Regeringens proposition till Riksdagen med förslag till lag om ändring av lagen om dataskydd vid elektronisk kommunikation och vissa lagar som har samband med den

PROPOSITIONENS HUVUDSAKLIGA INNEHÅLL

I denna proposition föreslås att lagen om dataskydd vid elektronisk kommunikation skall ändras. Dessutom föreslås vissa ändringar av närmast teknisk natur i lagen om integritetsskydd i arbetslivet, lagen om samarbete inom företag och lagen om samarbete inom statens ämbetsverk och inrättningar.

Sammanslutningsabonnenternas rätt att behandla identifieringsuppgifter för teknisk utveckling och för att reda ut olovligt brukande av avgiftsbelagda informationssamhällstjänster eller kommunikationsnät och brukande som strider mot anvisningarna för kommunikationstjänster förtydligas. Förslaget innebär att teleföretagen, de som tillhandahåller mervärdestjänster och sammanslutningsabonnenterna på vissa villkor ges rätt att med hjälp av automatisk databehandling behandla identifieringsuppgifter för statistisk analys.

Genom förslaget ges sammanslutningsabonnenterna rätt att på vissa villkor behandla identifieringsuppgifter, om det finns misstanke om olovligt röjande av företagshemligheter som är av central betydelse för näringsverksamheten. Sammanslutningsabonnenterna avses få behandla uppgifter om bland annat avsändaren och mottagaren av elektronisk post samt tidpunkten för kommunikationen, men inte innehållet i meddelandet.

Genom förslaget förbättras möjligheterna för teleföretag, tillhandahållare av mervärdestjänster och sammanslutningsabonnenter att ha hand om datasäkerheten för kommunikationsnät och -tjänster.

Det föreslås att dataombudsmannen skall övervaka bestämmelserna om sammanslutningsabonnenternas behandling av identifieringsuppgifter i missbrukssituationer. Dessutom föreslås Kommunikationsverket få mera omfattande rättigheter att lämna ut uppgifter i syfte att förebygga och utreda kränkningar av dataskyddet.

Lagarna avses träda i kraft den 1 januari 2009.

INNEHÅLLSFÖRTECKNING

ALLMÄN MOTIVERING

1 Nuläge

1.1 Lagstiftning och praxis

I lagen om dataskydd vid elektronisk kommunikation (516/2004) bestäms om skyldigheter för förmedlare av elektroniska meddelanden i syfte att genom en vanlig lag garantera konfidentialitet vid kommunikation och integritetsskydd för dem som använder kommunikationsnät. På konstitutionell nivå bestäms om skydd för privatlivet, dvs. integritetsskydd, i 10 § i grundlagen. Integritetsskyddet omfattar också konfidentialitet vid kommunikation, vilket innebär att skyddet förutom innehållet i meddelanden också gäller identifieringsuppgifter utifrån vilka fysiska personer kan identifieras. Genom lagen om dataskydd vid elektronisk kommunikation utsträcktes den reglering som garanterar konfidentialitet vid kommunikation till att gälla inte bara teleföretag utan också sammanslutningsabonnenter. Sammanslutningsabonnenter är företag eller sammanslutningar som är abonnenter på kommunikations- eller mervärdestjänster och som i sitt kommunikationsnät behandlar konfidentiella meddelanden från användare, identifieringsuppgifter eller lokaliseringsuppgifter om dem.

Enligt 4 § 1 mom. i lagen om dataskydd vid elektronisk kommunikation är meddelanden, identifieringsuppgifter och lokaliseringsuppgifter 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 definitionen i 2 § avses med identifieringsuppgifter uppgifter som kan förknippas med en abonnent eller användare och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden. Identifieringsuppgifterna kan inrymma uppgifter som hänvisar till bl.a. dirigering av kommunikationen, dess varaktighet och tidpunkt eller mängden information som överförs, det protokoll som använts, den plats där avsändarens eller mottagarens terminalutrustning är belägen inom området för en viss basstation, det sändande eller mottagande nätet eller början, slutet eller varaktigheten för en uppkoppling. Uppgifterna kan också gälla formatet hos det meddelande som förmedlas i nätet.

I jämförelse med traditionell postverksamhet kan identifieringsuppgifterna vid elektronisk kommunikation likställas med adress- och poststämpeluppgifterna på brev eller postpaket samt med storleken och formen på brev eller paket.

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. Identifieringsuppgifter får dessutom behandlas för fakturering, marknadsföringsändamål och teknisk utveckling, för att upptäcka missbruk som omfattar användning av tjänster och för att upptäcka fel och störningar.

Enligt 12 § får teleföretag, tillhandahållare av mervärdestjänster och sammanslutningsabonnenter behandla identifieringsuppgifter för teknisk utveckling av tjänster. I lagen tillåts inte att identifieringsuppgifter behandlas för statistisk analys.

Enligt 8 § 3 mom. är behandling av identifieringsuppgifter tillåten endast i den omfattning som behandlingens ändamål kräver och får behandlingen inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt. Identifieringsuppgifter får lämnas ut endast till dem 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.

Identifieringsuppgifter som kan användas för att identifiera en fysisk person är också personuppgifter. Enligt bestämmelserna om tillämpningsområde i 3 § skall personuppgiftslagen (523/1999) tillämpas på behand-

ling av personuppgifter, om inte något annat följer av lagen.

Vid utredning av missbruk av kommunikationsnäten och obehörigt röjande av företagshemligheter står informationsadministrativa metoder till förfogande, såsom kontroll av logguppgifterna om användarna, kontroll av uppgifterna om dem som loggar in i system som begränsar åtkomst samt uppgifter som samlats in i samband med tekniskt underhåll av systemen. I lagen om dataskydd vid elektronisk kommunikation uppställs inte några begränsningar för behandlingen av sådana uppgifter. Med hjälp av uppgifterna är det å andra sidan bara i undantagsfall möjligt att utreda missbruk i deras helhet.

Med andra ord är det möjligt att med hjälp av olika användaruppgifter, registreringsuppgifter och andra liknande logguppgifter fritt iaktta informationssystemen bl.a. vid utredning av missbruk.

I 6 kap. i lagen om integritetsskydd i arbetslivet (759/2004) finns bestämmelser om hämtning och öppnande av e-postmeddelanden som hör till arbetsgivaren samt om förfarandet i anslutning till detta i sådana fall då arbetstagaren är förhindrad att utföra sina arbetsuppgifter. Enligt 18 § har arbetsgivaren rätt att hämta och öppna meddelanden på en e-postadress som arbetsgivaren ställt till arbetstagarens förfogande endast då arbetsgivaren har vidtagit i lagen fastställda nödvändiga åtgärder för att skydda meddelandena.

I 19 § i lagen om integritetsskydd i arbetslivet bestäms närmare om grunderna för när arbetsgivaren på basis av uppgifter i rubrikfältet får hämta meddelanden som har kommit in eller skickats från arbetstagarens e-postadress och som det är nödvändigt att arbetsgivaren får vetskap om för att kunna slutföra förhandlingar i anslutning till sin verksamhet, betjäna kunder eller i övrigt trygga sina funktioner.

Enligt 20 § i lagen om integritetsskydd i arbetslivet får arbetsgivaren också öppna meddelanden som hör till arbetsgivaren, om det på basis av uppgifterna i rubrikfältet är uppenbart att meddelandet är avsett för arbetsgivaren och att arbetsgivaren måste få vetskap om innehållet och det inte går att få kontakt med avsändaren eller mottagaren för att ta reda på meddelandets innehåll eller för att få det sänt till en annan adress.

Över hämtandet och öppnandet skall utarbetas en rapport som undertecknas av de personer som deltagit i hämtandet och öppnandet och av vilken framgår vilket meddelande som har öppnats, varför meddelandet öppnats, tidpunkten och vem som utförde öppnandet samt till vem uppgift om meddelandets innehåll har givits. Rapporten skall utan obefogat dröjsmål tillställas arbetstagaren.

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. Som rekvisit för grov gärningsform anges i 4 § utnyttjande av särskild förtroendeställning, användning av specialanordningar eller program eller planmässighet eller föremålet är ett synnerligen förtroligt meddelande eller gärningen i hög grad kränker integritetsskyddet.

I 4 § i lagen om otillbörligt förfarande i näringsverksamhet (1061/1978) bestäms om skydd för affärshemligheter. Företagsspionageri, brott mot företagshemlighet och missbruk av företagshemlighet har kriminaliserats i 30 kap. 4–6 § i strafflagen. Begreppet företagshemlighet i strafflagen täcker både affärs- och yrkeshemligheter. Bestämmelser om skydd för affärs- och yrkeshemligheter finns dessutom i flera andra lagar.

Enligt 5 a kap. 3 § i tvångsmedelslagen (450/1987) kan teleövervakning utföras bl.a. vid utredning av sådana brott för vilka det strängaste straffet är fängelse i fyra år eller som riktat sig mot ett automatiskt databehandlingssystem. Eftersom det maximala straffet för brott mot företagshemlighet är fängelse i två år, kan teleövervakning använ-

das bara vid utredning av sådant företagsspioneri som samtidigt uppfyller rekvisitet för dataintrång enligt 38 kap. 8 § i strafflagen.

Med stöd av lagen om integritetsskydd i arbetslivet kan arbetsgivaren dömas till bötesstraff, om inte strängare straff har föreskrivits någon annanstans i lag.

Den gällande lagen om dataskydd vid elektronisk kommunikation tillåter inte att identifieringsuppgifter behandlas för utredning av obehörigt röjande av företagshemligheter.

I 20 § i lagen om dataskydd vid elektronisk kommunikation bestäms om åtgärdsrättigheter när det gäller att sörja för dataskyddet.

1.2 Europeiska unionens lagstiftning

Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (nedan personuppgiftsdirektivet) har genomförts genom personuppgiftslagen. Syftet med direktivet har varit att skydda enskilda personers grundläggande rättigheter och privatliv när personuppgifter behandlas.

Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (nedan direktivet om integritet och elektronisk kommunikation) har genomförts nationellt genom lagen om dataskydd vid elektronisk kommunikation. Lagen trädde i kraft i september 2004.

I artikel 5 i direktivet om integritet och elektronisk kommunikation bestäms om medlemsstaternas skyldighet att säkerställa konfidentialitet vid kommunikation via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster.

Enligt artikel 15 i direktivet om integritet och elektronisk kommunikation får medlemsstaterna genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i bl.a. artikel 5. Begränsningarna i ett demokratiskt samhälle skall vara nödvändiga, lämpliga och proportionella för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet eller för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i personuppgiftsdirektivet.

1.3 Den internationella utvecklingen samt lagstiftningen i utlandet

Allmänt

Bestämmelser om konfidentialitet vid kommunikation och i fråga om dataskydd ingår i några internationella konventioner. I artikel 8 i Europarådets konvention om skydd för de mänskliga rättigheterna och de grundläggande friheterna (FördrS 19/1990, Europeiska konventionen om mänskliga rätter) tryggas vars och ens rätt till respekt för privatliv och familjeliv, sin bostad och korrespondens.

Enligt artikel 5 i Europarådets konvention om skydd för enskilda vid automatisk databehandling av personuppgifter (FördrS 35–36/1992, Europarådets konvention om skydd av uppgifter) skall de personuppgifter som behandlas vid automatisk databehandling anskaffas och behandlas på ett tillbörligt och lagligt sätt. Uppgifterna får lagras endast för vissa bestämda och lagliga ändamål och de får inte användas på ett sätt som strider mot de nämnda ändamålen.

Den gällande regleringen baserar sig till centrala delar på direktivet om integritet och elektronisk kommunikation. När direktivet genomfördes nationellt utsträcktes de skyldigheter som garanterar konfidentiell kommunikation så att de också gäller sammanslutningsabonnenter.

De ändringar av regleringen som föreslås i denna proposition gäller till största delen detaljer i det nationella genomförandet och avhjälpande av problem som framkommit vid tillämpningen och tolkningen av den gällande nationella lagstiftningen. Begreppet sammanslutningsabonnent enligt lagen om dataskydd vid elektronisk kommunikation har inte tillägnats i andra länder. Den internationella jämförelsen har därför koncentrerats till en allmän presentation av lagstiftning som gäller skydd för privatlivet, skydd för företagshemligheter, skydd för personuppgifter

och dataskydd vid elektronisk kommunikation.

Sverige

Sveriges konstitution består av fyra författningar: regeringsformen (SFS 1974:152), successionsordningen, tryckfrihetsförordningen (SFS 1949:105) och yttrandefrihetsgrundlagen (SFS 991:1469). I 2 § i regeringsformen finns en bestämmelse om skydd för privatlivet. I 2 kap. 13 § i regeringsformen konstateras att yttrandefriheten och informationsfriheten, vilka tryggas konstitutionellt genom yttrandefrihetsförordningen, får begränsas med hänsyn till privatlivets helgd. I 2 kap. 3 § tryggas dessutom privatlivets helgd vid automatisk databehandling.

Sverige har en särskild lag om skydd för företagshemligheter (1990:40). Med företagshemlighet avses enligt 1 § sådan information om affärs- eller driftförhållanden i en näringsidkares rörelse som näringsidkaren håller hemlig och vars röjande är ägnat att medföra skada för näringsidkaren i konkurrenshänseende. Med information förstås både sådana uppgifter som har dokumenterats i någon form, inbegripet ritningar, modeller och andra liknande tekniska förebilder, och enskilda personers kännedom om ett visst förhållande, även om det inte har dokumenterats på något särskilt sätt. En arbetstagare som uppsåtligen eller av oaktsamhet utnyttjar eller röjer en företagshemlighet hos arbetsgivaren som han eller hon har fått del av i sin anställning under sådana förhållanden att han eller hon insåg eller borde ha insett att han eller hon inte fick avslöja den skall ersätta den skada som uppkommer genom hans eller hennes förfarande (7 §). Har förfarandet ägt rum sedan anställningen upphört, tillämpas bestämmelsen endast om det finns synnerliga skäl. Situationer av detta slag accentuerar betydelsen av avtal om sekretess.

Personuppgiftslagen (1998:2004) är den centrala dataskyddslagen i Sverige. Genom den har EU:s personuppgiftsdirektiv genomförts. I lagen regleras användningen av automatiserade personregister inom både den offentliga och den privata sektorn. I Sverige finns det inte någon särskild lag om integritetsskydd i arbetslivet, utan dessa angelägenheter regleras genom personuppgiftslagen. En separat lagberedning som gäller dataskydd i arbetslivet är aktuell, och lagförslaget lämnas antagligen under förra hälften av 2008.

Personuppgifter om arbetstagare får behandlas bara i de situationer som lagen tillåter. Syftet med behandlingen av personuppgifterna skall fastställas, och uppgifterna får inte behandlas för några andra ändamål. De vilkas uppgifter behandlas skall informeras om syftet. Exempel på situationer där behandling av personuppgifter tillåts enligt lagen är behandling på basis av samtycke, behandling på basis av avtal, varvid arbetstagaren och arbetsgivaren har kommit överens om behandlingen av personuppgifter för att avtalet skall genomföras, samt behandling för att en rättslig skyldighet skall kunna fullgöras. Personuppgifter kan likaså behandlas för att skydda ett vitalt intresse för arbetstagaren eller om uppgifterna används för att en arbetsuppgift i samband med myndighetsutövning skall kunna utföras samt i övriga fall där ett intresse hos arbetsgivaren eller någon annan till vilken personuppgifterna lämnas ut väger tyngre än skyddet av arbetstagarens personliga integritet. Arbetsgivarens rätt att utöva tillsyn på arbetsplatserna har inom rättspraxisen i Sverige avgjorts genom intresseprövning där arbetsgivarens direktionsrätt jämförs med arbetstagarnas integritetsskydd. De åtgärder som inskränker integriteten bör stå i rätt proportion till det mål som eftersträvas.

Direktivet om integritet och elektronisk kommunikation har genomförts i Sverige genom lagen om elektronisk kommunikation (2000:389). I lagen regleras även kommunikationsmarknadsfrågor, eftersom hela lagstiftningspaketet gällande fem EU-telekommunikationsdirektiv har genomförts genom lagen. Sverige har därmed inte någon särskild lag om dataskydd vid elektronisk kommunikation. Regleringen i den svenska lagen om elektronisk kommunikation riktas enbart till teleföretag och tillhandahållare av mervärdestjänster, dvs. inte till sammanslutningsabonnenter, som i sina kommunikationsnät behandlar användarnas förtroliga meddelande, identifieringsuppgifter och lokaliseringsuppgifter.

Enligt 2 § i lagen om elektronisk kommunikation lämpar personuppgiftslagen sig också i fråga om användning av kommunikationsnät och elektroniska kommunikationstjänster, om inte något annat följer av lagen.

Norge

Norges grundlag är från 1814 (Kongerikets Norges Grundlov). Grundlagen avviker till sin form en aning från de övriga länder som den internationella jämförelsen gäller, eftersom den inte innehåller några uttryckliga bestämmelser om skydd av privatlivet. I Norge har integritetsskyddet utformats genom rättspraxisen. År 1952 konstaterade högsta domstolen i Norge att identiteten åtnjuter skydd inom norsk rätt och att identitetsskyddet inbegriper skydd av privatlivet. Norge är inte medlem i Europeiska unionen men ingår i Europeiska ekonomiska samarbetsområdet, och därför är lagstiftningen inom den s.k. första pelaren, där direktiven om dataskydd och elektronisk handel ingår, bindande för Norge.

I Norge finns det inte någon särskild lag om skydd för företagshemligheter, utan bestämmelser om detta finns i marknadsföringslagen från 1972 (Lov om kontroll med markedsføring og avtalevilkår, markedsføringsloven).

