kostnader och med hjälp av de tekniska lösningar som finns. Avsikten har varit att utforma en reglering som är så teknologineutral som möjligt och som kan tillämpas även i fortsättningen när tekniken utvecklas. En teknologineutral reglering står dock i motsatsförhållande till de mål som gäller exakt och noggrant avgränsad reglering. Dessutom är bestämmelserna i det bakomliggande direktivet till vissa delar teknologibundna, och därför är det omöjligt att till alla delar nå ett fullständigt teknologineutralt slutresultat för regleringen. Avsikten har dock varit att beakta den framtida tekniska utvecklingen i den mån det är möjligt.

De begränsningar som gäller Internet och avgränsningen av skyldigheterna till att gälla uppgifter som är tillgängliga för tjänsteföretagen säkerställer att regleringen kan genomföras med hjälp av de tekniska lösningar som finns och med kostnader som är överkomliga med hänsyn till målen med regleringen. Avgränsningarna är nödvändiga också med tanke på proportionalitetsprincipen och medborgarnas grundläggande fri- och rättigheter.

3.2 De viktigaste förslagen

I denna proposition föreslås ändringar av lagen om dataskydd vid elektronisk kommunikation. Genom regleringen av lagringen av identifieringsuppgifter åläggs de tjänsteföretag som är skyldiga att göra en televerksamhetsanmälan att lagra vissa uppgifter om elektronisk kommunikation i tolv månaders tid. De lagringsskyldiga tjänsteföretagen ska dock komma överens om genomförandet av lagringen av uppgifterna med inrikesministeriet innan lagringen genomförs. Lagringsskyldigheten förutsätter därmed inga åtgärder från tjänsteföretagens sida förrän de har kommit överens om lagringen med inrikesministeriet. De uppgifter som ska lagras gäll-

er bl.a. vem som har ringt ett samtal eller skickat ett e-postmeddelande och när detta har skett. Genom regleringen åläggs företagen inte att förvara innehållet i meddelandena. Uppgifterna lagras för myndigheternas behov och i synnerhet för behov i samband med utredning av brott. Regleringen gäller enbart lagring av uppgifterna. Användningen av uppgifterna och myndigheternas rätt att ta del av uppgifterna bestäms särskilt i enlighet med de gällande nationella bestämmelserna. Inte heller i de bestämmelser eller avtal enligt vilka finländska myndigheter lämnar uppgifter till myndigheter i andra länder föreslås några ändringar. Det föreslås att den myndighet för vars behov uppgifterna lagras ska svara för ersättningen för de extra kostnader som lagringen av uppgifterna medför för teleföretagen.

Dessutom föreslås bestämmelser om bedömning av de samhälleliga effekterna av Kommunikationsverkets föreskrifter.

Förslaget siktar till att säkerställa att integritetsskyddet tillgodoses på ett tillbörligt sätt. Dessutom är avsikten att trygga skyddet för konfidentiella meddelanden bl.a. genom bestämmelser om krav som gäller dataskyddet. Dessutom ska teleföretagen lagra uppgifter om behandlingen av uppgifter som med stöd av gällande lagstiftning lagras för framtida behov, dvs. bland annat uppgifter om vem som har behandlat uppgifterna, när och hur länge.

4 Propositionens konsekvenser

4.1 Ekonomiska konsekvenser

Enligt Kommunikationsverkets beräkningar uppgår de totala investeringskostnaderna för genomförandet i Finland till 5-8 miljoner euro när lagringstiden för uppgifterna är 12 månader. De årliga driftskostnaderna är betydligt mindre; enligt de nuvarande beräkningarna rent av under 10 procent av investeringskostnaderna. Kostnaderna för genomförandet av förslaget beror i väsentlig grad av detaljerna i det tekniska genomförandet och av myndigheternas behov. Beloppet och periodiseringen av investeringskostnaderna kan påverkas av den faktiska tidpunkten för när vart och ett av de nuvarande tjänsteföretagen

ansluter sig till systemet, av att eventuella nya aktörer inträder på marknaden och av att systemet eventuellt bör förnyas.

De kostnader som förslaget medför för teleföretagen ska ersättas av den myndighet för vars verksamhet och behov uppgifterna lagras.

Utöver kostnaderna för den tekniska lagringen av identifieringsuppgifter kommer myndigheterna att åsamkas kostnader för uppbyggnaden av ett tekniskt system för den uppföljning och rapportering som genererar statistiska uppgifter och för den växande arbetsmängd som det tekniska genomförandet och underhållet föranleder

Förslaget bedöms inte ha några konsekvenser med tanke på Kommunikationsverkets verksamhetsbudget.

4.2 Konsekvenser för myndigheternas verksamhet

Det viktigaste syftet med det direktiv som ligger till grund för förslaget är att förbättra i synnerhet polisens verksamhetsmöjligheter genom att det säkerställs att teleföretagen under tillräckligt lång tid förvarar vissa av de uppgifter om kommunikationen som de har tillgång till och som myndigheterna behöver. Propositionen har konsekvenser som effektiviserar polisens och vissa myndigheters verksamhet.

4.3 Samhälleliga konsekvenser

Den föreslagna regleringen handlar om en betydande principiell förändring, eftersom det föreslås att uppgifter ska lagras för myndigheternas framtida behov och att uppgifter ska lagras i fråga om alla abonnenter och användare av kommunikationen för tjänsteföretag som lagrar uppgifterna.

Förslaget effektiviserar polisens verksamhet och har därmed konsekvenser när det gäller att främja tryggheten och säkerheten i samhället. Förslaget kan också minska antalet brott, eftersom det ökar risken för att någon ska bli fast.

Teoretiskt sett ökar alla former av förvaring av uppgifter om medborgarna riskerna i fråga om integritetsskyddet. I den föreslagna regleringen är avsikten dock att med alla me-

del säkerställa integritetsskyddet och medborgarnas övriga grundläggande fri- och rättigheter. Det bedöms därför att förslaget i praktiken inte har några negativa konsekvenser för medborgarnas grundläggande fri- och rättigheter.

Förslaget kan ha smärre konsekvenser för medborgarnas förtroende i samband med användningen av olika slags elektroniska tjänster och kommunikationstjänster. Det beror på att lagringsskyldigheten felaktigt kan relateras till tanken om kontroll av medborgarna, vilket åtminstone principiellt kan ha konsekvenser som minskar förtroendet.

Eftersom de extra kostnader som regleringen medför för teleföretagen ska ersättas av den myndighet för vars verksamhet uppgifterna lagras, har förslaget inte några negativa konsekvenser för konkurrenskraften hos aktörerna inom kommunikationsbranschen. Propositionen bedöms inte heller ha några andra konsekvenser för konkurrensen.

5 Beredningen av propositionen

5.1 Beredningsskeden och beredningsmaterial

Propositionen har beretts som tjänsteuppdrag vid kommunikationsministeriet. Under beredningen fördes ingående bilaterala diskussioner om utkastet till bestämmelser med bl.a. inrikesministeriet, centralkriminalpolisen, skyddspolisen, gränsbevakningsväsendet, justitieministeriet, Kommunikationsverket, Electronic Frontier Finland EFFI ry, FiCom ry, TeliaSonera Finland Abp, Finnetförbundet, Elisa Abp och Dataombudsmannens byrå. Under beredningen presenterades förslagen till bestämmelser vid olika seminarier och evenemang. I juni 2007 sändes propositionsutkastet dessutom för inofficiella kommentarer till de ovan nämnda, före den egentliga remissbehandlingen.

5.2 Remissyttranden och hur de har beaktats

Propositionsutkastet sändes för utlåtande till alla ministerier och flera hundra olika

sammanslutningar. Samtidigt begärdes utlåtande om Kommunikationsverkets utkast till en föreskrift om saken och utlåtande om utkastet till rekommendationer för tillämpningen av föreskriften. Remissmaterialet har varit tillgängligt på kommunikationsministeriets webbsidor ända från det att remissbehandlingen inleddes.

I utlåtandena förde teleföretagen fram sina synpunkter på vissa bestämmelser som enligt deras åsikt borde preciseras och göras tydligare. Att förslaget utgår från att kostnaderna ska ersättas ansågs motiverat av alla utom handels- och industriministeriet. EFFI ry tog upp flera frågor, bl.a. vilka konsekvenser propositionen kommer att ha i fråga om den personliga integriteten, och ansåg att förslaget inte uppfyller grundlagens krav. Centralkriminalpolisen och skyddspolisen framförde sin oro över bl.a. det faktum att utvecklingen av tjänster inom teleföretagsbranschen i fortsättningen kan leda till att de uppgifter som för närvarande är tillgängliga med tanke på myndigheternas behov inte kommer att vara tillgängliga i framtiden och att de föreslagna skyldigheterna i anslutning till statistikföringen inte får vara mera omfattande än vad som förutsätts i direktivet. Inrikesministeriets polisavdelning och Tullstyrelsen framförde bl.a. att de statistiska uppgifterna bör lämnas till riksdagens justitieombudsman i anslutning till berättelser om teleavlyssning och teleövervakning i stället för till Kommunikationsverket. Statens revisionsverk nämnde bl.a. behovet av att överväga myndighetsnätverkens ställning. Stakes oroade sig för att konfidentialiteten hos social- och hälsovårdsuppgifterna inte ska bevaras, men också för att integritetsskyddet i allmänhet ska äventyras och önskade att den föreslagna lagen antingen bör vara temporär eller stiftas i grundlagsordning. Undervisningsministeriet, Upphovsrättens informations- och övervakningscentral rf, Teosto rf och Kopiosto rf framhöll att innehavare av upphovsrätt och de instanser som representerar dem borde få de uppgifter som nu ska lagras för myndigheternas behov enligt lagen om upphovsrätt. En mängd andra utvecklingsförslag fördes fram i utlåtandena och ett flertal ändringar gjordes i förslaget utgående från utlåtandena.

6 Samband med andra propositioner

Delvis samtidigt med detta förslag till ändring av lagen om dataskydd vid elektronisk kommunikation har även ett annat, men separat, förslag till ändring av samma lag beretts vid kommunikationsministeriet. Syftet med det senare förslaget är att klargöra sammanslutningsabbonnenternas rätt att behandla

identifieringsuppgifter för att tekniskt utveckla tjänster och i sådana fall då kommunikationsnät och kommunikationstjänster används på ett obehörigt sätt. Enligt den föreslagna lagändringen ska sammanslutningsabbonnenter också ges rätt att behandla identifieringsuppgifter i sådana fall då företags-hemligheter som är väsentliga för näringsverksamheten har röjts.

DETALJMOTIVERING

1 Lagförslag

1.1 Lagen om dataskydd vid elektronisk kommunikation

Syftet med de föreslagna bestämmelserna om lagring av uppgifter är att säkerställa att vissa, för teleföretagen tillgängliga uppgifter i anslutning till elektronisk kommunikation lagras tillräckligt länge för att de ska kunna användas för att förebygga och utreda framför allt allvarliga brott och sörja för att sådana brott blir föremål för åtalsprövning så som föreskrivs särskilt i lag.

Syftet med regleringen är således att försöka säkerställa att teleföretagen lagrar sådana uppgifter som de har tillgång till och som avses i direktivet om lagring av identifieringsuppgifter och på ett sådant sätt som svarar mot myndigheternas behov. De uppgifter som ska lagras är sådana som teleföretagen redan för närvarande också annars lagrar för t.ex. sin fakturering eller för något annat ändamål som hänför sig till deras verksamhet, dvs. de är tillgängliga för teleföretagen. Avsikten är att den föreslagna regleringen ska säkerställa att teleföretagen enligt så enhetliga principer som möjlighet åtminstone en viss tid förvarar vissa av sina tillgängliga uppgifter. Uppgifterna ska lagras för den händelse att det senare uppkommer en situation där polisen behöver uppgifterna för att förebygga och utreda brott eller för att se till att brott blir föremål för åtalsprövning.

Den föreslagna regleringen utgår från att syftet med förslaget bara är att säkerställa att vissa, för teleföretaget tillgängliga uppgifter hålls i förvar hos teleföretaget en viss tid. Förutsättningarna för utnyttjande av uppgifterna, dvs. myndigheternas rätt få uppgifter, bestäms däremot enligt andra bestämmelser, såsom polislagen, tvångsmedelslagen eller tullagen. Det föreslås således inte några ändringar av bestämmelserna om myndigheternas rätt att få uppgifter. Myndigheterna ska även i fortsättningen få utnyttja uppgifter som teleföretagen förfogar över endast när de har en lagbaserad rätt att få uppgifterna av ett teleföretag. Enligt artikel 4 i direktivet om lagring av identifieringsuppgifter ska med-

lemsstaterna anta åtgärder för att säkerställa att uppgifter som lagras i enlighet med direktivet endast görs tillgängliga för behöriga nationella myndigheter, i närmare angivna fall och i enlighet med nationell lagstiftning. De förfaranden som ska följas och de villkor som ska uppfyllas för att erhålla tillgång till lagrade uppgifter i enlighet med nödvändighets- och proportionalitetskraven ska 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 det innehåll som fastställts genom rättspraxisen vid Europeiska domstolen för mänskliga rättigheter. I Finland uppfyller de gällande bestämmelserna om myndigheternas rätt att få uppgifter synnerligen väl de krav som ställs i direktivet. Det föreslås därför inte några ändringar av den gällande regleringen till denna del. Det föreslås inte heller någon ändring av tillsynsmyndigheternas rätt att ta del av uppgifterna och följaktligen har Kommunikationsverket rätt att få uppgifter på samma villkor som hittills. Med beaktande av direktivets syften och villkoren för överföring av uppgifter är det nödvändigt att se till att endast myndigheter har rätt att ta del av de uppgifter som ska lagras av teleföretagen.

De uppgifter som enligt förslaget ska lagras är exakt desamma som teleföretagen redan i dagens läge förvarar för egna behov och som myndigheterna kan ta del av med stöd av sin nuvarande rätt att få uppgifter. Det föreslås inte att uppgifterna ska lagras separat, utan endast att de ska lagras i tolv månader för myndigheternas behov. Eftersom det därmed handlar om exakt samma uppgifter som myndigheterna kan ta del av med stöd av sina nuvarande rättigheter att få uppgifter och eftersom det inte förutsätts t.ex. att uppgifterna ska införas på någon separat plats är det nödvändigt och motiverat att myndigheterna alltjämt ska kunna få de lagrade uppgifterna under samma förutsättningar som för närvarande. Av samma orsak är det i praktiken mycket problematiskt och eventuellt omöjligt att genomföra en sådan ändring av rättigheterna

att få uppgifter som skulle innebära att de lagrade uppgifterna t.ex. efter en viss tid omfattas av annorlunda bestämmelser om rätten att få uppgifter.

Enligt 3 § 7 mom. i lagen om dataskydd vid elektronisk kommunikation tillämpas lagen inte på myndighetsverksamhet i myndighetsnät som avses i kommunikationsmarknadslagen eller i andra kommunikationsnät som konstruerats för att tillgodose behov i anslutning till allmän ordning och säkerhet, landets försvar, räddningsuppgifter, befolkningsskydd eller trafiksäkerhet till lands, till sjöss, på räls eller i luften. Därmed gäller de föreslagna skyldigheterna att lagra uppgifter inte heller myndighetsverksamhet i myndighetsnät. Enligt kommunikationsmarknadslagen avses med myndighetsnät ett kommunikationsnät som byggts för behov i anslutning till allmän ordning och säkerhet, räddningsuppgifter eller befolkningsskyddet och i vilket anslutningar kan tillhandahållas utom myndigheterna även andra användargrupper som är nödvändiga med hänsyn till skötseln av dessa uppgifter. Som ett exempel på ett sådant myndighetsnät kan nämnas myndighetsradionätet (VIRVE), vars syfte är att effektivisera samarbetet myndigheterna emellan i såväl normalförhållanden som i undantagsförhållanden, och vilkas huvudsakliga användare är statliga och kommunala säkerhetsmyndigheter. I den föreslagna lagen avses med myndighetsnät även försvarsmaktens kommunikationsnät och kommunikationsnät som byggts för säkerhetsbehoven i anslutning till olika kommunikationsformer. Den föreslagna lagen tillämpas dock på annan kommunikation i myndighetsnäten, såsom privata samtal. På motsvarande sätt tillämpas lagen på annan än myndighetskommunikation t.ex. i sådana fall då myndighetsnätets anslutningar tillhandahålls sådana samslutningsabonnenter som ansvarar för energidistribution och deras användare.

Syftet med det direktiv som ligger till grund för förslaget är att vidmakthålla den europeiska kapaciteten att ingripa även i gränsöverskridande brottslighet genom att de nationella bestämmelserna om lagring av uppgifter förenhetligas. I de bestämmelser enligt vilka myndigheterna lämnar uppgifter till myndigheterna i andra länder föreslås

inga ändringar. Därmed kan myndigheterna i enlighet med nu gällande avtal och bestämmelser lämna ut sådana uppgifter som de erhållit från teleföretag, och som teleföretagen enligt förslaget ska lagra, till utländska myndigheter. Bestämmelser om att lämna ut uppgifter till utlandet finns i lagen om behandling av personuppgifter i polisens verksamhet (761/2003).

2 §. Definitioner. Det föreslås att lagen kompletteras med definitioner av tjänsteföretag och Internettelefonitjänst.

Enligt den nya 14 a punkten avses med tjänsteföretag företag enligt 2 § 19 punkten i kommunikationsmarknadslagen. Med tjänsteföretag avses enligt kommunikationsmarknadslagen ett företag som överför meddelanden i ett kommunikationsnät som det förfogar över eller har fått tillgång till av ett nätföretag eller som distribuerar eller tillhandahåller meddelanden i ett masskommunikationsnät. Förslaget hänför sig till lagringsskyldigheten enligt 14 a §, som föreslås riktas betydligt mera noggrant avgränsat till tjänsteföretag än till teleföretag.

Enligt den föreslagna nya 14 b punkten avses med Internettelefonitjänst en tjänst som ett teleföretag erbjuder och som fram till slutkunderna baserar sig på Internetprotokoll och möjliggör samtal.

I förslaget är det nödvändigt att avgränsa och åtskilja de tjänster som berörs av skyldigheten att lagra uppgifter. Det beror på att enligt det direktiv som ska genomföras gäller olika slags lagringsskyldighet för olika tjänster, och de aktuella nya skyldigheterna omfattar inte tjänster enligt definitionerna i den gällande lagstiftningen.

De skyldigheter som anges i den föreslagna 14 a § gäller endast Internettelefonitjänster som tjänsteföretagen själva tillhandahåller. Exempelvis sådana Internetsamtal som rings via ett program för ändamålet och så att de förmedlas i kommunikationsnätet från en dator till en annan utan någon Internettelefonitjänst som uttryckligen tillhandahålls av ett tjänsteföretag omfattas därför inte av skyldigheterna att lagra uppgifter.

Teleföretagen håller successivt på att ersätta det traditionella stamnätet i telefonnätet med nät som baserar sig på Internetprotokoll. Enligt definitionen innebär inte enbart an-

vändningen av ett Internetprotokoll att en tjänst blir en Internettelefontjänst, eftersom tjänsten enligt definitionen ska basera sig på ett Internetprotokoll fram till slutanvändarna för att det ska vara fråga om en sådan tjänst.

Det föreslås inte några ändringar i definitionen av identifieringsuppgift.

8 §. Allmänna bestämmelser om behandlingen. Det föreslås att den gällande paragrafen ändras så att motsvarande allmänna behandlingsprinciper som för närvarande tillämpas på behandlingen av identifieringsuppgifter ska tillämpas också på behandlingen och lagringen av de uppgifter som enligt förslaget ska lagras. Lagring ingår begreppsmässigt i definitionen av behandling, och målet uppnås därmed genom att den nuvarande hänvisningen till 9-14 § ändras till en hänvisning till 3 kap. Det handlar i hög grad om motsvarande principer som också tillämpas vid behandlingen av personuppgifter enligt personuppgiftslagen, dvs. principen om proportionalitet och respekten för integritetsskyddet. Utöver annan behandling ska även lagring genomföras med respekt för skyddet för konfidentiella meddelanden. I den föreslagna ändrade paragrafen uttrycks principen om att de lagrade uppgifterna får lämnas ut endast till dem som har rätt att behandla uppgifterna i förekommande fall. Enligt bestämmelsen gäller det att efter behandlingen se till att meddelandena och identifieringsuppgifterna förstörs eller görs anonyma, vilket också gäller lagrade identifieringsuppgifter. De principer som anges i bestämmelsen gäller behandlingen och lagringen av identifieringsuppgifter. Personuppgiftslagen ska däremot alltså tillämpas på kundregisteruppgifter som ska lagras.

14 a §. Skyldighet att lagra uppgifter för myndigheternas behov. I 1 mom. ingår den skyldighet att lagra uppgifter som är central med tanke på lagförslaget.

Det handlar om ett undantag från de gällande behandlingsreglerna enligt 3 kap. Enligt den föreslagna bestämmelsen ska ett tjänsteföretag som är skyldigt att göra televerksamhetsanmälan, i fråga om de uppgifter som det har tillgång se till att de uppgifter som nämns i artikel 5 i direktivet om lagring av identifieringsuppgifter lagras för myndigheternas behov i tolv månader från det datum

kommunikationen ägde rum. Uppgifterna består av vissa uppgifter som behövs för att spåra och identifiera fysiska eller juridiska personer som är användare, för att identifiera tidpunkten och varaktigheten för en tjänst, för att identifiera lokaliseringen av en mobilteleapparat samt för att identifiera telefoni-tjänsten, kommunikationsabonnemanget eller kommunikationstypen. Begreppsmässigt utgör en del av uppgifterna identifieringsuppgifter, en del lokaliseringsuppgifter och en del personuppgifter.

Med stöd av de gällande bestämmelserna om behandling av identifieringsuppgifter behandlas och lagras identifieringsuppgifter för teleföretagens egna behov av olika slag. Det kan hända att vissa teleföretag med stöd av någon av bestämmelserna om behandling av identifieringsuppgifter i 3 kap. redan nu förvarar vissa av de uppgifter som enligt den föreslagna regleringen ska lagras så, att uppgifterna förvaras rent av längre än tolv månader. Den föreslagna regleringen begränsar inte heller i fortsättningen på något sätt möjligheterna att behandla eller lagra uppgifter för teleföretagens egna behov. Uppgifterna får således även i fortsättningen t.ex. för fakturering lagras en längre tid än tolv månader, om teleföretaget har rätt att göra det med stöd av någon bestämmelse om behandling. Om ett tjänsteföretag i dagens läge behandlar och lagrar tillgängliga uppgifter en kortare tid än tolv månader, ska tjänsteföretaget enligt den gällande lagstiftningen antingen förstöra uppgifterna eller göra dem anonyma efter det att ändamålet med behandlingen har upphört. Enligt den föreslagna regleringen ska uppgifterna inte längre förstöras förrän förvaringstiden på tolv månader har gått ut, vilket innebär att tjänsteföretaget ska förlänga lagringstiden till tolv månader. Efter det att teleföretagets eget behov av att behandla vissa uppgifter upphört och lagringen av uppgifterna för myndigheternas behov vidtagit, får detta slag av uppgifter enbart användas för myndigheternas behov och inte längre för teleföretagets behov. Den föreslagna lagringsskyldigheten gäller dock bara vissa uppgifter om nämns i direktivet. De nuvarande bestämmelserna och förfarandena ska därför alltså tillämpas i fråga om övriga uppgifter som tjänsteföretagen behandlar och lagrar med

stöd av de nuvarande bestämmelserna om behandling. När det gäller behandling och lagring av de personuppgifter som nämns i direktivet har den föreslagna regleringen motsvarande förhållande till personuppgiftslagen.

Lagringsskyldigheten riktas entydigt till tjänsteföretag, som definieras i kommunikationsmarknadslagen. Skyldiga att lagra t.ex. e-postrelaterade uppgifter som ska lagras är därmed uttryckligen de tjänsteföretag som tillhandahåller e-posttjänsterna. Enligt förslaget ska lagringsskyldigheten inte gälla andra aktörer än tjänsteföretag som är skyldiga att göra televerksamhetsanmälan. Skyldigheten att lagra uppgifter gäller därmed inte e-posttjänster som tillhandahålls av tidningar inom datorbranschen eller e-posttjänster som tillhandahålls av olika slags andra tjänsteföretag än sådana som är skyldiga att göra televerksamhetsanmälan. Skyldiga att lagra uppgifter är på motsvarande sätt inte heller husbolag eller andra motsvarande aktörer som inte är tjänsteföretag. Skyldigheten riktas till tjänsteföretag, men tjänsteföretagen ska själv ordna lagringen antingen på egen hand eller i samråd med ett nätföretag. I vissa situationer måste ett tjänsteföretag eventuellt sörja för lagringsskyldigheten t.ex. genom avtalsrättsliga förfaranden med ett nätföretag så att nätföretaget eller någon annan tredje part i praktiken lagrar uppgifterna för tjänsteföretagets räkning. Det är också i sådana situationer uttryckligen tjänsteföretaget som är skyldigt att se till att de tillgängliga uppgifterna lagras i enlighet med förslaget. Lagringsskyldigheten har begränsats till att gälla tjänsteföretag som är skyldiga att göra televerksamhetsanmälan. Enligt 13 § i kommunikationsmarknadslagen gäller att innan allmän televerksamhet inleds ska en skriftlig anmälan göras till Kommunikationsverket. Anmälningsskyldigheten gäller inte allmän televerksamhet om den är tillfällig, riktar sig till ett litet antal mottagare eller annars är av ringa betydelse. Närmare bestämmelser om televerksamhet av ringa betydelse har utfärdats genom statsrådets förordning om televerksamhet av ringa betydelse (675/2003). I Finland finns det för närvarande ca 160 tjänsteföretag som gjort televerksamhetsanmälan.