Den nuvarande dataskyddslagen (Lov om behandling av personopplysninger) är från 2000. Den kompletteras av dataskyddsförordningen (Forskrift om behandling av personopplysninger). Lagen baserar sig på personuppgiftsdirektivet, och därmed har bestämmelserna nästan genomgående samma innehåll som bestämmelserna i direktivet.

I Norge har direktivet om integritet och elektronisk kommunikation genomförts genom en allmän lag om elektronisk kommunikation, dvs. Ekomloven (Lov om elektronisk kommunikasjon).

Det finns inte någon särskild lag om integritetsskydd i arbetslivet, utan anvisningar om detta har meddelats av Datatilsynet. Huvudregeln är att om arbetsgivaren vill läsa en arbetstagares e-post eller andra datafiler behöver arbetsgivaren arbetstagarens samtycke eller avgörs frågan på basis av 8 § f-punkten i dataskyddslagen och på basis av intresseprövning enligt direktivet. En norsk arbetsgivare får utifrån sin direktionsrätt bestämma att arbetsgivarens datasystem skall användas för arbetsrelaterade ändamål. Arbetsgivaren skall utforma regler för användningen av datasystemen, och då skall det preciseras i vilken omfattning systemet får användas för privata ändamål. Av reglerna, som skall fogas till företagets regler för intern kontroll, skall framgå under vilka omständigheter arbetsgivaren får läsa privat e-post. Utgångspunkten är att om sådana regler saknas har arbetsgivaren inte rätt att läsa arbetstagarnas e-post.

Om arbetsgivaren misstänker att en arbetstagare är illojal eller handlar i strid med interna regler och anvisningar, kan det för arbetsgivaren uppkomma rätt att kontrollera arbetstagarens e-post- eller brevkorrespondens. Om arbetsgivaren har tillräckliga grunder för misstankarna, kan kravet på i sak motiverade kontroller uppfyllas. Om arbetsgivarens kontrollintressen i ett konkret fall väger tyngre än arbetstagarens rätt till integritet, kan kontrollen utföras utan arbetstagarens samtycke.

Danmark

Den danska grundlagen från 1953 innehåller två bestämmelser om integritetsskydd. I 71 § garanteras medborgarna personlig integritet. Danska medborgare får inte berövas sin frihet på grund av politisk eller religiös övertygelse eller härkomst.

I 72 § bestäms om kränkning av hemfriden. Husrannsakan, beslagtagning och utforskning av brev och annat skriftligt material, liksom intrång i post, datakommunikation och telefonhemligheten får genomföras endast enligt föreläggande av domstol, om inte något annat anges i lag. Lagrummet är tillämpligt på all datakommunikation och elektronisk information.

Den danska marknadsföringslagen (Maerkedsfoeringsloven 1389, 21.12.2005) reglerar skyddet för företagshemligheter. Enligt 19 § får den som är anställd hos eller samarbetar med ett företag eller utför ett uppdrag för ett företag inte olovligen skaffa eller försöka skaffa information om eller komma över företagshemligheter som gäller det aktuella fö-

retaget. Om en person som avses ovan har fått information om företagshemligheter på laglig väg, får han eller hon inte utan tillstånd av den berörda lämna ut eller använda företagshemligheterna. Förbudet gäller i tre år efter det att anställningsförhållandet, samarbetet eller uppdraget har upphört. Reglerna tillämpas på samma sätt när det gäller andra personer som har laglig tillgång till företagsinformation.

Den danska dataskyddslagen (Lov om behandling af personoplysninger nr 429, 31.5.2000) är från 2000. Genom lagen genomfördes personuppgiftsdirektivet. Bestämmelser om dataskydd vid elektronisk kommunikation finns i 2003 års ändring av telelagstiftningen (Lov om konkurrence- og forbrugerforhold på telemarkedet Lov nr. 418 af 31. maj 2000), genom vilken direktivet om integritet och elektronisk kommunikation genomfördes.

Det finns inte någon särskild lag om integritetsskydd i arbetslivet, utan detta regleras utifrån personuppgiftslagen. Myndigheterna i landet har inte intagit någon speciellt stark ståndpunkt avseende integritetsskydd i arbetslivet. Den danska dataskyddslagen ger arbetsgivaren möjlighet att samla in och till och med röja personuppgifter utan arbetstagarens samtycke, om det är nödvändigt för att fullgöra en rättslig skyldighet, för att utföra ett uppdrag som är betydelsefullt med tanke på samhället eller för att uppfylla ett lagligt behov som väger tyngre än arbetstagarens intresse.

Tyskland

Tyska förbundsrepublikens grundlag (Grundgesetz) är från 1949. Den har senast ändrats i samband med återföreningen av Tyskland 1990. I artikel 10 i grundlagen tryggas brev- och datakommunikationshemligheten, och undantag från detta kan göras endast genom bestämmelser i lag. När syftet med en inskränkning är att säkerställa den demokratiska samhällsordningen eller säkerheten i en förbundsstat kan det i lagstiftningen bestämmas om att den person som blivit föremål för intrånget inte skall få veta om åtgärden. I stället för domstolar fungerar då organ som utsetts av förbundsdagen som rättsvägar.

I 85 § i telekommunikationslagen (Telekommunikationsgesetz) bestäms närmare om den kommunikationshemlighet som tryggas i grundlagen. Kommunikationshemligheten omfattar även försök att få kontakt. I 86 § i telekommunikationslagen bestäms om förbud mot teleavlyssning samt tystnadsplikt för den som ansvarar för mottagningsanordningarna. I 87 § bestäms på motsvarande sätt om att den som i yrkesmässigt syfte ansvarar för datakommunikationsanordningar skall ha tekniska skyddsmetoder bl.a. för att vidmakthålla kommunikationshemligheten.

I straffprocessordningen (Strafprozessordnung, StPO) bestäms om tvångsmedel, även när det gäller datakommunikation.

Bestämmelser om skydd för företagshemligheter finns i 17 § i en lag som gäller ohederlig konkurrens. Företagshemligheten omfattar kommersiellt värdefull information som inte är offentligt tillgänglig och den till vilken informationen tillhör har uttryckt en objektiv avsikt att hemlighålla informationen. Enligt 1 mom. skall straff utdömas för en arbetstagare, en person som deltar i läroavtalsutbildning eller någon annan som under anställningsförhållandet utan tillstånd röjer en sådan affärs- eller industrihemlighet för tredje part som anförtrotts eller delgetts honom eller henne inom ramen för anställningsförhållandet, om han eller hon röjer någonting med anledning av konkurrens eller personligt intresse, för att gagna tredje part eller skada näringsidkaren. Enligt 2 mom. bestraffas den som av de orsaker som beskrivs ovan olovligen skaffar affärs- eller industrihemligheter genom att använda tekniska metoder, skapa en kopia som innehåller hemligheter eller lösgöra ett föremål där hemligheter ingår. Detsamma gäller den som använder eller för någon annan uttrycker en affärsmässig eller industriell hemlighet som han eller hon har skaffat eller fått utan tillstånd av en arbetstagare som uttryckt den olovligen, eller som ett resultat av sitt eget eller någon annans agerande.

De tyska dataskyddslagarna hör till de striktaste inom Europeiska unionen. Världens första dataskyddslag stiftades 1970 i delstaten Hessen. Tysklands nuvarande data-

skyddslag (Bundesdatenschutzgesetz) är från 1990, och den har senast reviderats 2002. Lagen ger de registrerade vidsträckta möjligheter att motsätta sig behandlingen av uppgifter. Lagen kräver att företagen skall utse en dataskyddsansvarig om företaget samlar in, behandlar eller använder personuppgifter. Databaser som innehåller personuppgifter skall registreras hos dataskyddsmyndigheten. Vikten av samtycke av den som registreras har betonats.

Bestämmelser om dataskydd vid elektronisk kommunikation ingår i telekommunikationslagen som ändrades 2004 och med vilken har kombinerats dataskyddsförordningen gällande datakommunikation från år 2000.

Arbetsgivarens möjlighet att följa hur arbetstagarna använder e-post eller internet beror på gällande rättspraxis. I princip har arbetsgivaren inte rätt att få information om hur arbetstagarna använder e-post eller internet. Om arbetsgivaren har förbjudet användningen av kommunikationstjänsterna för privat bruk kan arbetsgivaren följa upp endast sådana identifieringsuppgifter som gäller användningen av internet. Om arbetsgivaren konkret misstänker, att kommunikationstjänsterna har använts olovligen får arbetsgivaren följa hur de används i den utsträckning som behövs för att reda ut missbruk.

Estland

Estlands nuvarande grundlag är från 1992. I lagen tillstås rätten till privatliv, konfidentialitet vid kommunikation och, åtminstone partiellt, dataskydd.

Enligt artikel 43 var och en har rätt till förtrolig kommunikation per brev, telegram, telefon eller något annat kommunikationsmedel som används allmänt. Undantag är möjliga endast med domstolens samtycke, i de fall som anges i lag och med iakttagande av lagenliga förfaranden i syfte att förebygga brott eller skaffa material för utredning av brott. För avlyssning av kommunikation krävs tillstånd av en domstol. Bevismaterial som skaffats illegalt får inte läggas fram inför domstol.

Skydd för företagshemligheter regleras i konkurrenslagen från 1993 (RT I 1993, 47, 642, i kraft den 1 januari 1994). I 7 § definieras missbruk av företagshemlighet som ojust konkurrens, som är förbjuden. I konkurrenslagen ingår inte några bestämmelser om arbetstagarnas skyldigheter när det gäller företagshemligheter. Dessa skyldigheter bestäms utifrån lojalitetsbestämmelserna i arbetslagstiftningen.

Estland fick sin första dataskyddslag 1996. Den nuvarande lagstiftningen, Estlands lag om skydd för personuppgifter (RT I 2003, 26, 158), genom vilken lagstiftningen ändrades så att den stämmer överens med personuppgiftsdirektivet, trädde i kraft den 1 oktober 2003 och har redan ändrats en gång efter det.

I 10 kap. i lagen om elektronisk kommunikation (RT2 I 2004, 87, 593, i kraft den 1 januari 2005) finns bestämmelser om informationssäkerhet och dataskydd.

Storbritannien

I Storbritannien baserar regleringen av de grundläggande fri- och rättigheterna sig på rättspraxis och på Europarådets människorättskonvention. Den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna sattes statsinternt i kraft i Storbritannien genom 1998 års Human Rights Act. Privatlivet och familjelivet skyddas genom artikel 8 i konventionen och yttrandefriheten genom artikel 10.

I Storbritannien baserar skyddet för företagshemligheter sig på rättspraxis och avtal om sekretess. Bestämmelser om skydd för personuppgifter finns i 1998 års Data Protection Act, genom vilken EU:s personuppgiftsdirektiv genomfördes. Direktivet om integritet och elektronisk kommunikation genomfördes 2003 genom författningen Privacy and Electronic Communications (EC Directive) Regulations 2003 (2003 No. 2426), där det finns bestämmelser för tillhandahållare av kommunikationstjänster om bl.a. förtroliga identifierings- och lokaliseringsuppgifter samt elektronisk direktmarknadsföring. I Storbritannien används inte begreppet sammanslutningsabonnent, som tillägnats i Finland. Enligt 29 punkten får tillhandahållare av kommunikationstjänster behandla uppgifter, om det är nödvändigt för att införa, an-

vända eller försvara lagliga rättigheter eller om det annars är nödvändigt att behandla uppgifterna i anslutning till en rättsprocess. Uppgifter får dessutom behandlas om det är nödvändigt för att förebygga eller utreda brott.

Konfidentialitet vid elektronisk kommunikation baserar sig i Storbritannien på Regulation of Investigatory Powers Actiin (RIPA) från år 2000. Med stöd av RIPA utfärdades år 2000 författningen Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (2000 No. 2699). Med avvikelse från huvudregeln för konfidentialitet vid kommunikation tillåter författningen att företag och offentliga instanser iakttar kommunikationen i sina nät även när det gäller innehållet i meddelandena, bl.a. i syfte att konstatera någon omständighet och säkerställa att författningar och användningsregler följs, av skäl som hänför sig till den nationella säkerheten, för att utreda och förhindra brott eller för att varsebli olovligt brukande.

Den som ansvarar för kommunikationsnätet skall informera nätanvändarna om att kommunikationen i nätet kan följas.

Ryssland

Rysslands grundlag är från 1993. Enligt artikel 23 i grundlagen har var och en rätt till privatliv, personliga och familjens hemligheter samt bevarande av personlig heder och personligt anseende. Dessutom har var och en rätt till integritet i fråga om brevhemlighet, telefon- och kabelkommunikation och andra kommunikationsformer. Undantag kan tillåtas endast genom föreläggande av domstol.

Frågor som gäller öppenhet och skydd i fråga om information har i praktiken koncentrerats till federationsnivå. Den centrala författningen är från 1995, Ryska federationens lag om information samt behandling och skydd av information. Den senaste ändringen av lagen trädde i kraft den 1 januari 2004.

Den nämnda lagen skyddar fri informationsförmedling. Enligt lagen skall bandupptagning av telefonsamtal, kontroll av elektronisk kommunikation, fördröjning, kontroll och beslagtagning av brevförsändelser och andra ingrepp i informationsförmedlingshemligheten basera sig på föreläggande av domstol.

I federationslagen om skydd för företagshemligheter (lag nr N98-FZ, 29.7.2004) regleras användningen av kommersiella hemligheter och möjligheterna att trygga konfidentiell information. I lagen definieras affärs- och yrkeshemligheter endast i allmänna termer. Den som innehar affärshemligheter skall specificera dem. I lagen förtecknas å andra sidan sådana uppgifter som under inga omständigheter kan betraktas som företagshemligheter och uppgifter som beroende på situationen kan betraktas som företagshemligheter. Sådana uppgifter gäller bl.a. antalet arbetstagare, belöningssystemen, arbetsförhållandena, inbegripet säkerhetsarrangemang, arbetsrelaterade olycksfall, yrkesrelaterade dödlighetssiffror, lediga arbetsplatser och lagbrott.

I lagstiftningen i Ryssland tryggas företagshemligheter också genom bestämmelser i civilkoden och konkurrenslagstiftningen. I artikel 139 i Ryska federationens civilkod bestäms om att affärs- och yrkeshemligheter är skyddade genom civilrättsliga rättsmedel, i synnerhet genom skadeståndsskyldigheter. Arbetstagare hos den som innehar företagshemligheter och en tredje person som olovligen tar emot information om företagshemligheter kan bli skadeståndspliktiga. Enligt den nämnda artikeln i civilkoden skall informationen ha ett faktiskt eller potentiellt konkurrensvärde. För det andra skall informationen vara okänd för utomstående samt allmänt taget onåbar för informationskanaler som lagen tillåter. För det tredje skall informationsägaren vidta åtgärder för att skydda informationens konfidentialitet. I annat fall kan den som äger informationen inte påvisa att den är en företagshemlighet.

Enligt lagstiftningen skall företaget vidta flera åtgärder för att informationen skall få status som företagshemlighet. Företaget skall förteckna material som omfattas av organisationens affärshemligheter och begränsa tillgången till affärshemligheter genom att utforma förfaranden för behandling av den aktuella informationen och för övervakning av att förfarandet iakttas. Företaget skall också förteckna de personer som har tillgång till in-

formationen i fråga. Dessutom skall företaget reglera förhållandet till användningen av information som gäller affärshemligheter. Det här genomförs beträffande arbetstagare med hjälp av arbetsavtal och beträffande affärspartner med hjälp av affärsavtal. Information som gäller affärshemligheter skall dessutom förses med en stämpel som utvisar ägaren till informationen.

Enligt rysk lag skall personalen följa de bestämmelser om konfidentialitet som arbetsgivaren infört. Medlemmar av personalen får inte heller röja arbetsgivarens affärshemligheter under en tid som fastställts i ett avtal med arbetsgivaren under anställningsförhållandet, eller under tre år efter det att anställningsförhållandet upphört, om inget avtal har ingåtts. Arbetstagaren skall ersätta arbetsgivaren för de skador som denne lidit på grund av att arbetstagaren har lämnat ut uppgifter om företagshemligheter som denne fått kännedom om. I den ryska arbetsavtalslagen finns exakta bestämmelser om arbetstagarens ersättningsskyldighet och straffansvar. När anställningsförhållandet upphör skall arbetstagaren tillhandahålla arbetsgivaren allt material som innehåller affärshemligheter. Arbetsgivaren skall i sin tur informera arbetstagarna om företagshemligheter, arbetstagarens skyldigheter och sanktioner vid överträdelser.

I lagen om information samt behandling och skydd av information regleras personuppgifter på ett allmänt plan, även om Ryssland inte omfattas av Europarådets dataskyddskonvention. Uppgifter som gäller personer betraktas som förtroliga uppgifter. Med personuppgifter, dvs. uppgifter om medborgarna, avses faktauppgifter, uppgifter om händelser och livsstil vilka specificerar enskilda medborgare. Enligt lagen är det förbjudet att utan personens samtycke samla in, lagra, använda och sprida uppgifter om en fysisk persons privatliv liksom att behandla personliga uppgifter eller uppgifter om familjehemligheter, om det inte handlar om behandling av uppgifter enligt föreläggande av domstol eller den berörda personen har samtyckt till åtgärden. Likaså får uppgifter som kränker kommunikationshemligheten samlas in, lagras, användas och spridas bara med stöd av särskilda bestämmelser eller samtycke av den som saken gäller.

I lagen om information samt behandling och skydd av information hänvisas till den mera detaljerade federationslagstiftningen. En detaljerad dataskyddslag är fortfarande under beredning. Förslag om dessa lämnades 1998 och 2000, och en lagproposition har behandlats i den ryska duman 2006. I bakgrunden finns Rysslands strävan att ratificera Europarådets dataskyddskonvention.

I Ryssland finns än så länge inte någon dataskyddslagstiftning för elektronisk kommunikation eller arbetslivet.