Enligt det föreslagna 2 mom. gäller tjänsteföretagens lagringsskyldighet sådana uppgifter i anslutning till telefonitjänster eller tilläggstjänster i fasta nät eller telefonitjänster, tilläggstjänster, textmeddelandetjänster, EMS-tjänster eller multimedietjänster i mobiltelenät, Internetåtkomsttjänster, elektroniska posttjänster och Internettelefonitjänster som tillhandahålls av ett tjänsteföretag. Lagringsskyldigheten gäller inte andra tjänster till någon del. Samtal omfattar t.ex. rösttelefoni, röstmeddelanden, konferenssamtal och datatelefoni. Tilläggstjänster omfattar t.ex. omstyrning och överflyttning av samtal. Meddelandetjänster i mobiltelenät omfattar bl.a. SMS-, EMS- och multimedietjänster (bildmeddelande- och videotelefonitjänster). I telefonitjänster i mobiltelenät ingår också anonyma tjänster som betalts på förhand, dvs. så kallade prepaid-tjänster. I fråga om Internetåtkomsttjänster, elektroniska posttjänster och Internettelefonitjänster gäller lagringsskyldigheten dessutom tillgängliga uppgifter endast i anslutning till tjänster som tjänsteföretagen själva tillhandahåller. Exempelvis i fråga om Internetbaserade samtal omfattar lagringsskyldigheten endast Internettelefonitjänster som teleföretagen själva tillhandahåller. Lagringsskyldigheten gäller inte alla tjänster enligt principerna för serverlösa nät eller samtal med hjälp av sådana eller andra motsvarande tjänster där de uppgifter som enligt förslaget ska lagras inte är tillgängliga för tjänsteföretagen på ett sådant sätt som förutsätts för lagringsskyldigheten. Tjänster av detta slag som uteslutande finns på Internet uppfyller inte heller nödvändigtvis definitionen av kommunikationstjänst i kommunikationsmarknadslagen.

Lagringsskyldigheten gäller inte till någon del innehållet i meddelandena eller identifieringsuppgifter som samlas vid bläddring på webbsidor. Med stöd av lagringsskyldigheten får således inte innehållet i meddelandena lagras och inte heller t.ex. uppgifter om vilka webbsidor en person har besökt. Bestämmelsen är informativ, vilket innebär att lagringsskyldigheten inte förutsätter att innehållet i meddelandena lagras och att den inte ger rätt att lagra innehållet i meddelandena. Om rätt att lagra innehållet i meddelanden följer av någon annan bestämmelse eller lag, hindrar

inte den föreslagna bestämmelsen som sådan lagenlig lagring av innehållet i meddelandena.

Lagringsskyldigheten gäller under samma förutsättningar även lagring av motsvarande uppgifter i anslutning till samtal som har kopplats men som inte besvarats eller som har blivit föremål för en driftsätgärd i nätet. Det väsentliga i fråga om sådana s.k. obesvarade samtal är att samtalet har kopplats. Med hänvisningen till driftsätgärder i nätet avses situationer där driftsätgärderna har förhindrat samtalet från att genomföras. Om samtalet inte har kunnat kopplas t.ex. på grund av ett tekniskt fel, omfattas samtalet inte av lagringsskyldigheten.

En viktig förutsättning för lagringsskyldighet är att uppgifterna är tillgängliga och har genererats eller behandlats i samband med tillhandahållande av teleföretagets allmänt tillgängliga kommunikationstjänster under de förutsättningar som anges i 10-14 § eller i personuppgiftslagen. Med allmänt tillgängliga kommunikationstjänster avses att lagringsskyldigheten gäller endast allmän televerksamhet i ett allmänt telenät. Förutsättningen att kommunikationstjänsterna ska vara allmänt tillgängliga är en central avgränsning i fråga om lagringen av uppgifter och på basis av den lagras endast uppgifter som är tillgängliga för tjänsteföretaget. Det innebär att det inte är nödvändigt att lagra alla de uppgifter i teleföretagens nät som nämns i direktivet och i Kommunikationsverkets föreskrift. Endast sådana i den ovan nämnda föreskriften nämnda uppgifter som genererats eller behandlats i samband med tillhandahållandet av tjänsteföretagets tjänster och som tjänsteföretaget också annars lätt kommer över utan några särskilda åtgärder ska lagras, eftersom tjänsteföretaget redan lagrar uppgifterna för sin egen verksamhet. Det innebär att ett teleföretag inte behöver skaffa eller generera en sådan uppgift för lagring som ingår i artikel 5 i direktivet om lagring av identifieringsuppgifter, om uppgiften inte är tillgänglig för teleföretaget. I praktiken handlar det därmed bara om uppgifter som tjänsteföretagen redan för närvarande behandlar med stöd av 9-14 § i lagen om dataskydd vid elektronisk kommunikation eller med stöd av personuppgiftslagen. När upp-

gifter för närvarande sparas lagligt i högst åtta månader, t.ex. för fakturering, ska uppgifterna i fortsättningen lagras på motsvarande sätt i ytterligare fyra månader. Det handlar således inte om nya uppgifter eller nya sätt att lagra uppgifterna, vilket är av betydelse också för bedömningen av förslaget konsekvenser för en inskränkning av skyddet för privatlivet samt i fråga om kostnaderna för samhället. För att uppgifterna ska kunna anses vara tillgängliga, bör de också tidsmässigt vara tillgängliga tillräckligt länge. Tillgänglighetskravet kan inte anses vara uppfyllt t.ex. i sådana situationer där vissa uppgifter är tillgängliga för tjänsteföretaget bara några dagar. Kravet att uppgifterna ska vara tillgängliga innebär också att om tjänsteföretagen i framtiden utvecklar sina tjänster så att vissa uppgifter inte längre behandlas för tillhandahållandet av en tjänst, är dessa uppgifter inte därefter tillgängliga och behöver således inte längre lagras. Regleringen begränsar därmed inte tjänsteföretagens möjligheter att utveckla servicen, men å andra sidan står uppgifterna inte längre till förfogande för behov i samband med utredning av brott.

Det kan bedömas att den föreslagna lagringstiden står i rätt proportion till de mål som eftersträvas med regleringen och till de kostnader som lagringsskyldigheten medför. Det är mycket vanligt att brott uppdrags först en tid efter det att de har begåtts. Dessutom kräver utredningen av brott oundvikligen sin tid, och då kan behovet av vissa uppgifter om kommunikationen uppkomma först flera månader efter det att brottet begicks. En bedömning utifrån bakgrundsutredningarna i samband med beredningen av förslaget ger vid handen att teleföretagen redan för närvarande i minst tolv månaders tid lagrar en stor del av de uppgifter som förslaget gäller. Eftersom förslaget inte inrymmer några ytterligare nya uppgifter som ska lagras, står förlängningen av lagringstiden och förenhetligandet tolv månader i rätt proportion till målen med och verkningarna av regleringen. Under beredningen av det direktiv som genomförs genom detta förslag förutsatte riksdagen att uppgifterna i vilket fall som helst inte bör lagras längre än tolv månader.

En närmare definition och tekniska detaljer i fråga om de uppgifter som med stöd av det

föreslagna 4 mom. ska lagras framgår av en teknisk föreskrift som utfärdas av Kommunikationsverket. Inom ramen för de krav som uppställs i direktivet om identifieringsuppgifter anger Kommunikationsverket genom sin juridiskt bindande föreskrift närmare vilka uppgifter som tjänsteföretagen ska lagra. Bemyndigandet för Kommunikationsverket att meddela föreskrifter begränsas till de uppgifter som enligt direktivet ska lagras. Bestämmelsen är nödvändig för preciseringen av tekniska detaljer i fråga om de uppgifter som ska lagras. Vid beredningen av föreskriften gäller det att höra framför allt inrikesministeriet och de lagringsskyldiga tjänsteföretagen.

Den föreslagna paragrafen och Kommunikationsverkets föreskrift om de uppgifter som ska lagras innebär att artiklarna 5 och 6 i direktivet om lagring av identifieringsuppgifter genomförs nationellt.

14 b §. Skyldigheter och förfaringsätt som ska iakttas vid behandlingen av uppgifter som lagras för myndigheternas behov. Enligt det föreslagna 1 mom. ska ett tjänsteföretag som är skyldigt att lagra uppgifter komma överens om genomförandet av lagringen med inrikesministeriet innan lagringsskyldigheten fullgörs. Målet är att säkerställa att uppgifterna lagras enligt myndigheternas behov. Syftet med den föreslagna bestämmelsen är att föra fram förfarandet enligt 98 § i den gällande kommunikationsmarknadslagen. Enligt förfarandet ska den myndighet för vilken en åtgärd genomförs och det teleföretag som genomför åtgärderna för myndighetens behov komma överens om genomförandet och samtidigt om de kostnader som myndigheten ska betala teleföretaget. Syftet med bestämmelsen är att säkerställa att det inte uppkommer sådana situationer där vissa teleföretag självständigt börja fullgöra sin lagringsskyldighet och sänder myndigheterna en räkning för åtgärderna i efterhand. En sådan situation kan bli oskälig för den myndighet som ska betala alla extra kostnader för lagringen och kan också äventyra en sådan lagring av uppgifterna som svarar mot myndigheternas behov. I praktiken är det nödvändigt att de myndigheter för vilkas behov uppgifterna lagras har möjlighet att före genomförandet av lagringen bedöma om lagringen

och genomförandet av den är förenliga med myndighetens behov. Den föreslagna bestämmelsen om överenskommelse om genomförandet av lagringen behövs uttryckligen därför att det föreslås att alla extra kostnader som teleföretagen orsakas med anledning av myndighetens behov ska betalas av myndigheten. Myndigheten bör därför ha möjlighet att påverka det praktiska genomförandet av lagringen. Lagringsskyldigheten förutsätter inga åtgärder avseende lagringen av uppgifterna från de tjänsteföretag som är skyldiga att göra en televerksamhetsanmälan förrän de har kommit överens om genomförandet av lagringen med inrikesministeriet. Eftersom det likväl handlar om lagringsskyldighet, får tjänsteföretag som är skyldiga att göra en televerksamhetsanmälan inte heller före överenskommelsen med inrikesministeriet lagra sådana uppgifter som förslaget gäller någon längre tid än de gällande bestämmelserna berättigar till.

Internetåtkomsttjänster avviker från de övriga uppgifter som ska lagras och som inte omfattas av övergångsbestämmelsen i 44 § på så vis att det beträffande Internetåtkomsttjänsterna är nödvändigt för teleföretagen att utforma nya lösningar då det gäller utlämnande av uppgifter till myndigheterna. I fråga om dessa tjänster bör det därför reserveras tillräckligt med tid för genomförandet av lagringen så att genomförandet på en gång blir fungerande och ändamålsenligt utan några temporära lösningar. När det gäller Internetåtkomsttjänster bör denna omständighet beaktas i samband med att inrikesministeriet och tjänsteföretaget kommer överens om hur lagringen ska genomföras.

I det föreslagna 1 mom. anges två centrala principer för regleringen, dvs. att man vid lagringen av uppgifterna bör undvika att uppgifterna i onödan lagras av fler tjänsteföretag än ett och att lagringen bör genomföras så att uppgifterna utan onödig fördröjning kan tillställas de myndigheter som är berättigade att ta del av dem. Med principen om undvikande av flerdubbel lagring avses t.ex. att om ett meddelande passerar flera teleföretags nät, vilket är mycket vanligt, gäller det att i mån av möjlighet i samband med varje kommunikationstransaktion försöka finna det tjänsteföretag som är skyldigt att lagra upp-

gifterna om en viss kommunikation. Situationen där flera teleföretag lagrar samma uppgifter bör således undvikas. Enligt det föreslagna momentet gäller dessutom att ett tjänsteföretag som är skyldigt att lagra uppgifter om så krävs ska sörja för fullgörandet av skyldigheten i samråd med ett nätföretag så att även de uppgifter enligt 14 a § som nätföretaget behandlar för genomförandet av tjänsteföretagets tjänster och enligt tjänsteföretagets behov lagras. Det är dock fortfarande uttryckligen fråga om tjänsteföretagets skyldighet. Lagringen av uppgifterna kan genomföras på många sätt, och avsikten är att bestämmelsen ska visa att även om ett tjänsteföretag är det primära föremålet för lagringsskyldigheten, ska det genomföra lagringen i samarbete med ett nätföretag, t.ex. om nätföretaget förfogar över och har tillgång till sådana identifieringsuppgifter som anger läget i mobiltelenätet som nätföretaget behandlar uttryckligen för att utföra tjänsteföretagets tjänster. Om det inte krävs några sådana uppgifter som nätföretaget förfogar över för att tillhandahålla tjänsteföretagets tjänster, behandlas dessa uppgifter inte för tjänsteföretagets behov och för utförande av tjänsteföretagets tjänster på det sätt som avses i bestämmelsen. Det är i sådana fall självklart att inte heller nätföretaget behöver lagra detta slag av uppgifter för myndigheternas behov. I 95 § i kommunikationsmarknadslagen bestäms om teleföretags skyldighet att utrusta sina nät och tjänster med sådana tekniska hjälpmedel och egenskaper att teleavlyssning och teleövervakning kan genomföras. Dessutom ska uppgifterna lagras så att de utan onödigt dröjsmål kan tillställas myndigheter som är berättigade att genomföra teleövervakning. Det föreslagna 1 mom. innebär att artikel 8 i direktivet om lagring av identifieringsuppgifter genomförs nationellt.

Enligt det föreslagna 1 mom. ska ett tjänsteföretag se till att abonnenten har tillgång till information om lagringsskyldigheten och syftet med lagringen. Bestämmelsen är principiellt viktig för att de personer som står som föremål för de uppgifter som lagras är medvetna om vad som görs med uppgifterna om deras kommunikation. Tjänsteföretag kan informera om lagringen t.ex. genom att in-

formera om detta på sina webbsidor, i samband med kundinformation eller på något annat lämpligt sätt.

I det föreslagna 2 mom. sägs att bestämmelser om ersättning för de kostnader som förorsakas av att lagringsskyldigheten fullgörs och av att motsvarande beredskap upprätthålls finns i 98 § i kommunikationsmarknadslagen. Förslaget är principiellt betydelsefullt och syftar till att utforma en entydig modell för ersättningen av kostnaderna. Teleföretagen ska få ersättning för alla extra kostnader för lagringen uttryckligen med stöd av ersättningsbestämmelserna i kommunikationsmarknadslagen. I fråga om kostnaderna för lagring ska inte ersättningsbestämmelserna i någon annan lag tillämpas. Den betalningsskyldiga myndigheten är entydigt den myndighet i vars intresse och för skötseln av vars uppdrag uppgifterna lagras. Med tanke på det egendomsskydd som tryggats i grundlagen är det ofrånkomligt att tjänsteföretagen inte får orsakas extra kostnader på grund av lagringsskyldigheten. I 98 § 3 mom. i gällande kommunikationsmarknadslag konstateras att teleföretagen inte får använda system, utrustning eller programvara som bekostats av myndigheten för sin kommersiella verksamhet. De uppgifter som enligt det aktuella förslaget ska lagras är emellertid exakt samma uppgifter som teleföretagen enligt nuvarande praxis lagrar för den egna affärsverksamheten. På grund av myndigheternas behov blir det nödvändigt för teleföretagen att i fortsättningen lagra dessa uppgifter längre än tidigare. Avsikten med förslaget är att förlänga lagringstiden för uppgifterna för att säkerställa att de sparas för myndigheternas behov.

Det föreslagna 2 mom. inrymmer en informativ bestämmelse, enligt vilken det i 4 kap. 4 b-c § i tvångsmedelslagen bestäms om föreläggande av säkra data för utredningen av det brott som undersöks. Enligt bestämmelsen i fråga gäller att om det finns skäl att anta att data som kan ha betydelse för utredningen av det brott som undersöks går förloerade eller förändras, kan en anställningsberättigad tjänsteman ålägga den som innehar eller har bestämmanderätten över dessa data, dock inte den som misstänks för brott, att säkra uppgifterna så att de inte ändras. På

begäran ska det ges ett skriftligt intyg över föreläggandet.

Föreläggandet kan också gälla sådana uppgifter i anslutning till ett meddelande som förmedlats med hjälp av ett informationssystem vilka anger meddelandets ursprung, destination, färdväg, storlek, tidpunkt, varaktighet, art och andra motsvarande omständigheter (trafikuppgifter).

Förundersökningsmyndigheten har inte med stöd av ett föreläggande att säkra data rätt att ta del av innehåller i ett meddelande, i trafikuppgifter eller i andra lagrade uppgifter. Om flera tjänsteleverantörer har deltagit i förmedlingen av ett meddelande, har förundersökningsmyndigheten rätt att ta del av de trafikuppgifter som behövs för att identifiera tjänsteleverantörerna. Ett föreläggande att säkra data utfärdas för viss tid, högst tre månader. Tiden kan förlängas med högst tre månader åt gången, om det är nödvändigt för utredningen av brottet. Den som fått ett föreläggande att säkra data är skyldig att hemlighålla det.

Eftersom villkoret för ett föreläggande om att säkra data är ett antagande om att data kan gå förlorade eller förändras, kan ett sådant föreläggande i praktiken inte gälla de uppgifter som ett tjänsteföretag är skyldigt att lagra med stöd av den reglering som nu föreslås under den tid uppgifterna ska lagras i enlighet med förslaget. Det beror på att det i princip är omöjligt att tänka att det finns risk för att de uppgifter som ska lagras med stöd av lagen går förlorade, om inte situationen är förenad med någon särskild egenskap.

Enligt det föreslagna 3 mom. ska Kommunikationsverket kunna utfärda närmare tekniska föreskrifter om hur lagringsskyldigheten tekniskt ska fullgöras. Bestämmelsen är nödvändig på grund av ärendets tekniska natur och den snabba tekniska utvecklingen, eftersom alla tekniska detaljer inte kan regleras i lagen. Vid beredningen av eventuella föreskrifter gäller det att höra framför allt inrikesministeriet och de lagringsskyldiga tjänsteföretagen.

I fråga om behandlingen av de lagrade uppgifterna tillämpas vad som i den gällande 15 § bestäms om registrering av uppgifter om behandlingen. Ett teleföretag ska således registrera detaljerade transaktionsuppgifter om

behandlingen av de uppgifter som ska lagras enligt 14 a §. Av uppgifterna ska framgå tidpunkten för behandlingen, dess varaktighet och vem som har utfört behandlingen. Uppgifterna ska förvaras två år från lagringen. Registrering av uppgifter om behandlingen är av central betydelse när det gäller att förebygga missbruk i samband med behandlingen av olika slags uppgifter. Med hjälp av de lagrade behandlingsuppgifterna är det möjligt att vid behov senare visa vem som har behandlat de lagrade uppgifterna och för vilket ändamål.

Begreppsmässigt utgör en del av de uppgifter som ska lagras identifieringsuppgifter och en del personuppgifter. Den centrala principen i den föreslagna lagen är att lagen enbart reglerar lagringen av uppgifter. Utnyttjandet av uppgifterna, dvs. myndigheternas rätt att få uppgifter, bestäms i enlighet med andra bestämmelser.

Endast de instanser som enligt lag har rätt att få uppgifter kan ta del av de lagrade uppgifterna. Under 2.1.1 i allmänna motiveringen utreds i detalj med stöd av vilka bestämmelser myndigheterna har rätt att få uppgifter av teleföretagen. När myndigheterna behandlar uppgifterna ska de iaktta de förfaringsätt och principer som enligt gällande bestämmelser ska tillämpas på behandlingen av uppgifter.

Enligt artikel 13 i direktivet om lagring av identifieringsuppgifter ska medlemsstaterna se till att förfaranden i strid med bestämmelserna om lagring av uppgifter beläggs med sanktioner som är effektiva, proportionerliga och avskräckande. Straffbestämmelserna i 42 § i lagen om dataskydd vid elektronisk kommunikation gäller också straffbarhet för behandling av lagstridigt lagrade uppgifter, eftersom definitionen av behandling inbegriper lagring. I fråga om straff tillämpas i övrigt de gällande bestämmelserna i strafflagen.

Den föreslagna paragrafen innebär att artikel 8 i direktivet om lagring av identifieringsuppgifter genomförs nationellt.

14 c §. *Statistikföring av användningen av uppgifter som lagras för myndigheternas behov.* Enligt det föreslagna 1 mom. ska inrikesministeriet varje år lämna Europeiska gemenskapernas kommission statistik över utnyttjande av de uppgifter som lagras med

stöd av lagen. Det handlar om den statistikskyldighet som krävs i direktivet om lagring av identifieringsuppgifter. Det är motiverat att skyldigheten införs för den myndighet vars verksamhet i första hand stöds genom lagringen av uppgifter.

Enligt den föreslagna bestämmelsen ska det av statistiken framgå

1) de fall där uppgifter som teleföretagen lagrat med stöd av lagen har skickats till behöriga myndigheter,

2) de fall där en behörig myndighets begäran om uppgifter som ska lagras inte kunde tillgodoses, samt

3) uppgift om den tid som i respektive fall gått från det att de uppgifter som lagras registrerades tills myndigheten begärde att uppgifterna överförs.

Med ett fall avses i förslaget varje situation där de lagrade uppgifterna begärts av en myndighet på inrikesministeriets förvaltningsområde eller tillställdes myndigheten. Det är motiverat att avgränsa statistikföring och de skyldigheter som gäller utlämnande av statistik enbart till utnyttjande av uppgifter på inrikesministeriets förvaltningsområde. Det beror på att uppgifterna endast används i begränsad utsträckning på andra förvaltningsområden.

I statistiken ska det också specificeras till vem och för vilka ändamål uppgifterna har getts. Dessutom ska det av statistiken naturligtvis på ett tillräckligt noggrant specificerat sätt framgå den mängd uppgifter som tillställts. Kommissionen behöver statistiken för att kunna bedöma den fortsatta användningen av lagrade uppgifter och de fortsatta behoven av att ändra regleringen.

Enligt det föreslagna 2 mom. ska inrikesministeriet särskilt beakta de statistikuppgifter som avses i 1 mom. i de berättelser om televlyssning och teleövervakning som lämnas till riksdagens justitieombudsman med stöd av polislagen, tvångsmedelslagen eller någon annan lag. Riksdagens justitieombudsman får redan för närvarande varje år av inrikesministeriet en berättelse över användningen av så kallade hemliga tvångsmedel. Uppgifterna är förknippade med myndighetsåtgärder som vidtagits i straffprocessuellt syfte, bland annat åtgärder enligt tvångsmedelslagen och polislagen. I berättelserna bor-

de i fortsättningen tas in även uppgifter som motsvarar de statistikuppgifter som avses i 1 mom. och specificeras tillräckligt noggrant hur de lagrade uppgifterna har använts på ett sätt som svarar mot de krav som ställs på den laglighetsövervakning som riksdagens justitieombudsman svarar för. Exempelvis ändamålet med användningen av uppgifterna ska specificeras så att det av statistiken framgår om uppgifterna har skaffats för att förhindra, avslöja eller utreda brott och vilken behörig myndighet har fått uppgifterna. Uppgifter om de som fått uppgifterna ska statistikföras på ett lämpligt sätt. Avsikten är till exempel inte att specificera varje enskilt fall där uppgifter lämnas ut helt normalt i takt med att en enskild brottsprocess framskrider. Vad gäller mängden uppgifter ska statistiken till exempel innehålla information om hur många abonnenter åtgärderna har gällt. Med tanke på laglighetsövervakningen är det också viktigt att veta, för hur lång tid bakåt uppgifter har begärts. Det är självklart att enskilda fysiska personer inte ska kunna identifieras utgående från statistiken och därför får statistiken inte innehålla några personuppgifter.

Förslaget är inte avsett att öka riksdagens justitieombudsmans nuvarande uppgifter. Statistiken och de uppgifter som gäller användningen av uppgifterna kan eventuellt ge riksdagens justitieombudsman större möjligheter än för tillfället att bedöma vilka konsekvenser användningen av uppgifterna har för de grundläggande fri- och rättigheterna samt för de mänskliga rättigheterna. Justitieombudsmannens uppgifter kan till sin karaktär närmast ses som ett komplement till inrikesministeriets och förundersökningsmyndighetens egen laglighetsövervakning.