1.4 Bedömning av nuläget

De mål i lagen om dataskydd vid elektronisk kommunikation som gäller sekretess har nåtts relativt bra i företag och sammanslutningar.

Lagen om dataskydd vid elektronisk kommunikation gör det möjligt för sammanslutningsabonnenter att behandla identifieringsuppgifter i den omfattning som är nödvändig för sammanslutningsabonnenternas normala verksamhet. I praktiken har det visat sig vara problematiskt att tillämpa vissa av de gällande bestämmelserna. I synnerhet 13 § har visat sig ha en så snäv formulering att den inte garanterar sammanslutningsabonnenterna tillräckliga förutsättningar för verksamheten.

Det har framkommit svårigheter när det gäller sammanslutningsabonnenternas möjligheter att utreda missbruk av sina kommunikationsnät med hjälp av elektronisk kommunikation och att låta sådana missbruk bli föremål för förundersökning. Det har förekommit oklarheter i fråga om tillämpningen av missbruksbestämmelsen i 13 § när det gäller missbruk av sammanslutningsabonnenternas kommunikationsnät. Det har ansetts att den gällande lagen inte tillåter att sammanslutningsabonnenterna själva samlar in bevis på missbruk, och i de flesta fall har inte heller teleövervakning stått till förfogande.

Enligt näringslivets och myndigheternas gemensamma strategi för att förebygga brott som riktas mot företagsverksamhet (Inrikesministeriets publikationsserie 15/2006) har lagen om dataskydd vid elektronisk kommu-

nikation visat sig något problematisk för företag som har blivit föremål för brott. I strategin ses det som en olägenhet att företagen har bristfälliga möjligheter att göra en polisundersökning av olovligt utlämnande av företagshemligheter, om utlämningen har skett i elektronisk form.

I undersökningar om företagssäkerhet som koncentrerats till underrättelseverksamhet, som bland annat skyddspolisen utför regelbundet, har ca 10 procent av företagen uppgett att de har upptäckt och 18 procent uppgett att de misstänker olovligt inhämtande av information under de senaste två åren.

När det gäller utredning av missbruk med hjälp av elektronisk kommunikation och när det gäller att låta sådant missbruk bli föremål för förundersökning har det framkommit problem som inte kunde förutses när lagen stiftades. Också teleföretagen har ställt sig avvaktande till tolkningen av bestämmelserna. Dessutom har problem kunnat uppstå på grund av att aktörerna har förväxlat de roller som avses i lagen beträffande kommunikationsparterna, teleföretagen och sammanslutningsabonnenterna.

Att producera och använda kommunikationstjänster kräver mycket utvecklingsarbete av teknisk natur. I praktiken har det kommit fram att det utvecklingsarbete som behövs delvis också innehåller utvecklingsarbete som inte är enbart tekniskt, men som är helt oumbärligt med tanke på utvecklingen. Därför bör regleringen göra det möjligt för sammanslutningsabonnenter att behandla identifieringsuppgifter för att utveckla deras tjänster och verksamhet också i annat än i enbart tekniskt hänseende. Likaså har det visat sig att teleföretagen på grund av lagen eller tolkningarna av den inte har lämnat ut sådana identifieringsuppgifter till sammanslutningsabonnenterna, utifrån vilka företaget eller sammanslutningen skulle ha kunnat optimera telefonitrafiken mellan sina fasta disponibla telefoner och mobiltelefoner på ett så kostnadseffektivt sätt som möjligt.

Dataskyddsbestämmelserna i 20 § i den gällande lagen motsvarar inte helt och hållet det som krävs i fråga om lämpligt arbete för dataskyddet. Efter det att lagen stiftades har hoten mot dataskyddet förändrats och breddats väsentligt. Det beräknas att mer än hälften av all e-posttrafik består av oönskade meddelanden inom direktmarknadsföring. Den stora mängden s.k. skräppost kan äventyra enskilda användares kommunikationsmöjligheter.

Därför bör effektiva åtgärder för att genomföra dataskyddet stå till förfogande på ett smidigare sätt än förut.

2 Målsättning och de viktigaste förslagen

I denna proposition föreslås ändringar av lagen om dataskydd vid elektronisk kommunikation och av vissa andra lagar.

Utifrån praktiska behov föreslås att teleföretag, de som tillhandahåller mervärdestjänster och sammanslutningsabonnenter skall ha rätt att med hjälp av automatisk databehandling behandla identifieringsuppgifter för statistisk analys, så att de aktörerna bl.a. skall kunna utveckla sina tjänster och verksamheter också i annat än i enbart tekniskt hänseende.

Det föreslås att sammanslutningsabonnenternas rättigheter att behandla identifieringsuppgifter i samband med missbruk skall utvidgas. Samtidigt föreslås att behandlingsrättigheterna i missbrukssituationer ses över när det gäller teleföretag och tillhandahållare av mervärdestjänster.

Det föreslås att regleringen preciseras så att en sammanslutningsabonnent under vissa förutsättningar skall ha rätt att behandla identifieringsuppgifter i samband med elektronisk kommunikation för att utreda olovligt brukande av sina avgiftsbelagda informationssamhällstjänster eller kommunikationstjänster samt brukande av kommunikationstjänster i strid med anvisningarna för användningen av dem.

Det föreslås att sammanslutningsabonnenternas rätt att behandla identifieringsuppgifter utvidgas så att en sammanslutningsabonnent under vissa förutsättningar skall få behandla identifieringsuppgifter när det är frågan om obehörigt röjande av företagshemligheter som är av central betydelse för näringsverksamheten.

Både i fråga om olovligt brukande i strid med anvisningarna och i fråga om företagshemligheter förutsätts att den planerade an-

vändningen av kommunikationsnätet och kommunikationstjänsterna samt skyddet för företagshemligheter har ordnats genom lämpliga åtgärder för dataskyddet och åtgärder för användarhanteringen. De föreslagna rättigheterna att behandla identifieringsuppgifter berättigar inte sammanslutningsabonnenterna till att ta del av innehållet i meddelanden.

Genom behandlingen av identifieringsuppgifterna får sammanslutningsabonnenterna inte reda på identifieringsuppgifterna för andra meddelanden än sådana som sänts eller tagits emot via deras egna kommunikationstjänster. När det gäller användningen av kommersiella e-posttjänster, nätbankstjänster eller andra tekniskt skyddade tjänster avslöjar identifieringsuppgifterna endast adressen på den tjänst som använts, tidpunkten för användningen och hur länge tjänsten har använts.

Sammanslutningsabonnenter i arbetsgivarställning skall ta upp ärenden som gäller behandling av identifieringsuppgifter till behandling i ett samarbetsförfarande och informera arbetstagarna om dem.

Dataombudsmannen skall övervaka den behandling av identifieringsuppgifter som enligt de föreslagna ändringarna blir möjlig för sammanslutningsabonnenterna.

Den föreslagna ändringen av dataskyddsbestämmelsen innebär att bestämmelsen bättre svarar mot de nuvarande behoven av att sörja för dataskyddet i kommunikationsnäten eller tjänsterna. De livsviktiga samhällsfunktionerna är nära beroende av kommunikationsnät, kommunikationstjänster och informationssystem. Säkerställandet av elektroniska informations- och kommunikationssystems funktion intar en central position när det gäller att skydda den kritiska infrastrukturen. De hot mot dataskyddet som Finland utsätts för härrör ofta från andra länder. Eftersom möjligheterna att påverka utländska aktörer och system är begränsade, måste det gå att minska de störande verkningarna av problemen genom åtgärder som vidtas av de inhemska teleföretagen, dem som tillhandahåller mervärdestjänster och sammanslutningsabonnenterna.

Syftet med de ändringar som gäller möjligheterna att lämna ut uppgifter som Kommunikationsverket erhållit är att effektivisera bekämpningen och utredningen av hot mot dataskyddet.

2.1 Uppföljning av ändringarnas konsekvenser

Kommunikationsministeriet tänker tillsätta en uppföljningsgrupp för att bedöma konsekvenserna av de föreslagna ändringarna. Uppföljningsgruppen bör bestå av företrädare för åtminstone sammanslutningsabonnenterna, Kommunikationsverket, dataombudsmannen, teleföretagen och arbetsmarknadscentralorganisationerna.

Uppföljningsgruppens mandattid avses börja i januari 2009 och pågå till utgången av juni 2010. Uppföljningsgruppen bör låta utföra undersökningar om hur de föreslagna ändringarna av rätten att behandla identifieringsuppgifter påverkar företagens dataadministration och konfidentialiteten vid elektronisk kommunikation. Dessutom skall gruppen följa upp hur myndighetsövervakningen av identifieringsuppgifter genomförs och tillräcklighet av övervakningens resurser.

3 Propositionens konsekvenser

3.1 Ekonomiska konsekvenser

Det kan bedömas att propositionen har positiva ekonomiska konsekvenser för teleföretagen, sammanslutningsabonnenterna, myndigheterna och konsumenterna. Tydliga och entydiga behandlingsregler och bestämmelser om erhållande av information minskar onödiga processer och sparar på resurserna för alla aktörer

Förslaget erbjuder bättre förutsättningar för elektronisk kommunikation, vilket på grund av kostnadseffekterna och konsekvenserna för konkurrenskraften har betydelse för den ekonomiska utvecklingen i hemlandet, för företagens konkurrenskraft, för den inre marknaden och därmed för utvecklingen av hela det europeiska välfärdssamhället. Samtidigt förbättras ställningen för de konsumenter som använder elektroniska tjänster och underlättas ställningen för de myndigheter som övervakar lagen.

I egenskap av sammanslutningsabonnenter tillämpar företag och andra organisationer

lagens bestämmelser om behandling av identifieringsuppgifter i samband med sin elektroniska kommunikation. Bestämmelserna om behandling har trots den strikt konfidentiella kommunikationen gjort det möjligt för sammanslutningsabonnenterna att få rätt att behandla användarnas identifieringsuppgifter. Det är viktigt att åläggandena enligt lagen är tydliga med tanke på de finländska företagens och sammanslutningarnas ställning.

3.2 Konsekvenser för företagsverksamheten

De föreslagna ändringarna av behandlingsreglerna för identifieringsuppgifter förbättrar verksamhetsförutsättningarna för både små och stora företag. Ändringarna ger sammanslutningsabonnenterna bättre möjligheter att säkerställa att deras kommunikationsnät och tjänster används på planerat sätt för att stödja näringsverksamheten.

Oklara tolkningar undanröjs när rättigheterna att behandla identifieringsuppgifter blir tydligare. Rätten enligt de nya 13 a–13 j § att behandla identifieringsuppgifter i fall av missbruk ger sammanslutningsabonnenterna bättre möjligheter att avvärja brukande i strid med anvisningarna eller olovligt brukande av deras kommunikationsnät och -tjänster Likaså kan olovligt brukande av tjänster som medför kostnader förebyggas och utredas effektivt.

De föreslagna ändringarna förbättrar sammanslutningsabonnenternas möjligheter att säkerställa att deras kommunikationsnät och tjänster används på planerat sätt som ett stöd för näringsverksamheten.

Genom propositionen förbättras sammanslutningsabonnenternas möjligheter att skydda företagshemligheter. Den föreslagna ändringen behövs för att säkerställa ett effektivt skydd för företagshemligheter som är centrala med tanke på teknologiskt eller annat utvecklingsarbete och företagets affärsverksamhet. Enligt de nya 13 a–13 j § skall en sammanslutningsabonnent få behandla identifieringsuppgifter när det finns grundad anledning att misstänka att någon har sänt företagshemligheter eller obehörigen gett tillträde till företagshemligheter. Genom bestämmelsen främjas den exklusiva rätt till egendom som ägaren av kunskapskapitalet har och dennes rätt att dra ekonomisk nytta av sin egendom. Den föreslagna revideringen tryggar också bättre än tidigare möjligheterna att säkerställa t.ex. fortsatt produktutvecklingsarbete oavsett informationsläckage, eftersom sammanslutningsabonnenten i väsentlig grad kan avgränsa dem som misstänks för läckaget.

De bestämmelser om dataskydd som föreslås bli ändrade möjliggör åtgärder för att genomföra dataskyddet också i syfte att trygga kommunikationsnäten eller därtill anslutna tjänster för dem som tillhandahåller mervärdestjänster eller för sammanslutningsabonnenterna samtidigt som åtgärdernas täckning görs smidigare och utformas så att de uppfyller de nuvarande kraven.

Den föreslagna nya regleringen enligt vilken teleföretagen får lämna ut identifieringsuppgifter till sammanslutningsabonnenter för statistisk analys öppnar nya affärsmöjligheter för teleföretagen. Propositionen medför inte några direkta investeringsbehov för teleföretagen på denna punkt, men den kan anses ha indirekta konkurrenskonsekvenser. Teleföretagen konkurrerar sinsemellan genom rapporteringstjänster, genom vilka de producerar och bearbetar uppgifter för kunderna om deras telefonbeteende när det gäller avgiftsbelagda tjänster. Då förslaget gör det möjligt att lämna ut fullständiga identifieringsuppgifter till kunderna, kan det förändra konkurrenssituationen i fråga om rapporteringstjänsterna men också möjliggöra nya tjänster.

De viktigaste ekonomiska konsekvenserna gäller tryggandet av företagens verksamhetsbetingelser. Teleföretagen, de som tillhandahåller mervärdestjänster och sammanslutningsabonnenterna får bättre möjligheter att utveckla sin verksamhet, avvärja brottslighet som riktas mot företagens kunskap och datanät, samt bättre möjligheter att upprätthålla dataskyddet.

De föreslagna skyldigheterna för sammanslutningsabonnenterna när rätten att behandla identifieringsuppgifter utövas medför ett visst mått av kostnader för de företag och övriga organisationer som börjar utöva rättigheterna enligt den föreslagna regleringen. Kostnader föranleds av personalutbildning och avgiftsbelagda övervakningsåtgärder

samt en ökad mängd administrativt arbete när skyldigheterna enligt de föreslagna 13 a–13 j § fullgörs.

3.3 Konsekvenser för myndigheterna

Det föreslås att uppgiftsfördelningen mellan Kommunikationsverket och dataombudsmannen ändras i fråga om identifieringsuppgifter som sammanslutningsabonnenterna behandlar i missbrukssituationer, t.ex. olovligt brukande i strid med anvisningarna för kommunikationsnätet och kommunikationstjänsten och obehörigt röjande av företagshemligheter.

Förslaget innebär inte att dessa tillsynsmyndigheters uppgifter utökas på ett sätt som skulle ha några direkta statsfinansiella konsekvenser. För dataombudsmannens byrå som i egenskap av en liten enhet inte kan anvisa resurser för den nya tillsynsuppgiften med hjälp av intern omstrukturering kräver den föreslagna tillsynen dock att anslagen ökas enligt en preliminär uppskattning med totalt 260 000 euro på årsnivå för att anställa två specialsakkunniga och en kontorsperson samt för att täcka de merkostnader dessa ger upphov till. Vid en exakt uppskattning av resurserna och kostnaderna för dem skall behöriga ministerier och de som avgiftsskyldigheten gäller höras. Avgiftsskyldigheten skall stå i rätt proportion till den som är föremål för tillsynen och verksamhetens art. Behovet av tilläggsresurser kan beaktas i form av en förordning om avgiftsbelagda prestationer som det ministerium som saken gäller skall bereda med stöd av lagen om grunderna för avgifter till staten (150/1992). De preciserade bestämmelserna anger tydligare villkor för tillsynsmyndigheternas, Kommunikationsverkets och dataombudsmannens arbete, vilket också effektiviserar övervakningen av lagen och möjligheterna att uppnå målen.

Förslaget bidrar till att främja myndigheternas internationella samarbete genom att Kommunikationsverket ges rätt att till sådana organ i andra stater som motsvarar CERT-FI-enheten och som har till uppgift att förebygga eller utreda kränkningar av dataskyddet riktade till kommunikationsnät och kommunikationstjänster, lämna ut identifieringsuppgifter som verket erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskyddet. Eftersom hoten mot dataskyddet i typiska fall är gränsöverskridande, innebär Kommunikationsverkets preciserade befogenheter ökade förutsättningar att främja dataskyddet i samråd med organisationer i andra länder.

3.4 Samhälleliga konsekvenser

Genom att precisera rättigheterna och skyldigheterna för olika parter i kommunikationen kan man förbättra i synnerhet konsumenternas och företagens allmänna förtroende för den elektroniska kommunikationen och därigenom den elektroniska affärs- och kommunikationsmiljön som helhet.

Den snabba teknologiska utvecklingen och den omfattande utbredningen av datatekniska verktyg i nätverk har samtidigt fört med sig nya risker och möjligheter att lamslå centrala samhällsfunktioner med hjälp av datanäten. Under sådana omständigheter får betydelsen av dataskydd och tidsenlig reglering av dataskyddet en allt tydligare framtoning.

Företagens och de övriga sammanslutningsabonnenternas verksamhetsmöjligheter förbättras genom förslaget, och regleringen ger bättre möjligheter att sörja för användbarheten hos och dataskyddet i sammanslutningsabonnenternas system samtidigt som lagens ursprungliga mål i fråga om integritetsskydd uppnås. De föreslagna kraven i fråga om förfaranden säkerställer integritetsskyddet och konfidentialiteten vid kommunikation för dem som använder kommunikationsnäten och tjänsterna. Det förbättrade skyddet för företagshemligheter utökar företagens verksamhetsmöjligheter och bidrar till att främja den ekonomiska utvecklingen och välfärden. Företagens förbättrade verksamhetsmöjligheter i hemlandet främjar deras verksamhet även i den internationella miljön och inom konkurrensen.