Erfarenheterna ger vid handen att det är nödvändigt att i fortsättningen också bedöma om bestämmelserna om lagringsskyldighetens omfattning och område utifrån kravet på proportionalitet är relevanta i jämförelse med de resultat som kan uppnås i praktiken. Förslaget innebär att artikel 10 i direktivet om lagring av identifieringsuppgifter genomförs nationellt.

19 §. Skyldighet att handha dataskyddet. Det föreslås att ett nytt 2 mom. som gäller lagring av uppgifter ska fogas till den gällande paragrafen. Enligt det nya momentet gäll-

er att den skyldighet att sörja för dataskyddet för tjänster som föreskrivs i 1 mom. gäller också den i 14 a § avsedda behandlingen av identifieringsuppgifter som behövs för fullgörandet av lagringsskyldigheten. Ett tjänsteföretag ska dessutom bestämma vilka personer som har rätt att behandla de uppgifter som ska lagras och naturligtvis också genom behövliga tekniska förfaranden se till att endast dessa personer har möjlighet att behandla de lagrade uppgifterna.

Tillämpningen av det gällande 1 mom. även i fråga om lagring av uppgifter innebär i praktiken bl.a. att tjänsteföretaget ska se till att de lagrade uppgifterna kvalitativt sett är likadana som de uppgifter som förmedlas i kommunikationsnätet samt se till att enhetligheten hos uppgifterna kvarstår. De lagrade uppgifterna ska dessutom skyddas mot oavsiktlig och obehörig förstörelse och ändring samt mot obehörig lagring och behandling och obehörigt utlämnande. De lagrade uppgifterna ska kvarstå oförändrade, dvs. de ska helt och hållet motsvara de uppgifter som förmedlas i kommunikationsnäten. Skyldigheten är av central betydelse för användbarheten hos de lagrade uppgifterna, eftersom de inte kan användas för utredning av brott om det inte på ett tillräckligt tillförlitligt sätt ses till att uppgifterna kvarstår som enhetliga.

Bestämmelsen om en avgränsning av de personer som behandlar de lagrade uppgifterna innebär att tjänsteföretaget ska se till att bara de personer som behöver uppgifterna för sina arbetsuppgifter får behandla dem. Avsikten är inte att den föreslagna bestämmelsen ska skärpa tjänsteföretagets nuvarande förfaranden så den personkrets som behandlar uppgifterna inskränks i förhållande till nuläget. Om de uppgifter som nu förutsätts bli lagrade har behandlats av vissa personer i t.ex. fakturerings syfte, får dessa personer behandla dem även i fortsättningen. Syftet med bestämmelsen är bl.a. att trygga uppgifternas konfidentiella läge och förebygga missbruk genom att avseende fästs vid att vem som helst inte får behandla de lagrade uppgifterna.

I det gällande 3 mom. föreslås vissa ändringar, enligt vilka ett tjänsteföretag ansvarar även för den lagring av uppgifter som en tredje part genomför. Ändringarna förtydli-

gar den nuvarande ordalydelsen i bestämmelsen.

Förslaget innebär att artikel 7 i direktivet om lagring av identifieringsuppgifter genomförs nationellt.

31 §. Kommunikationsverkets uppgifter. Det föreslås att ett nytt 2 mom. fogas till paragrafen. Enligt det nya momentet ska Kommunikationsverket höras och också i övrigt samarbeta med kommunikationsministeriet vid beredningen av närmare tekniska föreskrifter om lagring av uppgifter. Om en enskild föreskrift av Kommunikationsverket som gäller lagring av uppgifter kan ha betydande verkningar för den allmänna utvecklingen på kommunikationsmarknaden, ska bestämmelser om ärendet utfärdas genom förordning av statsrådet.

De bemyndiganden Kommunikationsverket har enligt gällande lag att meddela föreskrifter är nödvändiga på grund av ärendenas tekniska natur och den snabba tekniska utvecklingen, eftersom alla tekniska detaljer inte kan regleras i lagen. Kommunikationsverkets tekniska föreskrifter bör dock gälla endast närmare eller tekniska detaljer som anknyter till vissa bestämmelser i lagen om dataskydd vid elektronisk kommunikation, och föreskrifterna får inte ha några betydande verkningar för verksamheten på kommunikationsmarknaden. Förslaget är av viktig principiell betydelse för det praktiska bestämmandet av gränserna för bemyndigandet att meddela föreskrifter. Bemyndigandena för Kommunikationsverket har angetts så noggrant avgränsade som möjligt, men i och med den tekniska utvecklingen kan också de tekniska detaljerna få mera vittgående verkningar. Genom förslaget föreskrivs om ett förfarande som säkerställer att målen enligt 80 § 2 mom. i grundlagen uppnås. Eventuella verkningar av de tekniska detaljerna bör utvärderas på lämpligt sätt, och om sådana verkningar uppdrag ska bestämmelser om ärendena utfärdas genom förordning av statsrådet. Det är relevant att utfärda bestämmelser genom förordning av statsrådet alltid när en föreskrift kan ha sådana verkningar som avses i bestämmelsen. Det beror bl.a. på att verkningar av detta slag i typiska fall är verkningar över de sektoriella gränserna, Också av denna orsak är det befogat att genom för-

ordning av statsrådet utfärda bestämmelser om sådant som avses i bestämmelsen.

I praktiken bör samarbetet mellan ministeriet och ämbetsverket ordnas på ett ändamålsenligt sätt och under fria former så att det inte förbrukar parternas personalresurser i onödan. Å andra sidan gäller det samtidigt att säkerställa att alla föreskrifter som påverkar utvecklingen på kommunikationsmarknaden utvärderas av ministeriet. Det gäller i sista hand att i varje enskilt fall avgöra vad som avses med verkningar för utvecklingen på kommunikationsmarknaden eller i vidare bemärkelse för sammanslutningsabonnenternas verksamhet eller den verksamhet som utövas av dem som tillhandahåller mervärdetjänster. Om en föreskrift tydligt i enskilda situationer har sådana verkningar i fråga om kommunikationsmarknaden som avses i bestämmelsen, är det befogat att bestämma om detta genom förordning av statsrådet. En bestämmelse som i princip motsvarar denna finns i 6 § 2 mom. i den gällande radiolagen (1015/2001).

Vid beredningen av föreskrifter om lagring av uppgifter gäller det att också höra framför allt inrikesministeriet och de lagringsskyldiga tjänsteföretagen.

Kommunikationsverket övervakar redan i dagens läge den behandling av identifieringsuppgifter som avses i 3 kap. Därmed bör Kommunikationsverket i fortsättningen också övervaka efterlevnaden av den föreslagna regleringen av lagringen av uppgifter.

35 §. Utlämnande av uppgifter till myndigheter som mottar nödmeddelanden. Det föreslås vissa tekniska ändringar i 35 § 1 och 3-4 mom. i lagen om dataskydd vid elektronisk kommunikation. Polisens alarmeringscentraler lyder sedan ingången av 2006 inte längre under den benämningen, även om själva funktionen har bibehållits. Det finns t.ex. vid polisnrättningen i Helsingfors härad en central för ledning och kommunikation. Även om nödcentralens uppgift är att ta emot nödmeddelanden, riktas nödmeddelanden som gäller försvunna personer fortfarande till polisen. Ett teleföretag är skyldigt att lämna uppgifter till polisen i situationer där polisen är den myndighet som tar emot nödmeddelanden. Syftet med den föreslagna ändringen är inte att ändra det rådande rättsläget. Poli-

sen har enligt polislagen till uppgift att finna försvunna personer. Det föreslås därför att hänvisningen till polisens alarmeringscentral ersätts med en hänvisning till polisen.

36 §. Rätt för vissa andra myndigheter att få uppgifter. I 1 mom. föreslås en informativ bestämmelse som anger med stöd av vilka lagar myndigheterna får utnyttja de uppgifter som ska lagras enligt den föreslagna lagen. Enligt den föreslagna bestämmelsen föreskrivs om myndigheternas rätt att få identifieringsuppgifter och uppgifter som lagras med stöd av 14 a § för att förhindra, avslöja eller utreda brott i polislagen, gränsbevakningslagen, lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005), tullagen och tvångsmedelslagen.

I den föreslagna paragrafen hänvisas till både identifieringsuppgifter och uppgifter, eftersom en del av de uppgifter som ska lagras begreppsmässigt sett är identifieringsuppgifter och en del personuppgifter. Bestämmelsen visar samtidigt den centrala principen för den föreslagna lagen. Enligt den ska lagförslaget endast innehålla bestämmelser om lagring av uppgifter. Utnyttjandet av uppgifterna, dvs. myndigheternas rätt att få uppgifter, bestäms i enlighet med andra bestämmelser.

I det föreslagna 2 mom. konstateras som ett förtydligande att endast de myndigheter som enligt lag har rätt att få uppgifter kan ta del av de lagrade uppgifterna. Under 2.1.1 i allmänna motiveringen utreds i detalj med stöd av vilka bestämmelser myndigheterna har rätt att få uppgifter av teleföretagen. Andra instanser än myndigheter har inte rätt att få uppgifter som lagras för myndigheternas behov.

Genom den föreslagna paragrafen genomförs artikel 4 i direktivet om lagring av identifieringsuppgifter.

Ikraftträdande och övergångsbestämmelser. Enligt den föreslagna bestämmelsen ska tjänsteföretagen senast den 15 mars 2009 börja lagra uppgifter om e-posttjänster och Internettelefonitjänster med stöd av lagen.

Lagring av de uppgifter om Internettjänster som nämns i bestämmelsen förutsätter att tjänsteföretagen genomför betydligt fler ändringar i de tekniska systemen än vad som är fallet i fråga om övriga uppgifter. I fråga om

andra uppgifter än sådana som gäller uppgifter om e-posttjänster och Internettelefontjänster finns det redan i förhållandevis hög grad sådana system och förfaranden som behövs för lagring av uppgifterna och utlämnande till myndigheterna. Däremot måste funktionerna upprättas särskilt för uppgifterna om e-post och Internettelefontjänster. Det är därför motiverat att det anges en övergångsperiod för uppgifterna om e-post och Internettelefontjänster för att de lagringskyldiga på ett överkomligt sätt ska hinna vidta alla åtgärder som behövs för införandet av lagringsskyldigheten. Vid lagring som genomförs efter övergångsperioden ska 14 b § 1 mom. beaktas. Enligt momentet ska ett tjänsteföretag innan lagringsskyldigheten fullgörs komma överens om genomförandet av lagringen med inrikesministeriet i syfte att säkerställa att uppgifterna lagras enligt myndigheternas behov.

Det handlar om en övergångsperiod i enlighet med artikel 15.3 i direktivet om lagring av identifieringsuppgifter. Enligt artikel 15.3 får varje medlemsstat till och med den 15 mars 2009 skjuta upp tillämpningen av direktivet i fråga om lagringen av kommunikationsuppgifter rörande Internetåtkomst, Internettelefontjänster och Internetbaserad e-post.

När skyldigheten att lagra uppgifter träder i kraft innebär den att uppgifterna ska börja lagras efter det att lagen har trätt i kraft. Lagringsskyldigheten gäller därmed enbart kommunikation efter lagens ikraftträdande. En situation där uppgifterna sparas tolv månader uppnås således tidigast när det har gått tolv månader sedan lagen trädde i kraft.

2 Ikraftträdande

Lagen avses träda i kraft så snart som möjligt efter det att den har antagits och blivit stadfast.

3 Förhållande till grundlagen samt lagstiftningsordning

Integritetsskydd

De föreslagna bestämmelserna bör granskas ur perspektivet för de grundläggande fri-

och rättigheterna enligt grundlagen. I 10 § 1 mom. i grundlagen sägs att vars och ens privatliv är tryggt och att närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. Enligt 2 mom. är sekretessen då det gäller kommunikationen en grundläggande fri- och rättighet för varje medborgare. Enligt paragrafen är brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden okränkbara.

Dessa rättsliga intressen som skyddas är dock inte absoluta, eftersom det i vissa situationer är nödvändigt att inskränka dem, bl.a. om individens eller samhällets säkerhet kräver det. I 10 § 3 mom. i grundlagen sägs att genom lag kan bestämmas om sådana begränsningar i meddelandehemligheten som är nödvändiga vid utredning av brott som äventyrar individens eller samhällets säkerhet eller hemfriden, vid rättegång och säkerhetskontroll samt under frihetsberövande. I samband med grundrättsreformen avsågs att förteckningen över dessa möjligheter att begränsa skyddet för konfidentiell kommunikation skulle var uttömmande (RP 309/1993 rd, s. 54).