3.5 Konsekvenser för informationssamhället

Förutsättningen för de föreslagna behandlingsrättigheterna för sammanslutningsabonnenterna är skyldighet att sörja för dataskyddet avseende kommunikationsnäten och

skyddet för företagshemligheter och att utarbeta anvisningar för användningen av kommunikationsnäten och kommunikationstjänsterna samt för behandlingen av företagshemligheter. Det kan antas att skyldigheterna på lång sikt förbättrar planeringen av användningen av kommunikationsnäten och möjligheterna att skydda sig mot datasäkerhetsrisker samt möjligheterna att i en elektronisk omvärld skydda informationsmaterial som är viktigt för företagens verksamhet.

3.6 Konsekvenser för den enskildas ställning

De föreslagna ändringarna av sammanslutningsabonnenternas rättigheter att behandla identifieringsuppgifter påverkar medborgarnas konfidentiella kommunikation till den del de som använder sammanslutningsabonnenternas kommunikationsnät och tjänster använder en sammanslutningsabonnents kommunikationsmöjligheter för sin egen kommunikation. Avsikten med avgränsningen av behandlingsrättigheterna till att gälla allvarliga fall och förfaranden i anslutning till dem har varit att åstadkomma en balans mellan de berättigade intressena för dem som använder kommunikationsnäten och tjänsterna å ena sidan och sammanslutningsabonnenternas berättigade intressen å andra sidan.

Många sammanslutningsabonnenter är också arbetsgivare, vilket innebär att de skall ta upp ärenden som gäller elektronisk kommunikation och uppföljning av den till behandling i ett samarbetsförfarande och informera arbetstagarna om dessa.

Det kan antas att den tillägnade lösningen gör det möjligt att samordna behoven inom enskild kommunikation och elektronisk kommunikation å ena sidan och sammanslutningsabonnenternas behov å andra sidan så att sammanslutningsabonnenterna kan tillåta att deras kommunikationsnät används även för personliga syften utan att de behöver göra avkall på säkerheten i nätet.

Identifieringsuppgifterna för användarnas kommunikation skall få undersökas i vissa fall, men innehållet i meddelandena kommer under inga omständigheter att röjas för utomstående. I och med lagens bestämmelser om förfaranden får arbetstagarna kännedom om de situationer som berättigar till behandling av identifieringsuppgifterna.

Det kan bedömas att de föreslagna bestämmelserna också har positiva konsekvenser med tanke på integriteten för dem som använder kommunikationsnäten och tjänsterna, eftersom åtgärder som inverkar störande ofta kan äventyra inte bara verksamheten i näten och serviceverksamheten utan också möjligheterna att tillgodose användarnas integritetsskydd.

4 Beredningen av propositionen

4.1 Beredningsskeden och beredningsmaterial

Propositionen har beretts vid kommunikationsministeriet.

Efter det att lagen om dataskydd vid elektronisk kommunikation hade trätt i kraft 2004 tillsattes en uppföljningsgrupp för att bedöma konsekvenserna av lagen. Uppföljningsgruppen bestod av företrädare för AKAVA ry, Finlands näringsliv rf, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Fortum Abp, Konsumentverket, Centralhandelskammaren rf, kommunikationsministeriet, inrikesministeriet, Finlands Fackförbunds Centralorganisation FFC rf, Suomen Suoramarkkinointiliitto ry SSML, Tjänstemannacentralorganisationen FTFC rf, Upphovsrättens informations- och övervakningscentral rf, Dataombudsmannens byrå, arbetsministeriet och Kommunikationsverket.

Utifrån de behov som framkommit i uppföljningsgruppen bereddes vid kommunikationsministeriet på våren 2006 ett utkast till regeringsproposition bl.a. för att utvidga behandlingsrättigheterna för sammanslutningsabonnenterna. Ett utkast till regeringsproposition sändes till omfattande krets för utlåtande.

I utlåtandena framfördes över lag beröm över att lagen preciseras och görs tydligare. Det framfördes kritik över att det utkast som hade sänts för utlåtande inte innehöll någon bedömning av konsekvenserna eller någon internationell jämförelse. Bedömningen av konsekvenserna färdigställdes efter remissförfarandet. Utlåtandena om enskilda paragrafändringar varierade. Med anledning av

dem ändrades propositionen på flera punkter efter remissbehandlingen.

Efter remissbehandlingen erhölls de centrala ministeriernas ståndpunkter till ändringarna.

Kommunikationsministeriet bad också justitiekanslern ge sitt utlåtande om utkastet till regeringsproposition för att utreda om propositionen innehåller sådana problematiska punkter som hindrar att den överlämnas till riksdagen och dess grundlagsutskott för prövning. Justitiekanslern framförde som sin ståndpunkt att utkastet till proposition bör bedömas på ett mera övergripande sätt och i förekommande fall kompletteras i fråga om flera angelägenheter avseende de grundläggande fri- och rättigheterna.

Utgående från justitiekanslerns ståndpunkt omprövades propositionen.

Beredningen fortsatte i en arbetsgrupp tillsatt av kommunikationsministeriet den 3 oktober 2006 med uppgift utarbeta ett förslag till lag om ändring av 13 § i lagen om dataskydd vid elektronisk kommunikation. I förslaget gällde det att granska sammanslutningsabonnenternas behandling av identifieringsuppgifter i fråga om nät- och kommunikationstjänster i situationer med 1) olovligt brukande och 2) röjande av företagshemligheter. Till ordförande för arbetsgruppen utsågs överdirektören vid kommunikationsministeriet och till medlemmar företrädare för kommunikationsministeriet, justitieministeriet, inrikesministerier, arbetsministeriet, finansministeriet och arbetsmarknadscentralorganisationerna.

Som ett resultat av arbetsgruppens arbete kompletterades utkastets bestämmelser om behandling av identifieringsuppgifter med flera betydande preciseringar som alla preciserar och uppställer gränser för den behandling av identifieringsuppgifter som föreslås i 13 a a–13 j §.

De föreslagna bestämmelserna i 13 a–13 j §, detaljmotiveringen till dem och i tillämpliga delar allmänna motiveringen och motiveringen i fråga om lagstiftningsordningen bereddes i arbetsgruppen.

Propositionen fick också en helt ny internationell jämförelse.

4.2 Remissyttranden och fortsatt beredning

Ett utkast till regeringsproposition sändes för utlåtande till alla ministerier och flera hundra olika sammanslutningar. Dessutom lades utkastet ut på kommunikationsministeriets webbplats, för att också alla andra än de ovan nämnda instanserna skulle kunna yttra sig.

I flera av utlåtandena ansågs det vara bra att lagen preciseras. De flesta sammanslutningsabonnenter välkomnade regleringen av sammanslutningsabonnenternas rätt att behandla identifieringsuppgifter. Reformen av 20 § om åtgärder för att genomföra dataskyddet ansågs vara mycket behövlig.

Vissa remissinstanser tyckte däremot att den föreslagna rätten för sammanslutningsabonnenter att behandla identifieringsuppgifter är problematisk.

I utkastet till regeringsproposition ansågs 24 § om specificering av räkningar i huvudsak vara välkommen, men i synnerhet teleföretagen efterlyste en närmare utredning av bestämmelsen.

Till följd av de synpunkter som fördes fram i utlåtandena har propositionen preciserats på flera punkter och bestämmelsen om specificering av räkningar avskiljdes från den för att bli föremål för en separat beredning.

DETALJMOTIVERING

1 Lagförslag

1.1 Lagen om dataskydd vid elektronisk kommunikation

9 §. *Behandling av identifieringsuppgifter för att utföra och använda tjänster*. Det föreslås att 1 mom. ändras så att det tydligare än för närvarande framgår att omnämnandet av att sörja för dataskyddet avser uttryckligen de bestämmelser om dataskydd som finns längre fram i lagen.

Det bör beaktas att det i 8 § finns särskilda bestämmelser om en kommunikationsparts rättigheter och att både en fysisk person och en juridisk person kan vara part i kommuni-

kationen. Andra än kommunikationsparterna har enligt bestämmelsen rätt att behandla identifieringsuppgifter för att utföra och använda tjänster och för att sörja för dataskyddet. Här är det frågan om t.ex. att överföra telefonsamtal, e-post eller textmeddelanden från avsändaren till mottagaren eller att avlägsna skadliga program ur meddelandena när villkoren enligt 20 § uppfylls. Den som behandlar identifieringsuppgifterna agerar då i rollen som en utomstående i kommunikationen. När någon behandlar meddelanden och identifieringsuppgifter i egenskap av en utomstående får behandlingen äga rum endast med stöd av behandlingsrättigheterna enligt 3 kap.

Bestämmelserna i 5 kap. är bestämmelser om dataskydd enligt 9 § 1 mom. I 20 § bestäms uttömmande om de situationer där identifieringsuppgifter får behandlas för att sörja för dataskyddet och om de åtgärder som är berättigade i sådana situationer. Avsikten är att den föreslagna ändringen skall vara närmast informativ.

Det föreslås att förteckningen i 9 § 2 mom. över dem som får behandla identifieringsuppgifter kompletteras med fysiska personer som är anställda hos en juridisk person som är abonnent samt med fysiska personer som handlar för en sådan juridisk persons räkning. Tillägget behövs för att rätten enligt den nya 12 a § att behandla uppgifter för statistisk analys skall kunna utövas också av dem som behandlar t.ex. identifieringsuppgifter om mobiltelefonanslutningar för statistisk analys. Genom förslaget ändras också paragrafhänvisningarna i 2 mom. så att de gäller bestämmelserna om behandling i hela 3 kap. Avsikten med ändringen är inte att ändra rådande rättspraxis.

12 §. *Behandling för teknisk utveckling.* Förslaget innebär att 1 mom. ändras i första hand i skrivtekniskt hänseende. Samtidigt föreslås att 2 och 3 mom. skall byta plats. Avsikten är att det föreslagna 2 mom. skall skapa klarhet i en sammanslutningsabonnents rätt att behandla identifieringsuppgifter för teknisk utveckling. Enligt 3 mom. skall sammanslutningsabonnenten dessutom ha en liknande skyldighet att informera om behandlingen som den skyldighet som teleföretagen och de som tillhandahåller mervärdestjänster redan har med stöd av den gällande lagen.

I det gällande 1 mom. nämns enbart teknisk utveckling av tjänsterna, medan tjänsterna i de övriga bestämmelserna i kapitlet specificeras som nättjänster, kommunikationstjänster och mervärdestjänster. Genom förslaget ändras 1 mom. så att det motsvarar de övriga bestämmelserna i kapitlet.

Det föreslagna 2 mom. skapar klarhet i sammanslutningsabonnenternas rätt att behandla identifieringsuppgifter för teknisk utveckling. En sammanslutningsabonnent har därmed samma rättigheter att för teknisk utveckling behandla identifieringsuppgifter i sitt kommunikationsnät som de rättigheter som ett teleföretag och den som tillhandahåller mervärdestjänster har.

Det är viktigt att identifieringsuppgifter behandlas för teknisk utveckling, för att kommunikationsnäten och tjänsterna skall kunna utvecklas och nya tjänster skall kunna utformas för marknaden. Med teknisk utveckling avses t.ex. bättre teknisk kapacitet eller bättre användbarhet. Med egna tjänster som anslutits till kommunikationsnätet avses tjänster som sammanslutningsabonnenten själv utför för sina användare i sitt kommunikationsnät. Det handlar inte om t.ex. sådana informationssamhällstjänster som någon annan utför för sammanslutningsabonnenten, såsom nummerupplysning som den som tillhandahåller katalogtjänster erbjuder och som sammanslutningsabonnenten har beställt för sina användare av den nämnda leverantören.

Den föreslagna behandlingen av identifieringsuppgifter för teknisk utveckling skall omfattas även av de allmänna villkoren enligt 8 § 3 mom. och 9 §. Enligt 8 § 3 mom. är bl.a. behandling som avses i 12 § tillåten endast i den omfattning som behandlingens ändamål kräver. 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 skall meddelandena och identifieringsuppgifterna förstöras eller göras sådana att de inte kan förknippas med abonnenten eller användaren, om inte något annat bestäms i lag.

Enligt det föreslagna 9 § 2 mom. får identifieringsuppgifter behandlas endast av fysiska personer som är anställda hos ett teleföretag, hos den som tillhandahåller mervärdestjänster, hos en sammanslutningsabonnent och hos en juridisk person som är abonnent samt av fysiska personer som handlar för deras räkning och som har i uppdrag att behandla uppgifterna för att de mål som anges särskilt skall uppnås.

Enligt det gällande 2 mom. har teleföretagen och de som tillhandahåller mervärdestjänster varit skyldiga att informera abonnenterna eller användarna om sådan behandling av identifieringsuppgifter för teknisk utveckling som avses i 12 §. Det föreslås att 3 mom. kompletteras så att även en sammanslutningsabonnent i likhet med ett teleföretag och den som tillhandahåller mervärdestjänster åläggs att, innan behandlingen inleds, meddela vilka identifieringsuppgifter som behandlas och hur länge behandlingen räcker. Sammanslutningsabonnenten skall således meddela användaren vilka identifieringsuppgifter som behandlas och hur länge behandlingen kommer att pågå. Så som beskrivits i detaljmotiveringen till 12 § i propositionen med förslag till den gällande lagen kan teleföretagens och mervärdestjänsteleverantörernas anmälan ges t.ex. i anslutningsavtalet eller på teleföretagets eller mervärdestjänsteleverantörens hemsida. På samma sätt kan sammanslutningsabonnentens anmälan vara av engångskaraktär och gälla rent av en lång tidsperiod. Det kan ges en särskild anmälan om exceptionella och betydande åtgärder.

12 a §. *Behandling för statistisk analys*. Den föreslagna nya bestämmelsen ger teleföretagen, dem som tillhandahåller mervärdestjänster och sammanslutningsabonnenterna rätt att behandla identifieringsuppgifter för statistisk analys som genomförs med hjälp av automatisk databehandling. Likaså skall en juridisk person som är abonnent för statistisk analys få behandla identifieringsuppgifter om sin anslutning och sin terminalutrustning.

Enligt den gällande lagen har statistiska uppgifter fått samlas in utifrån s.k. anonyma uppgifter på basis av vilka abonnenten eller användaren inte har kunnat identifieras. Detta är möjligt också efter den föreslagna ändringen. Vem som helst kan upprätta statistik utifrån anonyma uppgifter eller i övrigt behandla anonyma uppgifter fritt. Den föreslagna bestämmelsen ger däremot rätt att för statistisk analys behandla även sådana uppgifter utifrån vilka abonnenten eller användaren kan identifieras. Fysiska personer skall givetvis inte kunna identifieras på basis av slutresultatet, dvs. den statistiska analysen. Enligt bestämmelsen skall den statistiska analysen utföras med hjälp av automatisk databehandling.

Syftet med statistisk analys är inte att upprätta egentlig statistik, utan att klarlägga någon annan omständighet, t.ex. hur en ändring i prissättningen påverkar omsättningen.

Det behövs rikligt med tekniskt utvecklingsarbete för utförandet och användningen av kommunikationstjänster. Bestämmelserna i 12 § möjliggör utvecklingsarbetet. I praktiken har det framkommit att tillbörligt utvecklingsarbete inrymmer drag som inte är enbart av teknisk natur men som är absolut nödvändiga med tanke på utvecklingen av verksamheten. Det kan handla om ekonomisk utveckling, såsom ekonomisk optimering av samtalsutgifter.

På grund av lagen eller tolkningarna av den har teleföretagen inte lämnat ut sådana identifieringsuppgifter till abonnenterna utifrån vilka ett företag eller en sammanslutning skulle ha kunnat t.ex. optimera telefonitrafiken mellan sina disponibla fasta telefoner och mobiltelefoner på ett så kostnadseffektivt sätt som möjligt. Detta har varit problematiskt i synnerhet i situationer där ett företag eller en sammanslutning på grund av sin storlek eller sin internationella verksamhet har beställt kommunikationstjänster från flera olika teleföretag. Exempelvis ett stort bolag som i egenskap av abonnent betalar sina användares telefonräkningar har ett betydande ekonomiskt intresse av att minimera kostnaderna. För organisationer som består av några tiotals personer är det redan en krävande uppgift att för upprättande av statistik gå igenom de specificerade räkningarna enligt 24 §. Å andra sidan kan teleföretagens rapporter variera betydligt från ett teleföretag till ett annat, vilket innebär att det i praktiken kan vara omöjligt att göra ett sammandrag av rapporterna. En abonnent har ett särskilt behov av att t.ex. i en situation med anbudsför-

farande få identifieringsuppgifter då den konkurrensutsätter teleföretag, för att abonnenten skall kunna beakta hur mycket av telefonitrafiken som består av t.ex. bolagets interna mobiltelefonitrafik.

Ett företags eller en annan sammanslutnings kommunikationsnät för samtal kan också bestå av köpta tjänster av ett eller flera teleföretag, ofta av telefonitjänster i det fasta nätet köpta av olika teleföretag samt av egna interna samtal i egna växelnät. Ett företag eller en annan sammanslutning kan ofta ha behov av att utveckla denna helhet även över landsgränserna, varvid antalet parter mångdubblas. För utvecklingen förmår ingen av de ovan nämnda parterna ensam producera alla rapporter som behövs, och uppgifterna i rapporterna kan inte kombineras på ett rationellt sätt. Genom statistisk analys ges aktörerna möjlighet att utveckla sina tjänster på ett tillbörligt sätt och sin verksamhet också i annat än enbart tekniskt hänseende.

Det kan antas att företagen eller sammanslutningarna i fortsättningen på ett samlat sätt även via sin egen terminalutrustning kan skaffa sådana uppgifter om samtalsriktningarna som är nödvändiga för att konkurrensutsätta teleföretag. Syftet med förslaget är att de som tillhandahåller tjänster, abonnenterna och sammanslutningsabonnenterna skall kunna förändra tjänsterna och verksamheterna så att de bättre svarar mot kraven i en verklighet som förändras, utan att skyddet av konfidentiella meddelanden äventyras.