Inskränkningarna i de grundläggande fri- och rättigheterna bör vara noggrant avgränsade och inte mera omfattande än vad som är nödvändigt för att det önskade målet ska uppnås. Det primära syftet med grundlagens reglering av skyddet för förtroliga meddelanden är enligt förarbetena till grundrättsreformen att mot utomstående skydda innehållet i ett meddelande som är avsett att vara konfidentiellt. Regleringen skyddar dock också sådana andra uppgifter om ett meddelande av detta slag som kan ha betydelse för att meddelandet ska förbli konfidentiellt. I motiveringen har som exempel nämnts identifieringsuppgifter om samtal (RP 309/1993 rd, s. 53).

I 14 a-14 b § i lagförslaget bestäms om lagring av identifieringsuppgifter. Enligt grundlagsutskottet (t.ex. GrUU 9/2004 rd) ingår identifieringsuppgifterna inte i kärnområdet i den grundläggande fri- och rättigheten för hemligheten i fråga om förtroliga meddelanden. Det innebär antagligen att det s.k. kvalificerade lagförbehållet enligt 10 § 3 mom. i grundlagen inte ska tillämpas i fråga om dem. Eventuella begränsningar bör således

granskas med tanke på de allmänna förutsättningarna att inskränka de grundläggande fri- och rättigheterna.

Den föreslagna regleringen innebär en mycket stor principiell förändring i jämförelse med det nuvarande rättsläget. I dagens läge lagrar teleföretagen identifieringsuppgifter endast i den utsträckning de behöver uppgifterna för sin egen affärsverksamhet under de förutsättningar som anges i lag. Utifrån förslaget ska uppgifterna däremot lagras i händelse av att lagtillsynsmyndigheterna behöver dem senare. Lagringen av uppgifter ska dessutom omfatta kommunikation som gäller alla medborgare och företag som är abonnenter eller användare hos de tjänsteföretag som lagrar uppgifterna. Förslaget innebär därmed betydande inskränkningar i det skydd för förtroliga meddelanden som tryggas i grundlagen. Inskränkningarna bör likväl betraktas som godtagbara med tanke på de grundläggande fri- och rättigheterna. Syftet med inskränkningarna är att säkerställa att vissa, för teleföretagen tillgängliga uppgifter i anslutning till elektronisk kommunikation lagras tillräckligt länge för att de ska kunna användas för att förebygga och utreda framför allt allvarliga brott och sörja för att sådana brott blir föremål för åtalsprövning så som föreskrivs särskilt i lag. Inskränkningarna bör därför anses vara påkallade av ett vägande samhällsbehov.

Trots att förslaget innebär en principiellt sett betydande förändring handlar det i praktiken inte om någon speciellt betydande förändring för medborgarna eller teleföretagen, eftersom teleföretagen inte ska lagra några nya uppgifter med stöd av den föreslagna regleringen utan endast sådana uppgifter som de också annars lagrar för sin verksamhet. Det handlar framför allt om att försöka säkerställa att dessa uppgifter som teleföretagen också annars förfogar över lagras i tolv månader.

Vid beredningen av förslaget har man särskilt försökt värna om medborgarnas grundläggande fri- och rättigheter genom att utforma en så noggrant avgränsad och exakt reglering som möjligt för genomförande av direktivet. Vid lagringen av uppgifter ska de principer som tillämpas för att trygga integriteten vid behandling av personuppgifter och

identifieringsuppgifter iakttas, de strikta krav som gäller för dataskyddet uppfyllas samt de personer som får behandla uppgifterna fastställas. Dessutom ska teleföretagen lagra uppgifter om vem som har använt uppgifterna, hur länge och vid vilken tidpunkt.

Det är dessutom viktigt att notera att systemet inte används för att övervaka medborgarna på något sätt som avviker från det nuvarande, eftersom myndigheterna även i fortsättningen ska ha lagbaserad rätt att få de uppgifter som teleföretagen lagrar. Regleringen blir inte heller oskälig för teleföretagen, eftersom den myndighet för vars verksamhet uppgifterna lagras ska betala teleföretagen ersättning för de extra kostnader som regleringen medför.

Regleringen bör bedömas framför allt med tanke på det skydd för personuppgifter som tryggats i 10 § 1 mom. i grundlagen. Regleringen är av betydelse också ur perspektivet för den hemlighet för förtroliga meddelanden som tryggats i 10 § 2 mom. i grundlagen, den yttrandefrihet som tryggats i 12 § 1 mom. liksom det egendomsskydd som tryggats i 15 §.

Enligt 10 § 1 mom. i grundlagen ska närmare bestämmelser om skydd för personuppgifter utfärdas genom lag. Grundlagshänvisningen innebär att det ska lagstiftas om denna rättighet (GrUB 25/1994 rd, s. 6) men att detaljerna i regleringen är beroende av lagstiftarens prövning. En sådan bestämmelse om de grundläggande fri- och rättigheterna binder lagstiftarens prövningsrätt visavi innehållet i mindre grad än en bestämmelse med ett sådant regleringsförbehåll där den grundläggande fri- och rättigheten konstateras föreligga i enlighet med vad som bestäms i lag (t.ex. GrUU 51/2002 rd, s 2).

Enligt grundlagsutskottets praxis (t.ex. GrUU 14/2002 rd, s. 2) begränsas dock lagstiftarens spelrum av att skyddet för personuppgifter utgör en del av skyddet för privatlivet i samma moment. Det är alltså fråga om att lagstiftaren ska trygga denna rättighet på ett sätt som kan anses godtagbart med hänsyn till de grundläggande fri- och rättigheterna.

Lagstiftaren är i sin prövning bunden av att det vid en registrering är viktigt att reglera åtminstone syfte, innehållet i de registrerade personuppgifterna, tillåtna användningsän-

damål, inbegripet uppgifternas tillförlitlighet och bevaringstiden för uppgifterna i personregistren samt den registrerades rättsskydd. Regleringen av dessa faktorer på lagnivå ska dessutom vara omfattande och detaljerad (t.ex. GrUU 51/2002 rd, s. 2).

Skydd för personuppgifter behandlas också i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Artikel 8 i den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna (människorättskonventionen) innehåller likaså bestämmelser om vars och ens rätt att åtnjuta respekt för sitt privatliv och sin korrespondens.

De föreslagna ålägganden som gäller lagringsskyldighet har entydigt begränsats till tjänsteföretag som är skyldiga att göra televerksamhetsanmälan. Därmed har andra tjänsteleverantörer än teleföretag – t.ex. privatpersoner och frivilligorganisationer liksom sammanslutningsabbonnenter – genom tillräckligt noggranna bestämmelser ställts utanför lagringsskyldigheten, så som grundlagsutskottet redan tidigare har förutsatt (GrUU 35/2004, s. 5).

Lagringstiden ska inte vara längre än vad som behövs för att målen med regleringen ska uppnås. Grundlagsutskottet har ansett att lagringen av identifieringsuppgifter alltid är förknippad med risker såväl i fråga om skyddet för konfidentiell kommunikation som i fråga om skyddet personuppgifter. Riskerna ökar ju längre uppgifterna lagras. Långa lagringstider kan bli problematiska också med tanke på egendomsskyddet i grundlagen (GrUU 35/2004 rd, s. 4). Den föreslagna lagringstiden hör nära samman med bestämmelserna om myndigheternas rätt att få uppgifter. Om behandlingen av förslaget resulterar i att lagringstiderna blir avsevärt kortare än vad som föreslås, innebär det att regleringen inte är till den nytta för myndigheternas verksamhet som direktivet eftersträvar. Om behandlingen av förslaget å andra sidan resulterar i att lagringstiderna blir avsevärt längre, kan det anses vara befogat att ompröva det angreppssätt som nu valts och som innebär att myndigheternas rätt att få uppgifter inte alls ändras.

Termen 'behandling' som används i förslaget fyller de allmänna kraven på exakthet och

noggrann avgränsning som fordras för att inskränka de grundläggande fri- och rättigheterna, eftersom man i detta fall tillämpar de allmänna bestämmelserna och principerna i 8 § i lagen om dataskydd vid elektronisk kommunikation.

Lagförslaget innebär inte heller några problem i förhållande till människorättskonventionen eller Europarådets dataskyddskonvention. Enligt artikel 8 i människorättskonventionen och enligt tolkningspraxisen vid Europeiska domstolen för mänskliga rättigheter ska kraven på nödvändighet och proportionalitet uppfyllas när myndigheter ingriper i privata rättigheter. Ingreppen bör därmed tjäna detaljerade, exakta och lagliga syften och genomföras på ett sätt som är tillräckligt, lämpligt och proportionerligt med hänsyn till målet med ingripandet.

De föreslagna behandlingsrättigheterna har avgränsats så entydigt och noggrant som möjligt. Med tanke på en minimiförpliktelse har grundlagsutskottet tidigare ansett det vara viktigt vilka uppgifter eller uppgiftstyper förpliktelsen omfattar. Detta slag av viktiga frågor och avgränsningar visavi regleringen bör framgå tydligt (GrUU 35/2004 rd, s. 3). Det är dock viktigt att notera att det handlar om uppgifter som också annars sparas i samband med det tekniska genomförandet av kommunikationerna när tjänsterna utförs eller används. Det ska således inte lagras några nya uppgifter med stöd av den föreslagna regleringen. Den föreslagna regleringen innebär dessutom att uppgifterna ska lagras bara under en bestämd tid. Det föreslås däremot inte några ändringar i myndigheternas rätt att få uppgifter, och därmed kommer myndigheterna att få information av teleföretagen under samma förutsättningar som tidigare. I den meningen är förslaget inte problematiskt med tanke på de grundläggande fri- och rättigheterna. Med tanke på kravet på proportionalitet är det viktigt att tjänsteleverantören inte särskilt förpliktas att generera eller skaffa uppgifter. De ska bara lagras de uppgifter som också annars är tillgängliga för leverantören (GrUU 34/2004 rd, s. 3). Regleringen behövs för att trygga säkerheten i samhället, och de begränsningar som den orsakar i integritetsskyddet eller i skyddet av förtroliga meddelanden står i ett rimligt förhållande till målet

med regleringen. Regleringen ingriper inte heller i innehållet i förtroliga meddelanden.

Egendomsskydd

Bestämmelser om egendomsskydd finns i 15 § i grundlagen, där det sägs att vars och ens egendom är tryggad. Angående expropriation av egendom för allmänt behov mot full ersättning bestäms i lag. Av betydelse för egendomsskyddet är framför allt att det föreslås att teleföretagen ska lagra uppgifter för myndigheternas behov, och i detta syfte är teleföretagen tvungna att bl.a. skaffa mer lagringskapacitet samt eventuellt göra även andra ändringar i sina system och tjänster. För att egendomsskyddet ska tillgodoses är det viktigt att teleföretagen i enlighet med förslaget får ersättning för de extra kostnader som orsakas uttryckligen av myndigheternas behov.

Normgivning på lägre nivå

I 80 § 1 mom. i grundlagen sägs att genom lag ska utfärdas bestämmelser om grunderna för individens rättigheter och skyldigheter. Enligt 80 § 2 mom. kan andra myndigheter genom lag bemyndigas att utfärda rättsnormer i bestämda frågor, om det med hänsyn till föremålet för regleringen finns särskilda skäl och regleringens betydelse i sak inte kräver att den sker genom lag eller förordning. Tillämpningsområdet för ett sådant bemyndigande ska vara exakt avgränsat. Av grundlagen följer dessutom att de frågor som ett bemyndigande omfattar ska fastställas noggrant i lag.

Grundlagsutskottet har upprepade gånger betonat att tolkningen av bestämmelserna om bemyndigande liksom också innehållet i bestämmelser som utfärdas med stöd av dem inskränks direkt av 80 § 1 och 2 mom. i grundlagen (se t.ex. GrUU 48/2001 rd, s. 4). Det går därmed inte att genom förordning eller myndighetsföreskrifter utfärda allmänna rättsregler om exempelvis grunderna för individens rättigheter och skyldigheter eller frågor som enligt grundlagen i övrigt hör till området för lag (GrUU 16/2002 rd, s 2).