Enligt den föreslagna bestämmelsen i 1 mom. skall ett teleföretag och den som tillhandahåller mervärdestjänster ges rätt att behandla identifieringsuppgifter som gäller nättjänsten, kommunikationstjänsten eller mervärdestjänsten, och skall en sammanslutningsabonnent ges rätt att för statistisk analys med hjälp av automatisk databehandling behandla identifieringsuppgifter som ingår i dess egna kommunikationsnät eller i en egen tjänst som anslutits till den. Eftersom t.ex. identifieringsuppgifter för mobiltelefonanslutningar inte är tillgängliga för sammanslutningsabonnenterna i deras egna kommunikationsnät föreslås det i 2 mom. att även juridiska personer som är abonnenter skall ha rätt att under de förutsättningar som anges i 1 mom. för statistisk analys behandla identifieringsuppgifter om sin anslutning eller terminalutrustning. Här handlar det om sådana anslutningar och sådan terminalutrustning som en juridisk person som är abonnent ställer till förfogande för sina användare.

Den föreslagna bestämmelsen innebär att ett teleföretag, för statistisk analys, får lämna ut identifieringsuppgifter om mobiltelefonanslutningar till en juridisk person som är abonnent. Ett företag eller någon annan sammanslutning kan av ett teleföretag få behövliga riktningsjämförelser av telefonsamtal och kan därmed konkurrensutsätta teleföretagens kommunikationstjänster.

Oavsett om det gäller ekonomisk eller någon annan utveckling av ett företags eller en annan sammanslutnings verksamhet eller ett teleföretags kundsegmentering, skall identifieringsuppgifterna i samtliga fall behandlas tekniskt i syfte att utföra statistisk analys. Efter det kan inte de fysiska personerna identifieras på basis av identifieringsuppgifterna.

Enligt den föreslagna bestämmelsen skall identifieringsuppgifter få behandlas endast för upprättande av statistik, inte alls för att kontrollera enstaka användares enstaka samtal. När identifieringsuppgifter behandlas i enlighet med paragrafen bör hänsyn också tas till begränsningarna i 8 § 3 mom., enligt vilka behandlingen av identifieringsuppgifter inte får begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt. Behandlingen av identifieringsuppgifter för statistikföring skall vara motiverad i sak.

Det bör också noteras att i vissa situationer kan ett företag, som också verkar som teleföretag, handla för en sammanslutningsabonnents räkning. Det är då frågan om att en underleverantör producerar information för sammanslutningsabonnenten. Så förhåller det sig t.ex. när ett företag ansvarar för sammanslutningsabonnentens system.

Behandlingen av identifieringsuppgifter för statistiska ändamål begränsas också av de förutsättningar som nämns i paragrafen. Enligt det föreslagna 1 mom. får uppgifterna behandlas, om den statistiska analysen inte annars kan utföras utan oskäligt besvär och om en fysisk person, dvs. enskilda beställare eller användare inte kan identifieras utifrån

analysen. Det bör alltid i varje situation noga övervägas om behovet av statistik kan tillgodoses med andra tillgängliga medel, t.ex. genom användning av uppgifter som redan gjorts anonyma. Det skall inte heller gå att identifiera enskilda abonnenter eller användare i den statistiska analysen. Det går därmed inte att producera statistisk analys, om det handlar om t.ex. en enda abonnent och dennes identifieringsuppgifter eller en så liten grupp användare att analysen inte kan utföras utan att fysiska personer kan identifieras.

13 §. *Rätten för teleföretag och den som tillhandahåller mervärdestjänster att behandla uppgifter i fall av missbruk.* I paragrafen föreslås bestämmelser om behandlingsrättigheterna för teleföretagen och dem som tillhandahåller mervärdestjänster.

Det föreslagna 1 mom. innehåller inte längre någon begränsning i fråga om enskilda fall av missbruk. För att den föreslagna behandlingsrätten skall kunna utövas förutsätts inte misstanke om ett visst enskilt missbruk. Behandlingen kan på ett mera omfattande sätt än tidigare gälla samtliga fall som nämns i bestämmelsen. Det handlar dock inte om att övervaka kommunikationen i den bemärkelsen att det är tillåtet att följa kommunikationen för enskilda parter i kommunikationen, utan om att upptäcka avvikelser som tyder på missbruk.

Enligt det föreslagna 2 mom. skall Kommunikationsverket, som övervakar efterlevnaden av lagen, ha rätt att meddela tekniska föreskrifter. Kommunikationsverket skall meddela föreskrifter för teleföretagen och dem som tillhandahåller mervärdestjänster. Föreskrifterna är nödvändiga för att möjliggöra den behövliga smidighet som krävs när den tekniska miljön förändras i snabb takt och för att reglera behövliga tekniska detaljer. Kommunikationsverkets befogenhet att meddela föreskrifter gäller inte informationssamhällstjänster som tillhandahålls av statsförvaltningen.

13 a §. *Sammanslutningsabonnenters behandlingsrätt i fall av missbruk.* Enligt det föreslagna 1 mom. skall en sammanslutningsabonnent ha rätt att behandla identifieringsuppgifter för att utreda olovligt brukande av avgiftsbelagda informationssamhällstjänster eller kommunikationsnät, brukande av kommunikationstjänster som strider mot anvisningarna eller för att utreda röjande av företagshemligheter enligt vad som bestäms i 13 b–13 j §.

Den föreslagna rätten att behandla identifieringsuppgifter har samband med att skydda användningen av sammanslutningsabonnenternas kommunikationsnät och kommunikationstjänster med att utreda obehörigt röjande av företagshemligheter. Med stöd av den föreslagna bestämmelsen får sammanslutningsabonnenterna behandla identifieringsuppgifter, när det är fråga om olovligt brukande som strider mot anvisningarna för användningen av avgiftsbelagda informationssamhällstjänster, kommunikationsnät eller kommunikationstjänster samt när det föreligger misstanke för obehörigt röjande av företagshemligheter.

Enligt 8 § 3 mom. i lagen om dataskydd vid elektronisk kommunikation är behandling av identifieringsuppgifter tillåten endast i den omfattning som behandlingens ändamål kräver och den skall genomföras utan att äventyra skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt. 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.

Av 8 § 3 mom. följer att missbruk i första hand bör utredas med hjälp av andra identifieringsuppgifter än sådana som gäller konfidentiell kommunikation. Om det är nödvändigt att behandla identifieringsuppgifter för att reda ut missbruk skall de identifieringsuppgifter som det blir aktuellt att behandla alltid avgränsas från fall till fall på basis av andra tillgängliga uppgifter. På grund av nödvändighetskravet kan även i dessa fall endast behandlas identifieringsuppgifter för meddelanden som användaren sänt och inte för meddelanden som användaren tagit emot.

På grund av de allmänna och särskilda villkor för rätten att behandla identifieringsuppgifter som ingår i den föreslagna paragrafen och nödvändighetsvillkoret i 8 § 3 mom. kan en sammanslutningsabonnent inte följa upp identifieringsuppgifterna för vanliga meddelanden. Till exempel en sammanslutnings-

abonnent i arbetsgivarställning kan inte följa upp användningen av kommunikationsnät eller kommunikationstjänster för arbetstidsuppföljning eller för att ta reda på om användaren har varit i kontakt med personalföreträdaren, arbetarskyddsmyndigheten eller företagshälsovården. Tidsmässigt är det möjligt att behandla endast de identifieringsuppgifter som är nödvändiga för att reda ut det aktuella fallet och bestämmelsen berättigar inte till att behandla uppgifterna i större omfattning än så.

Sammanslutningsabonnentens kommunikationstjänster och informationssamhällstjänster avses enligt den föreslagna bestämmelsen är tjänster som anknutits till sammanslutningsabonnentens kommunikationsnät samt sådana tjänster som används via sammanslutningsabonnentens kommunikationsnät, men som har karaktär av informationssamhällstjänster och i fråga om vilka sammanslutningsabonnenten betalar för användningen.

Enligt 2 § i lagen om tillhandahållande av informationssamhällets tjänster (458/2002) avses med informationssamhällets tjänster sådana tjänster som utförs på distans utan att parterna är samtidigt närvarande, på elektronisk väg, genom överföring av information på individuell begäran av en tjänstemottagare och vanligtvis mot vederlag.

Ett exempel på olovligt brukande avgiftsbelagda informationssamhällstjänster kan vara att en tjänst som prissatts enligt personalens storlek obehörigen delas ut till utomstående. I så fall är företaget skyldigt att betala för den användning som överstiger den avtalade nyttjanderätten.

Olovligt brukande av kommunikationsnätet eller brukande som strider mot anvisningarna för användningen av kommunikationstjänsten är sådan verksamhet som sammanslutningsabonnenten har bestämt i de anvisningar som avses i 13 b § 3 mom.

Vid utredning av obehörigt röjande av företagshemligheter står informationsadministrativa metoder till förfogande, såsom kontroll av logguppgifter om användarna, kontroll av uppgifterna om dem som loggar in i system som begränsar åtkomst samt uppgifter som samlats in i samband med tekniskt underhåll av systemen. Av dessa uppgifter framgår vem som har infört vilka uppgifter, i vilken form, när och till vilket medium, såsom hårddisk eller ett flyttbart medium. Flyttbara är t.ex. minnespinnar och cd-skivor. Även uppgifter om annan behandling av materialet, såsom uppgifter om utskrifter, kan sparas. I lagen om dataskydd vid elektronisk kommunikation uppställs inte några begränsningar för behandlingen av sådana uppgifter. Med hjälp av uppgifterna är det å andra sidan bara i undantagsfall möjligt att utreda röjanden av företagshemligheter i deras helhet.

Arbetsgivaren kan skydda företagshemligheter också genom andra åtgärder för att trygga informationssäkerheten. Som exempel kan nämnas att arbetsgivarna också kan ingå avtal om sekretess med arbetstagarna som en metod för att skydda företagshemligheter. Enligt lagen om säkerhetsutredningar (177/2002) får en arbetsgivare skaffa en utredning om arbetstagarnas tillförlitlighet, om det gäller att skydda anmärkningsvärt värdefulla affärs- eller yrkeshemligheter eller andra med dem jämförbara enskilda intressen som är av synnerligen stor betydelse.

Begreppet företagshemlighet enligt paragrafen motsvarar definitionen av företagshemlighet enligt 30 kap. 11 § i strafflagen. Enligt definitionen i 30 kap. 11 § i strafflagen av företagshemlighet avses med företagshemlighet en affärs- eller yrkeshemlighet eller någon motsvarande information om näringsverksamhet som en näringsidkare håller hemlig och vars röjande är ägnat att medföra ekonomisk skada för honom eller någon annan näringsidkare som har anförtrott honom informationen.

Företagshemlighet enligt definitionen i strafflagen är därmed i någon mån mera omfattande än tillämpningsområdet för den sekretessbestämmelse som finns i 24 § 1 mom. 20 punkten i lagen om offentlighet i myndigheternas verksamhet (621/1999) och som utfärdats för att skydda intressen i samband med näringsverksamhet och inte omfattar t.ex. uppgifter om näringsidkarens skyldigheter och fullgörandet av dessa. Begreppet täcker också sådana uppgifter om teknologiskt och annat utvecklingsarbete som ännu inte gäller t.ex. produkter som skall patentskyddas. Begreppet företagshemlighet omfattar därmed också sådana uppgifter som är

sekretessbelagda enligt 24 § 1 mom. 21 punkten i lagen om offentlighet i myndigheternas verksamhet.

I samband med beredningen av propositionen har begreppet företagshemlighet ansetts vara ett adekvat begrepp, eftersom begreppet är nära förknippat med näringsidkarens egen sekretessvilja och eftersom bestämmelserna verkar i förhållanden mellan enskilda parter.

Behandling av identifieringsuppgifter i strid med behandlingsreglerna i 13 a–13 j § och 8 § kan uppfylla brottsrekvisitet för kränkning av kommunikationshemlighet och grov kränkning av kommunikationshemlighet enligt 38 kap. 3 och 4 § i strafflagen. Försummelse av de förpliktelser som gäller tryggandet av tillbörlig behandling av identifieringsuppgifter som avses i 13 b–13 c § avses fylla brottsrekvisitet för i 42 § 2 mom. 5 punkten avsedd dataskyddsförseelse vid elektronisk kommunikation.

Behandling av identifieringsuppgifter i strid med behandlingsreglerna i 13 a–13 j § och 8 § kan uppfylla brottsrekvisitet för kränkning av kommunikationshemlighet och grov kränkning av kommunikationshemlighet enligt 38 kap. 3 och 4 § i strafflagen. Försummelse av de föregripande förpliktelser som gäller tryggandet av tillbörlig behandling av identifieringsuppgifter som avses i 13 b–13 c § skulle uppfylla brottsrekvisitet för i 42 § 2 mom. 5 punkten avsedd dataskyddsförseelse vid elektronisk kommunikation. Genom den föreslagna nya 9 punkten i 42 § 2 mom. blir det straffbart som dataskyddsförseelse vid elektronisk kommunikation att försumma de förpliktelser i efterhand som garanterar att behandlingen av identifieringsuppgifter är lagenlig.

Enligt det föreslagna 2 mom. är det olovligt brukande av kommunikationsnätet eller brukande av kommunikationstjänsten i strid med anvisningarna för användningen till exempel om någon i sammanslutningsabonnentens kommunikationsnät installerar anordningar, program eller tjänster i strid med de anvisningar som getts för användningen av nätet eller annars på jämförbart sätt använder kommunikationsnätet eller kommunikationstjänsterna på ett sätt som strider mot de anvisningar om användningen som avses i 13 b §.

I det föreslagna 3 mom. avgränsas identifieringsuppgifter för telefonitjänster i det fasta och mobila telefonnätet utanför bestämmelserna om missbruk. I så fall får sammanslutningsabonnenter inte behandla uppgifter, som gäller telefonsamtal, textmeddelanden eller liknande meddelanden. Enligt definitionen i lagen avses med meddelande samtal, elektronisk post, textmeddelande, talmeddelande och annat motsvarande meddelande mellan parterna eller till en mottagarkrets som inte är utvald på förhand (RP 125/2003 rd, s. 48–49). Om abonnentens rätt att få en specificerad räkning av samtalstjänsten har föreskrivits särskilt.

13 b §. Sammanslutningsabonnenters omsorgsplikt i fall av missbruk. I det föreslagna 1 mom. tas in bestämmelser om de förhandsvillkor, inom vars gränser sammanslutningsabonnenten kan reda ut olovligt brukande av avgiftsbelagda informationssamhällstjänster eller kommunikationsnät och brukande av kommunikationstjänster som strider mot anvisningarna.

Enligt den föreslagna regleringen är den primära metoden för att trygga en tillbörlig användning av kommunikationsnätet och kommunikationstjänsterna att sörja för dataskyddet, att meddela anvisningar för dem som använder näten och tjänsterna och att automatiskt kontrollera att anvisningarna följs.

I det föreslagna 1 mom. bestäms om sammanslutningsabonnents omsorgsplikt innan behandlingen av identifieringsuppgifter inleds i avsikt att förebygga olovligt brukande av avgiftsbelagda informationssamhällstjänster eller kommunikationsnät eller brukande av kommunikationstjänster som strider mot anvisningarna. Enligt 1 punkten är ett villkor för behandling av identifieringsuppgifter att sammanslutningsabonnenten har begränsat tillgången till sitt kommunikationsnät och sin kommunikationstjänst och brukandet av dem och har vidtagit andra åtgärder för att skydda sitt kommunikationsnät och sin kommunikationstjänst med lämpliga datasäkerhetsåtgärder.

Sammanslutningsabonnenten skall på förhand på tillbörligt sätt och med till buds stående metoder ha vidtagit åtgärder för att förhindra att kommunikationsnätet eller de

tjänster som anslutits till det används av utomstående eller sådana anställda hos sammanslutningsabonnenten, som inte har fått dem till sitt förfogande eller för att förhindra att kommunikationstjänster används i strid med anvisningarna. Sammanslutningsabonnenten skall likaså se till att nivån på informationssäkerheten är tillräcklig. Om nätet eller tjänsterna trots tillbörlig användarhantering och andra informationssäkerhetsåtgärder används olovligen, skall sammanslutningsabonnenten ha rätt att behandla identifieringsuppgifterna i utredningssyfte.

Enligt den föreslagna 1 mom. 2 punkten skall sammanslutningsabonnenten bestämma hurdana meddelanden som får förmedlas och hämtas via sammanslutningsabonnentens kommunikationsnät samt hur sammanslutningsabonnentens kommunikationsnät och kommunikationstjänster i övrigt får användas och till hurdana destinationsadresser kommunikation inte får utövas. För att det skall vara tillåtet att behandla identifieringsuppgifter på det sätt som föreslås, krävs att den som använder kommunikationsnätet eller kommunikationstjänsten känner till hur sammanslutningsabonnentens nät får användas. Genom att följa villkoren kan den som använder nätet undvika att sammanslutningsabonnenten får ta del av de identifieringsuppgifterna om hans eller hennes kommunikation.

I det föreslagna 2 mom. tas in bestämmelser om de förhandsåtgärder som sammanslutningsabonnenten skall vidta innan behandlingen av identifieringsuppgifter för att förebygga röjande av företagshemligheter får inleds.

Enligt den föreslagna regleringen är de primära metoderna för att trygga sekretessen av företagshemligheter att sörja för informationssäkerheten, att meddela anvisningar för dem som använder näten och tjänsterna och att automatiskt kontrollera att anvisningarna följs.

I den föreslagna 2 mom. 1 punkten förutsätts att företagshemligheter faktiskt skyddas från alla som med tanke på behandlingen av företagshemligheten är utomstående. Innan sammanslutningsabonnenten inleder behandlingen av identifieringsuppgifter skall sammanslutningsabonnenten ha begränsat tillträdet till centrala företagshemligheter och vidtagit andra åtgärder för att skydda uppgifterna med lämpliga informationssäkerhetsåtgärder. I praktiken betyder detta att endast användare som sköter vissa uppgifter i organisationen har tillgång till företagshemligheter. Tillgången kan i praktiken begränsas med hjälp av informationsadministrativa åtgärder, såsom användarnamn och lösenord eller genom annan administrering av användarrättigheter.

Enligt den föreslagna 2 mom. 2 punkten skall sammanslutningsabonnenten bestämma på vilket sätt företagshemligheter får överföras, lämnas ut eller på annat sätt behandlas och till hurdana destinationsadresser de personer som har rätt att behandla företagshemligheter inte får skicka meddelanden. De som kommer i kontakt med uppgifter som skyddas i egenskap av företagshemligheter bör uppfatta uppgifterna som konfidentiella, vilket bör framgå av ett begränsat tillträde samt särskilda informationssäkerhetsåtgärder och behandlingsregler i fråga om uppgifterna. Om sammanslutningsabonnenten vill helt och hållet förbjuda kommunikationen till en viss typ av destinationsadresser, skall också detta fastställas i anvisningarna.

Ett krav enligt det föreslagna 3 mom. är att sammanslutningsabonnenten har gett skriftliga anvisningar där det slås fast hur sammanslutningsabonnentens kommunikationsnät och tjänster får användas. Det är klart att anvisningarna till användarna skall innehålla tillräckligt noggrann information om de begränsningar som införts i fråga om användningen av kommunikationsnätet. Om sammanslutningsabonnenten vill begränsa eller helt och hållet förhindra kommunikationen till en viss typ av destinationsadresser, skall också detta fastställas i anvisningarna. Destinationsadresserna kan fastställas på en förhållandevis allmän nivå. Av definitionen skall det dock tydligt framgå vad som anses vara missbruk.

13 c §. *Sammanslutningsabonnenters planerings- och samarbetsplikt i fall av missbruk.* Enligt 13 c § 1 mom. i förslaget är ett villkor för sådan behandling av identifieringsuppgifter som avses i 13 a § 1 mom. att sammanslutningsabonnenten antingen har utsett de personer, till vilkas uppgifter det hör

att behandla identifieringsuppgifter eller bestämt dessa uppgifter. Identifieringsuppgifter får behandlas endast av personer som svarar för driften av och informationssäkerheten i sammanslutningsabonnentens kommunikationsnät och kommunikationstjänst och för säkerheten. Med tanke på användarnas rättsskydd är det viktigt att de vet, vilka personer som på sammanslutningsabonnentens vägnar får behandla identifieringsuppgifter. Sammanslutningsabonnenten bör fastställa åtminstone de uppgifter eller t.ex. de verksamhetsenheter, i vilka identifieringsuppgifter får behandlas i de situationer som avses i 13 a–13 j §. Om sammanslutningsabonnenten skaffar tjänsten av en utomstående leverantör, räcker det med att dessa uppgifter eller funktioner has definierats för tjänsteleverantörens del.

Om en person som är anställd hos ett utomstående företag deltar i behandlingen av identifieringsuppgifter bör sammanslutningsabonnenten innan några åtgärder vidtas försäkra sig om att de villkor som ställs på behandlingen i 13 a–13 d § fylls.

I det föreslagna 2 mom. föreskrivs om de skyldigheter som gäller för en sammanslutningsabonnent i arbetsgivarställning och som skall följas utöver de skyldigheter som avses i 1 mom.

I 4 § i lagen om integritetsskydd i arbetslivet bestäms om att insamling av personuppgifter när någon anställs och under ett arbetsavtalsförhållande omfattas av samarbetsförfaranden enligt samarbetslagstiftningen och bestämmelser om behandlingen av ärenden finns i bl.a. lagen om samarbete inom företag (334/2007), lagen om samarbete inom statens ämbetsverk och inrättningar (651/1988) samt lagen om samarbete mellan kommunala arbetsgivare och arbetstagare (449/2007).

Arbetsgivaren skall också följa bestämmelserna i 21 § i lagen om integritetsskydd i arbetslivet. Enligt 21 § omfattas syftet med övervakning av arbetstagarna med hjälp av tekniska metoder, ibruktagandet av dem och de metoder som används samt användningen av elektronisk post och andra datanät av samarbetsförfarandena enligt den ovan nämnda samarbetslagstiftningen.

Efter samarbetsförfarandet eller förfarandet med hörande skall arbetsgivaren definiera ändamålet med och metoderna för övervakningen med tekniska metoder av arbetstagarna samt informera arbetstagarna om syftet med, ibruktagandet av och metoderna för övervakningen samt om användningen av elektronisk post och datanät. Dessutom bör det beaktas att även andra bestämmelser i den ovan nämnda speciallagen tillämpas på sammanslutningsabonnenter i arbetsgivarställning, t.ex. 6 kap. där det bestäms om hämtning och öppnande av e-postmeddelanden som hör till arbetsgivaren.

På grund av författningarnas inbördes förhållande är det nödvändigt att utfärda bestämmelser om saken också i lagen om dataskydd vid elektronisk kommunikation. Behovet av reglering accentueras dessutom av att den behandling av identifieringsuppgifter som avses i 13 a och 13 b § inte alltid är sådan behandling av personuppgifter som avses i personuppgiftslagen.

Enligt 2 mom. 1 punkten skall arbetsgivaren för det första i ett samarbetsförfarande enligt 4 kap. i lagen om samarbete inom företag, lagen om samarbete inom statens ämbetsverk och inrättningar och lagen om samarbete mellan kommunala arbetsgivare och arbetstagare behandla grunderna och praxisen för de i 13 a–13 j § avsedda förfaranden som skall tillämpas vid behandlingen av identifieringsuppgifter. Det innebär att innan arbetsgivaren tar i bruk de förfaranden som avses i 13 a–13 j § eller ändringar av dem skall grunderna, målen, syftet och verkningarna diskuteras med företrädarna för de arbetstagare som berörs.

Samarbetsförfarandet avses omfatta centrala frågor i anslutning till olovligt brukande av kommunikationsnätet eller brukande av kommunikationstjänsten som strider mot anvisningarna. Som exempel kan nämnas anvisningar för användningen av kommunikationsnätet, funktionsprinciperna för automatisk sökning och på vilka grunder olovligt brukande i strid med anvisningarna anses orsaka betydande men eller skada för arbetsgivaren. En sammanslutningsabonnent skall på motsvarande sätt också redogöra för de omständigheter och grunder som möjliggör automatisk eller manuell behandling för att utreda röjande av företagshemligheter.

I ett samarbetsförfarande skall för det andra behandlas de arbetsuppgifter enligt det före-

slagna 1 mom. där identifieringsuppgifter kan behandlas.

Utöver det skall arbetsgivaren så som bestäms i 21 § i lagen om integritetsskydd i arbetslivet informera arbetstagarna eller deras företrädare om sina beslut i sådant som behandlats.

Enligt 3 mom. skall arbetsgivaren i andra företag och offentligrättsliga sammanslutningar än sådana som omfattas av samarbetslagstiftningen före beslutsfattandet bereda arbetstagarna eller deras representanter tillfälle att bli hörda i de angelägenheter som nämns ovan.

I 4 mom. föreslås bli bestämt om den informationsskyldighet som gäller vid utnyttjande av rätten till behandling av identifieringsuppgifter för sådana sammanslutningsabonnenter som inte är i arbetsgivarställning. Informationsskyldigheten skall följas utöver de skyldigheter som avses i 13 b och 13 c § 1 mom. I praktiken gäller bestämmelsen närmast läroanstalter, bibliotek och andra organisationer, som tillhandahåller kommunikationstjänster för sina användare.

Enligt den föreslagna bestämmelsen skall sammanslutningsabonnenten informera användarna om det förfarande enligt 13 a–13 j § som tillämpas på behandlingen av identifieringsuppgifter och de arbetsuppgifter enligt 13 c § 1 mom. som utförs av personer som har rätt att behandla identifieringsuppgifter. Underrättelsen är av engångskaraktär och den kan göras antingen i samband med att användaren tilldelas rätt att använda ett kommunikationsnät eller en kommunikationstjänst eller om det inte är möjligt, på något annat lämpligt sätt.

13 d §. *Villkor för sammanslutningsabonnenters behandlingsrätt i fall av missbruk.* I 13 d § bestäms om de förfaranden som tillämpas på behandlingen av identifieringsuppgifter och villkoren för förfarandet.

Enligt 1 mom. får sammanslutningsabonnenten behandla identifieringsuppgifter med hjälp av en automatisk sökfunktion som kan basera sig på meddelandenas storlek, deras sammanlagda storlek, meddelandenas typ, antal eller uppkopplingssätt eller de destinationsadresser till vilka meddelandena skickas.

Innan behandlingen av identifieringsuppgifter inleds skall sammanslutningsabonnenten se till att alla de villkor för behandlingen som avses i 13 a–13 j § fylls.

Med automatisk sökfunktion avses en funktion där sökningen inte från fall till fall inriktas med mänsklig arbetskraft utan där en sökmotor automatiskt söker avvikelser i kommunikationsnätet enligt vissa på förhand fastställda kriterier. Det är frågan om automatisk sökning när kommunikationstrafiken analyseras i form av massbehandling t.ex. på basis av volym, typ eller typ av destinationsadress men inte på basis av uppkopplingsadressen för användaren av kommunikationsnätet eller kommunikationstjänsten. Vid automatisk sökning får en fysisk person inte ta del av identifieringsuppgifterna för en enskild användares meddelanden.

Olovligt brukande av kommunikationsnät och brukande av kommunikationstjänster som strider mot anvisningarna kan i praktiken utredas med hjälp av bl.a. automatiska mätare för kapacitetsanvändningen eller med program som förhindrar intrång, t.ex. brandväggar. Samma tekniska tillämpningar används också för att automatiskt övervaka kapaciteten samt för att automatiskt upptäcka fel och störningar. Genom samma tillämpningar kan sammanslutningsabonnenterna också fastställa gränser för användningen av sina kommunikationsnät och kommunikationstjänster: de kan t.ex. förhindra trafiken från sitt nät till vissa uppkopplingsadresser eller helt och hållet förhindra en viss typ av trafik.

Vid automatisk sökning identifieras olovligt brukande som strider mot anvisningarna eller röjande av företagshemligheter på basis av meddelandenas storlek, typ och antal, uppkopplingssätt eller meddelandenas destinationsadress. Med meddelandets typ avses t.ex. i vilken form ett meddelande, en del av det eller dess bilagor har sparats, t.ex. .doc eller .mp3. Med uppkopplingssätt avses t.ex. det protokoll enligt vilket meddelandet förmedlas i kommunikationsnätet, t.ex. http eller tcp. Med destinationsadress avses sådana tjänster eller andra adresser till vilka sammanslutningsabonnenten har förbjudit, begränsat eller helt och hållet förhindrat trafik.

Syftet med de ovan nämnda definieringarna av automatisk sökning är att övervakningen av identifieringsuppgifter inte skall inriktas på sedvanliga e-postmeddelanden och att begränsningarna även i övrigt skall vara sakliga och motiverade för att säkerställa att nätet används på behörigt sätt.

Enligt det föreslagna 13 d § 2 mom. skall en sammanslutningsabonnent under vissa förutsättningar få ta identifieringsuppgifter också till manuell behandling.

Med manuell behandling avses behandling av uppgifter i elektronisk form när behandlingen med mänsklig arbetskraft från fall till fall inriktas på identifieringsuppgifter som gäller en viss användares uppkopplingsadress eller uppkopplingsadresserna för en viss grupp av användare.

Det är skäl att observera att de föreslagna 13 d § 3 och 4 mom. begränsar rätten till manuell behandling.

Enligt 2 mom. 1 punkten skall uppgifter få tas till manuell behandling om en avvikelse i de faktorer som avses i 1 mom. har uppdagats med hjälp av en automatisk sökfunktion Med avvikelse avses sådana meddelanden i fråga om vilka en observation har registrerats i den automatiska sökfunktionen på basis av meddelandenas storlek, typ, antal, uppkopplingssätt eller destinationsadress.

Enligt den föreslagna 2 mom. 2 punkten skall identifieringsuppgifter få tas till manuell behandling, om kostnaderna för användningen av en avgiftsbelagd informationssamhällstjänst har stigit ovanligt mycket.

Enligt 2 mom. 3 punkten är manuell behandling tillåten, om det upptäckts att en anordning, ett program eller en tjänst obehörigen har installerats i kommunikationsnätet.

Enligt 2 mom. 4 punkten är det tillåtet att behandla uppgifterna manuellt, om en företagshemlighet har offentliggjorts eller utnyttjats olovligen.

Enligt 2 mom. 5 punkten är manuell behandling i ett enskilt fall tillåten, om sammanslutningsabonnenten utifrån en annan med 1–4 punkten jämförbar allmänt konstaterbar omständighet har anledning att misstänka att avgiftsbelagda informationssamhällstjänster eller kommunikationsnätet används olovligen eller att kommunikationstjänsten används i strid med anvisningarna eller om en företagshemlighet olovligen har röjts för en utomstående.

Med obehörigt röjande av företagshemligheter för en utomstående avses det att den som använder kommunikationsnät eller kommunikationstjänst sänder eller olovligen ger en utomstående tillgång till företagshemligheter via sammanslutningsabonnentens kommunikationsnät eller genom utnyttjande av sammanslutningsabonnentens kommunikationstjänst.

Det finns grundad anledning att misstänka olovligt brukande t.ex. när det i samband med informationsadministrativt underhåll konstateras att en anordning eller tjänst uppenbarligen obehörigen har installerats i kommunikationsnätet. Det att anordningen eller tjänsten har installerats obehörigen kan framgå av t.ex. en avvikande benämning eller funktion. Det kan då utredas hurdan trafik som har ägt rum från anordningen eller tjänsten.

Det finns grundad anledning att misstänka olovligt brukande eller brukande i strid med anvisningarna också när det konstateras att det från en sammanslutningsabonnents uppkopplingsadress utgår trafik av främmande typ i förhållande till attributen för kommunikationstjänsterna eller på basis av andra motsvarande omständigheter. Ett exempel är att det i en sammanslutningsabonnents nät upptäcks att det i nätet olovligen har upprättats en offentlig, nätbaserad bostadsförmedlingstjänst eller någon annan tjänst som inte ingår i sammanslutningsabonnentens verksamhet.

Grundad anledning att misstänka obehörigt röjande av företagshemligheter kan finnas t.ex. när företagshemligheter har offentliggjorts eller när någon utifrån uppgifter som gäller ett hemligt utvecklingsarbete tillsammans med en part som utövar utvecklingsarbete har utformat en likadan anordning eller tjänst.

I 3 mom. bestäms om villkoren för såväl automatisk som manuell behandling av identifieringsuppgifter. Enligt momentet krävs det för att sammanslutningsabonnenten skall ha rätt att behandla identifieringsuppgifter med hjälp av en automatisk sökfunktion eller manuellt att incidenten eller gärningen sannolikt orsakar betydande men eller skada för sammanslutningsabonnenten eller att det

misstänkta röjandet av företagshemlighet gäller företagshemligheter som är centrala för sammanslutningsabonnentens egen eller dess samarbetsparters näringsverksamhet eller resultaten av tekniskt eller annat utvecklingsarbete som sannolikt är viktiga med tanke på att starta eller utöva näringsverksamhet.

Betydande men enligt bestämmelsen kan vara bl.a. ökade kostnader eller sådan ökad användning av dataöverföringskapaciteten, ett sådant hot mot informationssäkerheten eller något annat motsvarande som äventyrar, försvårar eller fördröjer möjligheterna att använda kommunikationsnätet eller tjänsterna för det planerade ändamålet.

Det skall vara möjligt att behandla identifieringsuppgifter om det är fråga om företagshemligheter som är av central betydelse för näringsverksamheten eller resultaten av tekniskt eller annat utvecklingsarbete. Bland annat sådana uppgifter som ger företaget konkurrensfördelar och som inte kan klarläggas utifrån offentliga källor är centrala företagshemligheter på ett sådant sätt som avses i bestämmelsen. Som centrala uppgifter kan betraktas uppgifter om vilka näringsidkaren har meddelat särskilda anvisningar för behandlingen och skyddandet och utformat skyddsförfaranden så som förutsätts i 13 b §.

Resultat av utvecklingsarbete nämns särskilt i bestämmelsen, eftersom det inte alltid är klart i vilket skede de bör anses vara centrala för affärsverksamheten. Som resultat av utvecklingsarbete kan också betraktas sådana etappresultat av forsknings- och utvecklingsprojekt som i sig är betydelsefulla samt resultat som visar att det inte lönar sig att fortsätta utvecklingsarbetet. Det föreslås att rätten att behandla identifieringsuppgifter utsträcks till situationer där det finns misstankar om obehörigt röjande av resultaten av utvecklingsarbete. Uppgifterna bör vara viktiga med tanke på att utöva eller påbörja näringsverksamhet. Obehörigt röjande av resultaten av utvecklingsarbete kan vara synnerligen skadligt för deras ägare och förhindra bl.a. erhållande av immaterialrättsligt skydd.

Obehörigt röjande av resultaten av utvecklingsarbete kan vara synnerligen skadligt för deras ägare och förhindra bl.a. erhållande av immaterialrättsligt skydd.

I det föreslagna 4 mom. bestäms om särskilda förutsättningar för behandlingen av identifieringsuppgifter. Villkor för manuell behandling är dessutom att uppgifterna är nödvändiga för att reda ut missbruket och de som svarar för det och för att göra slut på olovligt brukande eller brukande i strid mot anvisningarna.