De bemyndiganden att meddela föreskrifter som föreslås för Kommunikationsverket är

nödvändiga av särskilda skäl som hänför sig till föremålet för regleringen. Föremålen för regleringen är speciellt tekniska, och den snabba tekniska utvecklingen förändrar oavbrutet föremålet för regleringen. Av samma orsak är det också en mycket krävande uppgift att bedöma konsekvenserna av föreskrifterna. Exempelvis den tekniska utvecklingen kan innebära att Kommunikationsverkets föreskrifter får mera vittgående konsekvenser eller konsekvenser över de sektoriella gränserna. Avsikten är att de föreslagna förordningar av statsrådet som eventuellt utfärdas på basis av en bedömning av konsekvenserna av föreskrifterna enligt 31 § i förekommande fall ska innehålla preciserande och avgränsande bestämmelser om innehållet i de föreskrifter som Kommunikationsverket utfärdar med stöd av de som sådana i lagen exakt och noggrant avgränsade skyldigheterna och rättigheterna samt med stöd av i lagen exakta föreskrivna bemyndiganden att meddela föreskrifter. Den exceptionellt svåra bedömningen av konsekvenserna av regleringen är ett sådant särskilt skäl relaterat till föremålet för regleringen som gör det nödvändigt att utfärda bestämmelser genom förordning. Det är omöjligt att genom lag utfärda bestämmelser om alla detaljer i enlighet med kraven i den tekniska miljön som förändras i snabb takt.

Bemyndigandet att utfärda rättsnormer har definierats så noggrant och exakt som möjligt på så vis att det gäller endast omständigheter som formellt omfattas av Kommunikationsverkets rätt att meddela föreskrifter men som likväl vid den tidpunkt då föreskrifterna meddelas eller i ljuset av den tekniska utvecklingen längre fram kan ha mera vittgående konsekvenser när situationen har förändrats. I vilket fall som helst har de bemyndiganden att meddela föreskrifter som föreslås för Kommunikationsverket och de föreslagna bestämmelserna om bemyndigande att utfärda förordning begränsats till att gälla endast detaljer av teknisk natur medan alla grunder för rättsställningen bestäms utifrån bestämmelser i lagen. De föreslagna bemyndigandena att utfärda rättsnormer står därför inte i strid med 80 § i grundlagen.

Den föreslagna ändringen av 31 § handlar inte om en sänkning av författningsnivån

utan om en upphöjning till en högre nivå i normhierarkin. Regleringen harmonierar därmed med grundlagens syften. De förslag som gäller föreskrifter av Kommunikationsverket är inte problematiska ur perspektivet för grundlagens bestämmelser om överföring av lagstiftningsbehörigheten.

En bestämmelse som i princip motsvarar den föreslagna 31 § finns i 6 § 2 mom. i den gällande radiolagen.

Bedömning av lagstiftningsordningen

I denna proposition har målet varit att med hänsyn till särdragen inom elektronisk kommunikation sammanjämka å ena sidan abonnenternas och användarnas integritetsskydd och teleföretagens egendomsskydd och å andra sidan myndigheternas behov. Avsikten

har varit att utforma så noggrant avgränsade och exakta bestämmelser som möjligt. Det kan inte heller anses att begränsningarna överskrider det som är nödvändigt för att uppnå begränsningarnas godtagbara syfte, vilket innebär att de också står i överensstämmelse med proportionalitetsprincipen. Förslaget är inte problematiskt i konstitutionellt hänseende och uppfyller till alla delar de allmänna grunderna för inskränkning av de grundläggande fri- och rättigheterna.

Med stöd av vad som anförts ovan kan lagförslaget behandlas i vanlig lagstiftningsordning. Regeringen anser det dock vara önskvärt att grundlagsutskottets utlåtande om propositionen begärs.

Med stöd av vad som anförts ovan föreläggs Riksdagen följande lagförslag:

Lagförslag

1.

Lag**om ändring av lagen om dataskydd vid elektronisk kommunikation**

I enlighet med riksdagens beslut

ändras i lagen av den 16 juni 2004 om dataskydd vid elektronisk kommunikation (516/2004) 8 § 3 mom., 19 § 2 och 3 mom., 35 § 1, 3 och 4 mom. samt 36 § 1 mom., av dem 36 § 1 mom. sådant det lyder i lag 599/2005, samt

fogas till 2 §, sådan den lyder delvis ändrad i lag 198/2006, nya 14 a och 14 b punkter, nya 14 a–14 c §, till 19 § ett nytt 2 mom., varvid det ändrade 2 och 3 mom. blir 3 och 4 mom., till 31 § ett nytt 2 mom. samt till 36 §, sådan den lyder delvis ändrad i nämnda lag 599/2005, ett nytt 2 mom., varvid det nuvarande 2 och 3 mom. blir 3 och 4 mom., som följer:

2 §

Definitioner

I denna lag avses med

14 a) *tjänsteföretag* företag enligt 2 § 19 punkten i kommunikationsmarknadslagen,

14 b) *Internettelefonitjänst* en tjänst som ett teleföretag tillhandahåller och som ända till slutkunderna baserar sig på Internetprotokoll och möjliggör samtal,

8 §

Allmänna bestämmelser om behandlingen

Behandling enligt detta kapitel är tillåten endast i den omfattning som behandlingsändamål kräver och behandlingen får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt. Identifieringsuppgifter får endast utlämnas till den som har rätt att behandla uppgifterna i förekommande fall. Efter behandlingen skall meddelandena och identifieringsuppgifterna förstöras eller göras sådana

att de inte kan förknippas med abonnenten eller användaren, om inte något annat bestäms i lag.

14 a §

Skyldighet att lagra uppgifter för myndigheternas behov

Utan hinder av vad som i detta kapitel bestäms om behandling av identifieringsuppgifter, ska ett tjänsteföretag som är skyldigt att göra televerksamhetsanmälan, på de villkor som anges nedan, se till att de uppgifter som nämns i artikel 5 i 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 lagras i tolv månader från det datum kommunikationen ägde rum.

Lagringsskyldigheten gäller uppgifter i anslutning till

1) sådana telefonitjänster eller tilläggstjänster i fasta nät eller sådana telefonitjänster, tilläggstjänster, textmeddelandetjänster, EMS-tjänster eller multimedietjänster i mobiltelenät som tillhandahålls av ett tjänsteföretag,

2) Internetåtkomsttjänster som tillhandahålls av ett tjänsteföretag,

3) elektroniska posttjänster som tillhandahålls av ett tjänsteföretag,

4) Internettelefontjänster som tillhandahålls av ett tjänsteföretag,

5) samtal som har kopplats men som inte besvarats eller samtal som har förhindrats till följd av en driftsåtgärd i nätet.

Lagringsskyldigheten gäller inte innehållet i meddelandena eller identifieringsuppgifter som samlats vid bläddring av webbsidor.

För lagringsskyldighet krävs att uppgifterna är tillgängliga och har genererats eller behandlats i samband med tillhandahållande av tjänsteföretagets allmänt tillgängliga kommunikationstjänster med stöd av detta kapitel eller personuppgiftslagen.

En närmare definition och tekniska detaljer i fråga om de uppgifter som ska lagras ingår i en teknisk föreskrift som utfärdas av Kommunikationsverket.

14 b §

Skyldigheter och förfaringssätt vid behandling av uppgifter som lagras för myndigheternas behov

Ett tjänsteföretag som är skyldigt att lagra uppgifter ska innan lagringsskyldigheten fullgörs komma överens om genomförandet av lagringen med inrikesministeriet i syfte att säkerställa att uppgifterna lagras enligt myndigheternas behov. Det bör undvikas att flera tjänsteföretag lagrar samma uppgifter. De uppgifter som lagras ska utan onödigt dröjsmål kunna lämnas till de myndigheter som har rätt att få uppgifterna. Ett tjänsteföretag som är skyldigt att lagra uppgifter ska vid behov sörja för fullgörandet av skyldigheten i samråd med ett nätföretag, så att även de tillgängliga uppgifter enligt 14 a § som nätföretaget behandlar för tillhandahållande av tjänsteföretagets tjänster lagras. Ett tjänsteföretag som är skyldigt att lagra uppgifter ska se till att abonnenten har tillgång till information om att uppgifter lagras och om syftet med lagringen.

På ersättning för de kostnader som orsakas av lagringsskyldigheten och av motsvarande beredskap tillämpas 98 § i kommunikationsmarknadslagen. I 4 kap. 4 b och 4 c § i tvångsmedelslagen (450/1987) föreskrivs om föreläggande att säkra data för utredningen av ett brott som undersöks.

Kommunikationsverket kan utfärda närmare föreskrifter om hur lagringsskyldigheten tekniskt ska fullgöras.

14 c §

Statistikföring av användningen av uppgifter som lagras för myndigheternas behov

Inrikesministeriet ska varje år lämna Europeiska gemenskapernas kommission statistik över utnyttjande av de uppgifter som lagras med stöd av denna lag. Av statistiken ska framgå

1) de fall där uppgifter som lagrats har skickats till myndigheter,

2) de fall där en myndighets begäran om uppgifter som lagrats inte kunde tillgodoses,

3) uppgift om den tid som gått från det att uppgifterna lagrades till det att myndigheten begärde att uppgifterna överförs.

Inrikesministeriet ska särskilt beakta de statistikuppgifter som avses i 1 mom. i de berättelser som ministeriet med stöd av polislagen, tvångsmedelslagen eller någon annan lag avger om teleövervakning och teleavlyssning.

19 §

Skyldighet att handha dataskyddet

Den skyldighet att handha dataskyddet för tjänster som föreskrivs i 1 mom. gäller också i 14 a § avsedd behandling av uppgifter som behövs för fullgörandet av lagringsskyldigheten. Ett tjänsteföretag ska dessutom utse de personer som har rätt att behandla uppgifter som lagras.

Ett teleföretag och den som tillhandahåller mervärdestjänster är gentemot abonnenterna och användarna ansvariga för det dataskydd som avses i 1 och 2 mom. också i fråga om sådan tredje part som helt eller delvis utför nättjänsten, kommunikationstjänsten, lagringen av uppgifter eller mervärdestjänsten. Ansvaret gäller en sammanslutningsabonnent i fråga om den behandling av användarnas identifierings- och lokaliseringssuppgifter som utförs av tredje part.

Kommunikationsverket kan ge ett teleföretag närmare föreskrifter om ovan i 1–3 mom. avsett dataskydd för tjänster eller lagring av uppgifter.

31 §

Kommunikationsverkets uppgifter

När Kommunikationsverket bereder närmare tekniska föreskrifter om lagring av uppgifter ska verket höra och samarbeta med kommunikationsministeriet. Om Kommunikationsverkets föreskrifter om lagring av uppgifter kan ha betydande konsekvenser för den allmänna utvecklingen på kommunikationsmarknaden, ska bestämmelser om ärendet utfärdas genom förordning av statsrådet.

35 §

Utlämnande av uppgifter till myndigheter som mottar nödmeddelanden

Ett teleföretag är skyldigt att till en nödcentral, sjöräddningscentral, sjöräddningsundercentral och polisen för behandling lämna ut

1) identifierings- och lokaliseringssuppgifter om den anslutning och den terminalutrustning från vilken nödmeddelandet har sänts, samt uppgifter om anslutningens abonnent, användare och installeringsadress, samt

2) identifierings- och lokaliseringssuppgifter som anger läget för den terminalutrustning och anslutning som innehas av den användare

re som är föremål för nödmeddelandet, om den myndighet som mottagit nödmeddelandet har grundad anledning att anta att användaren befinner sig i uppenbar nöd eller i omedelbar fara.

Den som tillhandahåller mervärdestjänster har rätt att lämna ut de uppgifter som avses i 1 mom. till en nödcentral, sjöräddningscentral, sjöräddningsundercentral och polisen.

Teleföretagen ska utan dröjsmål till en nödcentral, sjöräddningscentral, sjöräddningsundercentral och polisen anmäla sådana fel och störningar i kommunikationsnätet, nättjänsterna och kommunikationstjänsterna som är av betydelse för förmedlingen av nödsamtal.

36 §

Rätt för vissa andra myndigheter att få uppgifter

I fråga om myndigheternas rätt att få identifieringsuppgifter för att förhindra, avslöja eller utreda brott bestäms i polislagen (493/1995), gränsbevakningslagen (578/2005), lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005), tullagen (1466/1994) och tvångsmedelslagen.

Endast de myndigheter som med stöd av lag har rätt att få uppgifter av ett tjänsteföretag kan av tjänsteföretagen få sådana uppgifter som ska lagras med stöd av 14 a §.

Denna lag träder i kraft den 200 .

Åtgärder som verkställigheten av lagen förutsätter får vidtas innan lagen träder i kraft.

Tjänsteföretagen ska senast från den 15 mars 2009 lagra uppgifter om elektroniska posttjänster och Internettelefonitjänster med stöd av denna lag.