Nödvändighetsvillkoret i 8 § 3 mom. i lagen om dataskydd vi elektronisk kommunikation ställer gränser för behandlingen av identifieringsuppgifter både i fråga om sakinnehåll och tidpunkt.

På grund av de allmänna och särskilda villkor för rätten att behandla identifieringsuppgifter som ingår i den föreslagna paragrafen och nödvändighetsvillkoret i 8 § 3 mom. kan en sammanslutningsabonnent inte följa upp identifieringsuppgifterna för vanliga meddelanden. Till exempel en sammanslutningsabonnent i arbetsgivarställning kan inte följa upp användningen av kommunikationsnät eller kommunikationstjänster för arbetstidsuppföljning eller för att ta reda på om användaren har varit i kontakt med personalföreträdaren, arbetarskyddsmyndigheten eller företagshälsovården. Tidsmässigt är det möjligt att behandla endast de identifieringsuppgifter som är nödvändiga för att reda ut det aktuella fallet och bestämmelsen berättigar inte till att behandla uppgifterna i större omfattning än så.

Enligt 8 § 3 mom. i lagen om dataskydd vid elektronisk kommunikation är behandling av identifieringsuppgifter tillåten endast i den omfattning som behandlingens ändamål kräver och den skall genomföras utan att äventyra skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt. 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.

13 e §. *Särskilda begränsningar av behandlingsrätten i fall av missbruk.* Enligt det föreslagna 13 e § 1 mom. får automatiska sökning inte riktas så att den används i avsikt att ta reda på uppgifter som omfattas av källskyddet. Identifieringsuppgifterna får inte heller tas till manuell behandling i avsikt att ta reda på dylika omständigheter.

Utan hinder av de allmänna behandlingsreglerna i lagen och avgränsningarna av behandlingsrätten har det under lagberedningen ansets vara nödvändigt att genom en särskild bestämmelse precisera det faktum att den föreslagna behandlingsrätten inte får användas får att ta reda på omständigheter som omfattas av källskyddet.

I det föreslagna 2 mom. skall behandlingsrätt för att utreda röjande av företagshemligheter begränsas till att gälla endast för sammanslutningsabonnenter i arbetsgivarställning. Endast sådana personers identifieringsuppgifter får behandlas som sammanslutningsabonnenten har gett eller som på något annat av sammanslutningsabonnenten godkänt sätt har fått tillgång till företagshemligheter. Rätt till tillgång kan ges t.ex. genom administrering av användarrättigheter. Personer med tillgång till företagshemligheter är i första hand de som arbetar med sakkunnig- och utvecklingsuppgifter och till vilkas arbetsuppgifter det hör att behandla företagshemligheter. Därutöver kan de som arbetar i olika biträdande uppgifter och personer som svarar för drift och service av informationssystem genom sina arbetsuppgifter eller omfattande användarrättigheter få vetskap om företagshemligheter.

13 f §. *Sammanslutningsabonnenters skyldighet att lämna uppgifter till användare i fall av missbruk.* Enligt det föreslagna 1 mom. skall sammanslutningsabonnenten utarbeta en redogörelse för den manuella behandling av identifieringsuppgifter som avses i 13 d § 1 och 2 mom.

Redogörelsen skall innehålla uppgift om hurdan incident eller gärning enligt 13 d § 2 mom. som utgör grunden för behandlingen och på vilka grunder den manuella behandlingen av identifieringsuppgifter har inletts. Enligt 13 d § 2 mom. får identifieringsuppgifter tas till manuell behandling på basis av en avvikelse som har upptäckts med hjälp av den automatiska sökfunktionen eller utifrån allmänt konstaterbara omständigheter. Om behandlingen har inletts på grundval av en automatisk sökning, skall det utredas vilket sökkriterium för den automatiska sökfunktionen som ligger till grund för att identifieringsuppgifterna har blivit föremål för manuell behandling. Om behandlingen har inletts på grundval av en allmänt konstaterbar omständighet, skall omständigheten uppges. Av redogörelsen skall också framgå tidpunkten för behandlingen, vem som behandlade uppgifterna och vem som beslutade om behandlingen.

Enligt 2 mom. skall redogörelsen undertecknas av de personer som har deltagit i behandlingen. Redogörelsen behövs med tanke på rättssäkerheten för användarna av kommunikationsnäten och tjänsterna, för dem som deltagit i behandlingen av uppgifterna och för den som beslutat om behandlingen. Det bör vara möjligt att i efterhand utreda vem som har behandlat uppgifterna, vid vilken tidpunkt och på vems initiativ. Med hjälp av uppgifterna kan eventuella missbruk utredas i efterhand. Det föreslås bli bestämt att redogörelsen skall förvaras i två år.

Den 10 februari 2003 meddelade dataombudsmannens byrå anvisningar för behandlingen av användarlogguppgifter enligt personuppgiftslagen. Enligt anvisningarna får registrerade logguppgifter förvaras så länge den registrerade kan framställa straffrättsliga yrkanden mot den som behandlat personuppgifter eller mot tredje man. I anvisningarna konstateras att eftersom lagstridig behandling av personuppgifter och intrång i register är kriminaliserade gärningar i fråga om vilka åtalsrätten preskriberas inom två år, skall loggen förvaras i två år, om det inte tidigare har kunnat konstateras att grunden för förvaringen har förlorat sin betydelse. Redogörelsen och de registrerade uppgifterna bildar ett personregister som avses i personuppgiftslagen och som omfattas av alla bestämmelser om behandling av personuppgifter, t.ex. bestämmelserna om rätt till insyn (26 §) men också bestämmelserna om inskränkningar i rätten till insyn (27 §).

Enligt det föreslagna 3 mom. skall användaren informeras om den redogörelse som avses i 1 mom. så snart det är möjligt utan att syftet med behandlingen äventyras. Efter att ha fått kännedom om behandlingen av identifieringsuppgifterna har användarna möjlighet att försäkra sig om att åtgärderna är lagenliga och i förekommande fall kontakta dataombudsmannen eller polisen. Om användaren är en arbetstagare, kan han eller hon också kontakta sin fackorganisation.

I momentet föreslås en bestämmelse enligt vilken användaren av kommunikationsnätet eller kommunikationstjänsterna, utan hinder av sekretess som baserar sig på lag eller avtal, skall ha rätt att för behandlingen av ett ärende som gäller användarens intressen och rättigheter överlämna redogörelsen och de uppgifter användaren fått i samband med den. Bestämmelsen är tvingande och kan inte frångås genom avtal.

Det är likväl inte nödvändigt att ge redogörelsen till sådana användare vilkas identifieringsuppgifter har behandlats manuellt så att behandlingen har utförts i form av massbehandling utan att riktas till en viss användares identifieringsuppgifter.

Det föreslås inte någon tidsgräns för när redogörelsen skall delges. Redogörelsen eller uppgifterna skall lämnas så snart som möjligt efter det att behandlingen har avslutats. Utredningsrelaterade omständigheter med anledning av en pågående förundersökning eller därmed jämförbara orsaker kan berättiga till att delgivningen av redogörelsen senareläggs tills den kan delges utan att undersökningen äventyras.

Nödvändighetsvillkoret i 8 § 3 mom. i lagen begränsar för sin del också möjligheterna att senarelägga delgivningen av redogörelsen för utredningsrelaterade orsaker. Behandlingen får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än vad som är nödvändigt med tanke på ändamålet. Så snart det misstänkta missbruket har utretts tillräckligt skall behandlingen avslutas och en redogörelse för behandlingen upprättas och ges till användaren.

13 g §. *Sammanslutningsabonnenters skyldighet att lämna uppgifter till företrädare arbetstagarna i fall av missbruk.* I det föreslagna 13 g § 1 mom. bestäms om arbetsgivarens skyldighet att årligen till företrädaren för arbetstagarna ge en redogörelse för den manuella behandling av identifieringsuppgifter som avses i 13 d § 2 mom. för att effektivt övervaka integritetsskyddet. Till innehållet skall redogörelsen motsvara den utredning som avses i 13 h § 2 mom., av den skall framgå antalet manuella behandlingar av identifieringsuppgifter under ett år och grunderna för dem.

Enligt 2 mom. avses med arbetstagarnas företrädare, till vilken den i 1 mom. avsedda redogörelsen skall lämnas, i första hand antingen en förtroendeman i enlighet med arbetskollektivavtalet eller ett förtroendeombud enligt 13 kap. 3 § i arbetsavtalslagen. Om någon personalgrupp inte har någon sådan företrädare skall de representeras av ett samarbetsombud enligt lagen om samarbete i företag. Om inte heller någon sådan har utsetts skall redogörelsen delges samtliga arbetstagare som hör till personalgruppen i fråga.

En del av de uppgifter som ingår i samarbetsförfarandet eller informationen är inte offentliga. Med tanke på den fortsatta näringsverksamheten och syftet med förfarandena är det viktigt att uppgifterna inte sprids till en bredare krets än vad som avses i paragrafen. Därför föreslås det i 3 mom. att den företrädare för arbetstagarna eller arbetstagare som avses i paragrafen skall hemlighålla de kränkningar av företagshemligheten och de misstänkta fall av kränkningar av företagshemlighet som de tagit del av.

Uppgifter som omfattas av tystnadsplikten får inte röjas för utomstående ens efter det att personen inte längre utför den uppgift där han eller hon tagit del av informationen. Tystnadsplikten fortsätter att gälla för både arbetstagarna och deras företrädare under hela den tid anställningsförhållandet pågår. Bestämmelser om straff för brott mot tystnadsplikten föreslås ingå i 42 §.

Bestämmelser om sekretess finns i 24 § i lagen om offentlighet i myndigheternas verksamhet (621/1999). Bestämmelsen är delvis överlappande i fråga om vilka uppgifter som skall vara sekretessbelagda enligt den föreslagna lagen, vilket är oändamålsenligt. Det föreslås därför bli bestämt att i fråga om tystnadsplikten för tjänstemän och andra anställda hos myndigheter gäller vad som bestäms i lagen om offentlighet i myndigheternas verksamhet och någon annanstans i lag.

Den föreslagna tystnadsplikten skall inte hindra att uppgifter lämnas ut till de myndigheter som övervakar lagen.

I förslaget tas inte ställning till frågor som berör situationer då ett anställningsförhållande upphör. Frågan om när olovligt brukande av avgiftsbelagda informationssamhällstjäns-

ter eller kommunikationsnät eller brukande av kommunikationstjänster som strider mot anvisningarna eller brottslig verksamhet berättigar till att upphäva ett anställningsförhållande avgörs med stöd av arbetsavtalslagen och annan arbetsrättslig lagstiftning. I rättegångar som gäller upphävning av ett arbetsförhållande är arbetsgivaren skyldig att påvisa grunden för att arbetsförhållandet har upphävts. Förslagen medför inga ändringar i dessa principer.

13 h §. *Förhandsanmälan och årlig redogörelse till dataombudsmannen i fall av missbruk.* I den föreslagna 13 h § bestäms om en sammanslutningsabonnents skyldighet att lämna dataombudsmannen en redogörelse med uppgifter om behandlingen av identifieringsuppgifter.

Enligt 1 punkten skall en sammanslutningsabonnent innan en behandling av identifieringsuppgifter inleds lämna dataombudsmannen en redogörelse av engångsnatur av vilken framgår grunderna och praxisen för behandlingen av identifieringsuppgifterna enligt 13 d §. Enligt 2 punkten skall det av förhandsanmälan framgå i vilka arbetsuppgifter enligt 13 c § 1 mom. uppgifterna behandlas. Till denna del bör det av redogörelsen framgå samma omständigheter som enligt 13 c § 2 mom. skall behandlas i ett samarbetsförfarande. Av redogörelsen skall enligt 3 punkten också framgå hur sammanslutningsabonnenten har informerat eller informerar användarna av kommunikationsnäten och tjänsterna om dessa omständigheter. Om de omständigheter som redogörelsen gäller förändras väsentligt, skall en ny redogörelse om förändringarna lämnas in.

Enligt 13 § i den gällande lagen kräver behandling av identifieringsuppgifter i fall av missbruk inga som helst förhandsåtgärder innan behandlingen inleds. Inte heller i 6 kap. i lagen om integritetsskydd i arbetslivet, i vilket bestäms om hämtning och öppnande av e-postmeddelanden som hör till arbetsgivaren, föreskrivs om något särskilt anmälnings- eller tillståndsförfarande som skall genomföras på förhand.

Genom den föreslagna anmälningsplikten förbättras användarnas rättskydd. Jämfört med t.ex. ett tillståndsförfarande kan det föreslagna lämnandet av en förhandsanmälan anses stå i rätt proportion till det intresse som skyddas. Dataombudsmannen får på förhand information om vilka instanser som börjar använda sin rätt att behandla identifieringsuppgifter och dataombudsmannen kan genom att ordna sin verksamhet på ett ändamålsenligt sätt börja utöva övervakning enligt den föreslagna 32 § 1 mom 1 punkten.

Enligt det föreslagna 2 mom. skall en sammanslutningsabonnent årligen ge dataombudsmannen en redogörelse av vilken det för det gångna året och för varje gång som identifieringsuppgifter har behandlats framgår huruvida behandlingen har grundat sig på olovligt brukande i strid med anvisningarna för kommunikationsnätet eller kommunikationstjänsten eller på röjande av företagshemlighet.

13 i §. *Sammanslutningsabonnenters rätt att lagra identifieringsuppgifter i fall av missbruk.* I 13 i § föreslås en förtydligande bestämmelse om att bestämmelserna i 13 a–13 h § inte ger sammanslutningsabonnenten rätt att lagra identifieringsuppgifter i registret längre än vad som annars är tillåtet enligt lag.

Enligt 8 § 3 mom. skall identifieringsuppgifterna efter behandlingen förstöras eller göras sådana att de inte kan förknippas med abonnenten eller användaren.

Sådana identifieringsuppgifter av vilka det går att identifiera en fysisk person är också de personuppgifter som avses i personuppgiftslagen. Till följd av det begrepp om personregister som antagits i personuppgiftslagen utgör sådana identifieringsuppgifter ett i personuppgiftslagen avsett personregister trots att uppgifterna inte lagras i ett särskilt tekniskt register (personuppgiftslagen, 3 § 3 punkten).

13 j §. *Sammanslutningsabonnenters rätt att lämna ut uppgifter i fall av missbruk.* I paragrafen föreslås en bestämmelse som berättigar en sammanslutningsabonnent att i samband med polisanmälan eller begäran om utredning i egenskap av målsägande lämna ut till polisen för behandling sådana identifieringsuppgifter om användare av sammanslutningsabonnentens kommunikationsnät som sammanslutningsabonnenten fått vid ett förfarande som avses i de föreslagna 13 a–13 i §.

I formuleringen i den föreslagna bestämmelsen har det beaktats att den också skall berättiga polisen att behandla de uppgifter polisen fått på detta sätt. Bestämmelsen behövs för att sammanslutningsabonnenterna skall kunna föra till brottsutredning sådana fall där det kan vara fråga om gärningar som angetts som straffbara, såsom olovligt brukande eller brott som gäller företagshemligheter.

14 §. *Behandling för att upptäcka tekniska fel eller brister*. Eftersom det skall vara möjligt att inte bara upptäcka fel och brister utan också att förhindra och utreda dem föreslås det att bestämmelsen preciseras. Också i ljuset av detaljmotiveringen till 14 § i regeringspropositionen med förslag till den gällande lagen är det klart att bestämmelsen är avsedd inte bara för att upptäcka utan också för att förhindra och utreda fel och brister.

20 §. *Åtgärder för att genomföra dataskyddet.* I paragrafen föreslås bestämmelser om rättigheterna för teleföretagen, dem som tillhandahåller mervärdestjänster och sammanslutningsabonnenterna att vidta åtgärder för att sörja för dataskyddet. Bestämmelserna gör det möjligt att upptäcka, förhindra och utreda åtgärder som inverkar störande på dataskyddet i fråga om kommunikationsnäten och de tjänster som anslutits till dem och för att göra åtgärderna föremål för förundersökning.

Typiska hot mot informationssäkerheten är hot som riktas mot kommunikationsnätet eller -tjänsterna utifrån t.ex. i avsikt att ta reda på användarens uppgifter eller för att kapa datorer i syfte att göra blockeringsattacker eller för att skicka oönskad direktreklam. Informationssäkerhetsåtgärderna riktas vanligen till den trafik som kommer in i kommunikationsnätet eller tjänsten, fastän det i vissa situationer kan finnas ett behov att rikta åtgärderna också för att utreda hot som äventyrar informationssäkerheten i den utgående trafiken.

I 1 mom. specificeras de som är berättigade att vidta dataskyddsåtgärder samt de situationer där sådana åtgärder kan vidtas. Utöver de kommunikationsrelaterade åtgärder som föreslås i paragrafen kan dataskyddet ombesörjas också genom informationsadministrativa metoder och genom att det införs sådana tekniska begränsningar för användningen av kommunikationsnätet eller tjänsten för vilka det i lagen om dataskydd vid elektronisk kommunikation inte anges några restriktioner.

Som exempel på i 1 mom. 1 punkten avsedda åtgärder som inverkar menligt på dataskyddet kan nämnas omfattande spridning och användning av avsiktligt skadliga program. Åtgärder som inverkar menligt är också användning av kommunikationsnätet för att sända eller i stor utsträckning ta emot oönskade direktmarknadsföringsmeddelanden eller användning av andra meddelanden för att lamslå datakommunikationen eller informationssystemen eller andra störningar som är mycket allvarliga för funktionsdugligheten hos kommunikationsnätet eller de tjänster som anslutits till det. Också situationer där den normala verksamheten i kommunikationsnätet störs på något annat sätt eller där man olovligen förstör eller ändrar uppgifter som sparats i maskinvaran kan utgöra åtgärder som inverkar störande.