Helsingfors den 23 november 2007

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

*Bilaga
Parallelltext*

1.

Lag

om ändring av lagen om dataskydd vid elektronisk kommunikation

I enlighet med riksdagens beslut

ändras i lagen av den 16 juni 2004 om dataskydd vid elektronisk kommunikation (516/2004) 8 § 3 mom., 19 § 2 och 3 mom., 35 § 1, 3 och 4 mom. samt 36 § 1 mom., av dem 36 § 1 mom. sådant det lyder i lag 599/2005, samt

fogas till 2 §, sådan den lyder delvis ändrad i lag 198/2006, nya 14 a och 14 b punkter, nya 14 a–14 c §, till 19 § ett nytt 2 mom., varvid det ändrade 2 och 3 mom. blir 3 och 4 mom., till 31 § ett nytt 2 mom. samt till 36 §, sådan den lyder delvis ändrad i nämnda lag 599/2005, ett nytt 2 mom., varvid det nuvarande 2 och 3 mom. blir 3 och 4 mom., som följer:

Gällande lydelse

Föreslagen lydelse

2 §

2 §

Definitioner

Definitioner

I denna lag avses med

I denna lag avses med

14 a) **tjänsteföretag** företag enligt 2 § 19 punkten i kommunikationsmarknadslagen,

14 b) **Internettelefontjänst** en tjänst som ett teleföretag tillhandahåller och som ända till slutkunderna baserar sig på Internetprotokoll och möjliggör samtal,

8 §

8 §

Allmänna bestämmelser om behandlingen

Allmänna bestämmelser om behandlingen

Behandling enligt 9–14 § är tillåten endast i den omfattning som behandlingens ändamål kräver och behandlingen får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt. Identifieringsuppgifter får endast utlämnas till den som har rätt att behandla uppgifterna i förekommande fall. Efter behandlingen skall meddelandena och identifieringsuppgifterna

Behandling enligt *detta kapitel* är tillåten endast i den omfattning som behandlingens ändamål kräver och behandlingen får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt. Identifieringsuppgifter får endast utlämnas till den som har rätt att behandla uppgifterna i förekommande fall. Efter behandlingen skall meddelandena och identifie-

förstöras eller göras sådana att de inte kan förknippas med abonnenten eller användaren, om inte annat bestäms i lag.

ringsuppgifterna förstöras eller göras sådana att de inte kan förknippas med abonnenten eller användaren, om inte något annat bestäms i lag.

14 a §

Skyldighet att lagra uppgifter för myndigheternas behov

Utan hinder av vad som i detta kapitel bestäms om behandling av identifieringsuppgifter, ska ett tjänsteföretag som är skyldigt att göra televerksamhetsanmälan, på de villkor som anges nedan, se till att de uppgifter som nämns i artikel 5 i 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 lagras i tolv månader från det datum kommunikationen ägde rum.

Lagringskyldigheten gäller uppgifter i anslutning till

1) sådana telefonitjänster eller tilläggs-tjänster i fasta nät eller sådana telefonitjänster, tilläggstjänster, textmeddelandetjänster, EMS-tjänster eller multimedietjänster i mobiltelenät som tillhandahålls av ett tjänsteföretag,

2) Internetåtkomsttjänster som tillhandahålls av ett tjänsteföretag,

3) elektroniska posttjänster som tillhandahålls av ett tjänsteföretag,

4) Internettelefonitjänster som tillhandahålls av ett tjänsteföretag,

5) samtal som har kopplats men som inte besvarats eller samtal som har förhindrats till följd av en driftsåtgärd i nätet.

Lagringskyldigheten gäller inte innehållet i meddelandena eller identifieringsuppgifter som samlats vid bläddring av webbsidor.

För lagringskyldighet krävs att uppgifterna är tillgängliga och har genererats eller behandlats i samband med tillhandahållande av tjänsteföretagets allmänt tillgängliga kommunikationstjänster med stöd av detta kapitel eller personuppgiftslagen.

En närmare definition och tekniska detaljer i

fråga om de uppgifter som ska lagras ingår i en teknisk föreskrift som utfärdas av Kommunikationsverket.

14 b §

Skyldigheter och förfaringssätt vid behandling av uppgifter som lagras för myndigheternas behov

Ett tjänsteföretag som är skyldigt att lagra uppgifter ska innan lagringskyldigheten fullgörs komma överens om genomförandet av lagringen med inrikesministeriet i syfte att säkerställa att uppgifterna lagras enligt myndigheternas behov. Det bör undvikas att flera tjänsteföretag lagrar samma uppgifter. De uppgifter som lagras ska utan onödigt dröjsmål kunna lämnas till de myndigheter som har rätt att få uppgifterna. Ett tjänsteföretag som är skyldigt att lagra uppgifter ska vid behov sörja för fullgörandet av skyldigheten i samråd med ett nätföretag, så att även de tillgängliga uppgifter enligt 14 a § som nätföretaget behandlar för tillhandahållande av tjänsteföretagets tjänster lagras. Ett tjänsteföretag som är skyldigt att lagra uppgifter ska se till att abonnenten har tillgång till information om att uppgifter lagras och om syftet med lagringen.

På ersättning för de kostnader som orsakas av lagringskyldigheten och av motsvarande beredskap tillämpas 98 § i kommunikationsmarknadslagen. I 4 kap. 4 b och 4 c § i tvångsmedelslagen (450/1987) föreskrivs om föreläggande att säkra data för utredningen av ett brott som undersöks.

Kommunikationsverket kan utfärda närmare föreskrifter om hur lagringskyldigheten tekniskt ska fullgöras.

14 c §

Statistikföring av användningen av uppgifter som lagras för myndigheternas behov

Inrikesministeriet ska varje år lämna Europeiska gemenskapernas kommission statistik över utnyttjande av de uppgifter som lag-

ras med stöd av denna lag. Av statistiken ska framgå

1) de fall där uppgifter som lagrats har skickats till myndigheter,

2) de fall där en myndighets begäran om uppgifter som lagrats inte kunde tillgodoses,

3) uppgift om den tid som gått från det att uppgifterna lagrades till det att myndigheten begärde att uppgifterna överförs.

Inrikesministeriet ska särskilt beakta de statistikuppgifter som avses i 1 mom. i de berättelser som ministeriet med stöd av polislagen, tvångsmedelslagen eller någon annan lag avger om teleövervakning och teleavlyssning.

19 §

Skyldighet att handha dataskyddet

Ett teleföretag och den som tillhandahåller mervärdestjänster är gentemot abonnenterna och användarna ansvarig för det dataskydd som avses i 1 mom. också i fråga om sådan tredje part som helt eller delvis utför nät-, kommunikations- eller mervärdestjänsten. Det som avses ovan i detta moment gäller en sammanslutningsabonnent i fråga om behandlingen av användarnas identifierings- och lokaliseringssuppgifter.

Kommunikationsverket kan ge ett teleföretag närmare föreskrifter om dataskydd för i 1 och 2 mom. avsedda tjänster.

31 §

Kommunikationsverkets uppgifter

19 §

Skyldighet att handha dataskyddet

Den skyldighet att handha dataskyddet för tjänster som föreskrivs i 1 mom. gäller också i 14 a § avsedd behandling av uppgifter som behövs för fullgörandet av lagringsskyldigheten. Ett tjänsteföretag ska dessutom utse de personer som har rätt att behandla uppgifter som lagras.

Ett teleföretag och den som tillhandahåller mervärdestjänster är gentemot abonnenterna och användarna ansvarig för det dataskydd som avses i 1 och 2 mom. också i fråga om sådan tredje part som helt eller delvis utför nättjänsten, kommunikationstjänsten, lagringen av uppgifter eller mervärdestjänsten. Ansvaret gäller en sammanslutningsabonnent i fråga om den behandling av användarnas identifierings- och lokaliseringssuppgifter som utförs av tredje part.

Kommunikationsverket kan ge ett teleföretag närmare föreskrifter om ovan i 1–3 mom. avsett dataskydd för tjänster eller lagring av uppgifter.

31 §

Kommunikationsverkets uppgifter

När Kommunikationsverket bereder närmare tekniska föreskrifter om lagring av uppgifter ska verket höra och samarbeta med

kommunikationsministeriet. Om Kommunikationsverkets föreskrifter om lagring av uppgifter kan ha betydande konsekvenser för den allmänna utvecklingen på kommunikationsmarknaden, ska bestämmelser om ärendet utfärdas genom förordning av statsrådet.

35 §

Utlämnande av uppgifter till myndigheter som mottar nödmeddelanden

Ett teleföretag är skyldigt att till en nödcentral, sjöräddningscentral, sjöräddningsundercentral och polisens alarmeringscentral för behandling lämna ut

1) identifierings- och lokaliseringssuppgifter om den anslutning och den terminalutrustning från vilken nödmeddelandet har sänts, samt uppgifter om anslutningens abonnent, användare och installeringsadress, samt

2) identifierings- och lokaliseringssuppgifter som anger läget för den terminalutrustning och anslutning som innehas av den användare som är föremål för nödmeddelandet, om den myndighet som mottagit nödmeddelandet har grundad anledning att anta att användaren befinner sig i uppenbar nöd eller i omedelbar fara.

De i 1 mom. avsedda uppgifterna skall lämnas ut utan hinder av i 5 § avsedd tystnadsplikt och utan hinder av de förutsättningar som gäller behandling av i 4 kap. avsedda lokaliseringssuppgifter samt oberoende av vad abonnenten eller användaren har överenskommit med teleföretaget om hemlighållande av uppgifter.

Den som tillhandahåller mervärdestjänster har rätt att lämna ut i 1 mom. avsedda uppgifter till en nödcentral, sjöräddningscentral, sjöräddningsundercentral och polisens alarmeringscentral.

Teleföretagen skall utan dröjsmål till en nödcentral, sjöräddningscentral, sjöräddningsundercentral och polisens alarmeringscentral anmäla om sådana fel i och störningar av kommunikationsnätet, nättjänsterna och kommunikationstjänsterna som är av betydelse för förmedlingen av nödsamtal.

35 §

Utlämnande av uppgifter till myndigheter som mottar nödmeddelanden

Ett teleföretag är skyldigt att till en nödcentral, sjöräddningscentral, sjöräddningsundercentral och *polisen* för behandling lämna ut

1) identifierings- och lokaliseringssuppgifter om den anslutning och den terminalutrustning från vilken nödmeddelandet har sänts, samt uppgifter om anslutningens abonnent, användare och installeringsadress, samt

2) identifierings- och lokaliseringssuppgifter som anger läget för den terminalutrustning och anslutning som innehas av den användare som är föremål för nödmeddelandet, om den myndighet som mottagit nödmeddelandet har grundad anledning att anta att användaren befinner sig i uppenbar nöd eller i omedelbar fara.

Den som tillhandahåller mervärdestjänster har rätt att lämna ut de uppgifter som avses i 1 mom. till en nödcentral, sjöräddningscentral, sjöräddningsundercentral och *polisen*.

Teleföretagen ska utan dröjsmål till en nödcentral, sjöräddningscentral, sjöräddningsundercentral och *polisen* anmäla sådana fel och störningar i kommunikationsnätet, nättjänsterna och kommunikationstjänsterna som är av betydelse för förmedlingen av nödsamtal.

36 §

Rätt för vissa andra myndigheter att få uppgifter

I fråga om myndigheternas rätt att få identifieringsuppgifter för att förhindra och avslöja brott bestäms i polislagen (493/1995), i gränsbevakningslagen (578/2005) och i tullagen (1466/1994). Angående myndigheternas rätt att få identifieringsuppgifter för att utreda brott bestäms i tvångsmedelslagen (450/1987).

36 §

Rätt för vissa andra myndigheter att få uppgifter

I fråga om myndigheternas rätt att få identifieringsuppgifter för att förhindra, avslöja eller utreda brott bestäms i polislagen (493/1995), gränsbevakningslagen (578/2005), lagen om behandling av personuppgifter vid gränsbevakningsväsendet (579/2005), tullagen (1466/1994) och tvångsmedelslagen.

Endast de myndigheter som med stöd av lag har rätt att få uppgifter av ett tjänsteföretag kan av tjänsteföretagen få sådana uppgifter som ska lagras med stöd av 14 a §.

*Denna lag träder i kraft den 200 .
Åtgärder som verkställigheten av lagen förutsätter får vidtas innan lagen träder i kraft.*

Tjänsteföretagen ska senast från den 15 mars 2009 lagra uppgifter om elektroniska posttjänster och Internettelefontjänster med stöd av denna lag.