Med tjänster som anslutits till kommunikationsnätet avses i den föreslagna bestämmelsen förutom kommunikationstjänster enligt definitionen i 2 § 1 mom. 6 punkten och mervärdestjänster enligt definitionen i 7 punkten i samma lagrum i den gällande lagen också tjänster som sammanslutningsabonnenterna köper från annat håll och de tjänster som sammanslutningsabonnenterna själva tillhandahåller.

I 2 punkten föreslås ett särskilt omnämnande av tryggandet av kommunikationsmöjligheterna för den som sänder eller mottar ett meddelande, eftersom det antal oönskade direktmarknadsföringsmeddelanden och andra motsvarande meddelanden som slutanvändaren får kan bli så stort att slutanvändarens kommunikationsmöjligheter förhindras helt och hållet även om antalet meddelanden av detta slag inte påverkar hela kommunikationsnätets eller kommunikationstjänstens funktion. Dessutom kan angrepp mot dataskyddet riktas till en viss användare, vars kommunikation då helt kan förhindras. Den föreslagna ändringen behövs för att det skall bli klart att åtgärder för att genomföra dataskyddet kan vidtas även i dessa fall.

I 3 punkten föreslås en bestämmelse om rätt att vidta åtgärder även för att förhindra förberedelse till betalningsmedelsbedrägerier enligt 37 kap. 11 § i strafflagen vilka planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna. Här handlar det om s.k. phishing (nätfiske), dvs. meddelanden till en stor grupp användare i syfte att ta reda på uppgifter om användarnas identitet och betalmedel och använda dem för illegala ändamål.

Förberedelse till betalningsmedelsbedrägeri omfattar situationer där den som för utförande av betalningsbedrägeribrott tillverkar, i landet inför, anskaffar, tar emot eller innehar en betalningsmedelsblankett eller som tillverkar, i landet inför, anskaffar, tar emot, innehar säljer eller överlåter redskap eller tillbehör som särskilt lämpar sig för tillverkning av betalningsmedelsblanketter, eller upptagningar, programvara, redskap eller tillbehör som särskilt lämpar sig för betalningsrörelse som sker via datanät.

I motiveringen till strafflagen (RP 38/1997 rd) konstateras att för att det skall handla om sådana medel eller upptagningar som avses i lagrummet skall man antingen kunna utföra betalningar, kontoöverföringar eller uttag med dem, eller så skall deras användning vara en nödvändig förutsättning för att man skall kunna utföra nämnda transaktioner. Det finns dock situationer där betalning inte kan ske utan att tilläggsinformation lämnas. Sådan tilläggsinformation utgörs enligt regeringspropositionen av t.ex. olika identifieringsmetoder med vilka användaren av betalningsmedlet förknippas med betalningen eller med en annan transaktion. Betalning av räkningar i nätbanken förutsätter att man uppger det kundnummer som banken gett samt ett signum eller lösenord som byts vid varje användning. Enligt propositionen är det motiverat att jämställa sådana förutsättningar som är nödvändiga för att ett betalningsmedel skall kunna användas med de medel och upptagningar med hjälp av vilka de egentliga transaktionerna utförs.

I de föreslagna 2 och 3 mom. bestäms om åtgärder som kan vidtas för att sörja för dataskyddet. Åtgärderna kan gälla själva meddelandena men också eventuella bilagor till dem.

I 2 mom. 1 punkten föreslås som en åtgärd en automatisk analys av innehållet i meddelanden. För automatisk filtrering av skadliga meddelanden och även i övrigt för upprätthållande av dataskyddet krävs det i praktiken att meddelandena kontinuerligt analyseras automatiskt. Vid automatisk analys identifieras skadliga program och kommandon på basis av definitioner som utformats på förhand, och fysiska personer får då inte ta del av innehållet i meddelandena.

Enligt 20 § 3 mom. i den gällande lagen får ingrepp göras i meddelandets innehåll endast med tekniska medel för att kontrollera meddelandet. Kontrollen är bunden vid vissa brottsrekvisit. Av det att möjligheten att ingripa i innehållet i meddelandena är bunden vid brottsrekvisit följer att en analys kan göras bara när handlingen är uppsåtlig. I praktiken sänds skadliga meddelanden inte alltid med uppsåt. För att dataskyddet skall kunna upprätthållas bör det vara möjligt att analysera också meddelanden som sänts utan uppsåt och som äventyrar dataskyddet.

I den föreslagna 2 punkten föreslås begränsning av förmedling eller mottagande som en ny åtgärd utöver förhindrande av förmedling och mottagande av meddelanden. Det preciseras dessutom att både begränsning och förhindrande av förmedling eller mottagande av meddelanden skall utföras automatiskt enligt på förhand utformade definitioner. Begränsning gör det möjligt att vidta lindrigare åtgärder än att helt och hållet avbryta en tjänst.

Automatisk begränsning av förmedling och mottagande av meddelanden kan bli aktuell t.ex. i en situation där ett förbindelsesätt eller ett certifierings- eller identifieringsförfarande visar sig innehålla en farlig svaghet och användningen bör förhindras utan några ingrepp i förmedlingen av andra meddelanden. Likaså gäller att om det noteras att skadliga meddelanden kommer från en viss uppkopplingsadress kan mottagandet av meddelanden från den adressen begränsas. Automatisk begränsning kan bli aktuell också när den kvantitativa eller kvalitativa ökningen av ett kommunikationssätt hotar förhindra de övriga kommunikationssätten. Förhindrande av förmedling eller mottagande av meddelanden kan bli aktuellt t.ex. när datorn har tagits i

besittning och hotet inte kan avvärjas med metoder som begränsar kommunikationen i mindre grad. På samma sätt som i fråga om att förhindra skall det vara tillåtet att begränsa endast om åtgärderna är nödvändiga för att målen enligt 1 mom. skall kunna uppnås.

Enligt den föreslagna 3 punkten skall skadliga datorprogram få avlägsnas ur meddelanden med hjälp av automatisk databehandling. Avlägsnandet skall genomföras automatiskt enligt på förhand utformade definitioner. Sådana program eller kommandon som avsiktligt orsakar icke önskade transaktioner i datorn eller datasystemet är skadliga på det sätt som avses i bestämmelsen. Sådana program kan t.ex. ge utomstående tillträde till nätet eller de dator som anslutits till det, ändra eller för utomstående röja uppgifter som sparats i datorerna eller ge utomstående möjlighet att ha kontroll över datorn.

Enligt den föreslagna 4 punkten skall även andra, med de i momentet tidigare förtecknade åtgärderna jämförbara tekniska åtgärder stå till förfogande när det gäller att sörja för dataskyddet. Sådana åtgärder kan omfatta analys av identifieringsuppgifterna för trafiken för flera datorer i syfte att upptäcka kausalitet, vilket är nödvändigt för att varsebli olovlig distansstyrning och isolera skadliga kommandon samt artificiell uppbromsning av kommunikationen eller andra motsvarande åtgärder.

I det föreslagna nya 3 mom. ingår en bestämmelse om rätt att behandla innehållet i enstaka meddelanden manuellt, om det är uppenbart att en automatisk databehandling av innehållet inte kan trygga uppnåendet av målen enligt det föreslagna 1 mom. Det föreslagna momentet berättigar till manuell kontroll av innehållet i meddelanden i allvarliga hotfulla situationer där det på basis av typen av meddelande, meddelandets form eller någon annan motsvarande omständighet är uppenbart att meddelandet innehåller ett skadligt datorprogram eller ett skadligt kommando och en automatisk analys av innehållet inte räcker till för att garantera dataskyddet.

Om det vid en automatisk analys av innehållet upptäcks att ett meddelande utgör ett hot mot dataskyddet men problemet inte kan lösas enbart på basis av analysen, skall innehållet i och identifieringsuppgifterna för meddelandet få behandlas även manuellt. Vid en automatisk analys av innehållet identifieras inte alltid skadliga program eller skadliga kommandon i meddelandena fullständigt, vilket kan äventyra kommunikationssystemen. Funktionsprincipen hos skadliga program i meddelanden kan vara obekant för det automatiska analysprogrammet. Det är då ytterst viktigt att manuellt utreda vad som orsakade den farliga situationen och hur detta skall kunna avvärjas i fortsättningen. Informationssystemen kan också sända automatiska meddelanden till varandra, vilka i händelse av fel bör kunna genomgås manuellt för att felet skall kunna åtgärdas. Också i sådana fall då datorn olovligen har börjat styras på distans kan det vara nödvändigt att klarlägga innehållet i de styrningsrelaterade meddelandena för att situationen skall kunna utredas.

Manuell behandling aktualiseras i samband med skadliga meddelanden som kan innehålla t.ex. ett skadligt program eller ett skadligt kommando som syftar till att lamslå hela nätet eller tjänsten. Om man inte lyckas avlägsna de skadliga meddelandena, kan de skadliga program de innehåller äventyra kommunikationsmöjligheterna för alla som använder nätet eller äventyra konfidentialiteten hos data som sparats i datorerna. Avsändaren och mottagaren skall underrättas om ingrepp i innehållet i meddelandena, om underrättelsen inte äventyrar uppnåendet av målen enligt 1 mom. En underrättelse främjar inte alltid ändamålet, exempelvis då ett meddelande innehåller t.ex. en skadlig kod som lamslår informationssystemen. Underrättelse om den skadliga koden gagnar inte tryggandet av dataskyddet i näten eller tjänsterna eller tryggandet av mottagarens kommunikationsmöjligheter. Underrättelsen kan i stället medföra ytterligare problemsituationer.

Rätten att granska innehållet i meddelanden innebär inte någon allmän rätt att kontrollera, utan det handlar om synnerligen exceptionella situationer. Enligt det föreslagna 4 mom. skall manuell behandling av innehållet i meddelanden vara nödvändig för att sörja för dataskyddet.

Enligt det föreslagna 4 mom. skall åtgärderna utföras omsorgsfullt och de skall stå i proportion till den störning som skall avvärjas. Åtgärderna skall likaså utföras utan att

yttrandefriheten eller skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än nödvändigt.

I 4 mom. föreslås att de detaljerade hänvisningarna till tjänster och säkerställande av kommunikationsmöjligheterna för mottagaren av ett meddelande ersätts med en hänvisning till det som bestäms ovan i paragrafen. Det handlar om en ändring av teknisk natur som inte syftar till att förändra det rådande rättsläget.

Det föreslås att 5 mom. preciseras så att Kommunikationsverkets rätt att meddela tekniska föreskrifter begränsas till att gälla föreskrifter endast för teleföretagen och dem som tillhandahåller mervärdestjänster.

32 §. *Dataombudsmannens uppgifter*. Det föreslås att dataombudsmannens uppgifter utökas med uppgiften att övervaka i 13 a–13 j § avsedd behandling av identifieringsuppgifter som utförs av en sammanslutningsabonnent i situationer med olovligt brukande av avgiftsbelagda informationssamhällstjänster eller kommunikationsnät eller brukande av kommunikationstjänster som strider mot anvisningarna och situationer med obehörigt röjande av företagshemligheter. I praktiken är det nödvändigt att koncentrera övervakningsåtgärderna till vissa sakkomplex. Dataombudsmannen skall i enlighet med personuppgiftslagen övervaka behandlingen av personuppgifter. Lagen om integritetsskydd i arbetslivet övervakas av arbetarskyddsmyndigheterna i samråd med dataombudsmannen. Eftersom företag i egenskap av arbetsgivare är en av de största grupperna av sammanslutningsabonnenter är det följdriktigt att dataombudsmannen delvis skall övervaka efterlevnaden av denna lag.

Det föreslås att man i paragrafens andra moment tar in en bestämmelse enligt vilken det är möjligt att ta ut en avgift av sammanslutningsabonnenten för de åtgärder som tillsynen av efterlevnaden av bestämmelserna i 13 a–13 j § ger upphov till. Beslut om avgiftsbelagda åtgärder och avgiftens storlek fattas genom förordning av justitieministeriet enligt de grunder som föreskrivs i lagen om grunderna för avgifter till staten (150/1992). Vid en exakt uppskattning av resurserna och kostnaderna för dem skall behöriga ministerier och de som avgiftsskyldigheten gäller höras. Avgiftsskyldigheten skall stå i rätt proportion till den som är föremål för tillsynen och verksamhetens art. Det är motiverat att tillsynen blir avgiftsbelagd, eftersom den behandling av identifieringsuppgifter som avses i 13 a–13 j § är valfri för sammanslutningsabonnenten.

33 §. *Styrnings- och övervakningsmyndigheternas rätt att få uppgifter*. Enligt den gällande lagen gäller att för att utföra sina i denna lag föreskrivna uppgifter har Kommunikationsverket och dataombudsmannen rätt att få identifierings- och lokaliseringsuppgifter och i 20 § 2 mom. avsedda meddelanden förutsatt att vissa till brottsrekvisitet starkt bundna kriterier uppfylls. Det föreslås att 20 §, som gäller dataskyddet, ändras så att automatisk analys av innehållet i meddelanden tillåts och så att det i vissa situationer skall vara tillåtet att ingripa i innehållet i meddelanden också på något annat sätt än med metoder för automatisk analys av innehållet. Det föreslås därför att hänvisningen till ett visst moment i lagen upphävs. Här handlar det om de övervakande myndigheternas bedömning av att något av brottsrekvisiten uppfylls, och för att de skall kunna fullgöra sin uppgift som sig bör är det nödvändigt att de i vissa situationer i samband med tillsyn över efterlevnaden av lagen får såväl informations- och lokaliseringsuppgifter som meddelanden.

34 §. *Tillsynsmyndigheternas tystnadsplikt*. Det föreslås att dataombudsmannens tystnadsplikt skall omfatta även de i det föreslagna 13 h § avsedda redogörelser för behandling av identifieringsuppgifter som sammanslutningsabonnenterna skall lämna in till dataombudsmannen.

Det föreslås att bestämmelserna i 34 § 1 och 5 mom. i den gällande lagen skall kvarstå i 34 § och att 2, 3 och 4 mom. skall överföras till 34 a §. Ändringen är av teknisk natur.

34 a §. U*tlämnande av tillsynsmyndigheternas uppgifter*. Det föreslås att bestämmelserna i 34 § 2, 3 och 4 mom. i den gällande lagen tas in i den nya paragrafen. Ändringen är närmast av teknisk natur. Enligt 1 mom. utökas samtidigt Kommunikationsverkets rätt att utan hinder av sekretessbestämmelserna eller andra förbud mot utlämnande av uppgifter till de teleföretag, till dem som tillhanda-

håller mervärdestjänster och till de sammanslutningsabonnenter som sannolikt kan utsättas för kränkning av dataskydd lämna ut identifieringsuppgifter som verket erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskydd. Kommunikationsverket kan då till de instanser som nämns i paragrafen lämna ut t.ex. uppgifter om den IP-adress från vilken ett angrepp mot dataskyddet har genomförts. Dessa kan i sin tur förhindra att deras system utsätts för angrepp från adressen.

Enligt det nya 3 mom. skall Kommunikationsverket dessutom ha rätt att till sådana organisationer som är verksamma i andra stater och som har till uppgift att förebygga kränkningar av dataskydd riktade mot kommunikationsnät och -tjänster lämna ut identifieringsuppgifter som verket erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskydd. Här är det frågan om sådana instanser i andra stater som samordnar arbetet för att motverka och observera kränkningar av dataskydd och som motsvarar gruppen CERT-FI (Computer Emergency Response Team FICORA) vid Kommunikationsverket. Instanserna skall förebygga och observera kränkningar av dataskydd och finna lösningar på dessa frågor samt informera vid hot mot dataskyddet.

Enligt det föreslagna 4 mom. skall uppgifter till de ovan nämnda instanserna få lämnas ut endast i den omfattning som är nödvändig för att förebygga eller avvärja kränkningarna. Utlämnandet av uppgifter skall inte få begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt.

I situationer av kränkningar av dataskydd som riktats mot eller genomförts med hjälp av kommunikationsnät och kommunikationstjänster är det ofta omöjligt att förebygga kränkningar eller utreda kränkningarna enbart utgående från uppgifter som kan fås av finländska aktörer, eftersom de som startat kränkningarna använder sig av utrustning utanför Finlands gränser. Exempelvis i samband med nätfiskefall har inte en enda dator som sänt ut bluffmeddelanden funnits i ett finländskt nät. En dator som förorenats med skadliga program används inte bara för att sända bluffmeddelanden utan ofta också för att t.ex. distribuera skadliga program, göra angrepp som syftar till tillgänglighetsförlust i fråga om nät- och kommunikationstjänster eller andra tjänster som tillhandahålls via nätet samt för att dölja spåren efter dem som genomfört kränkningar av dataskyddet. För att avvärja kränkningar av dataskyddet vilka genomförs med hjälp av datorer som obehörigen tagits i besittning är det nödvändigt att förmedla uppgifter om förorenade datorer till de organisationer som i mållandet ansvarar för dataskyddet i fråga om kommunikationsnäten och kommunikationstjänsterna.

De uppgifter som utväxlas i syfte att förebygga kränkningar av dataskyddet är i typiska fall sådana uppgifter som exempelvis i Finland inte kan förknippas med någon fysisk person. Det är tänkbart att det i utlandet går att förknippa dem med en viss anordning och därigenom eventuellt med den person eller organisation som administrerar anordningen. Det händer också ofta att en anordning som används för angrepp mot kommunikationsnät och tjänster eller för andra kränkningar av dataskyddet obehörigen innehas av någon annan, dvs. den riktiga ägaren är i praktiken inte ens medveten om att anordningen används för kränkningar av dataskyddet. I situationer av detta slag är det nödvändigt och lämpligt att för avvärjning och förebyggande av kränkningar av dataskyddet lämna ut uppgifter till sådana instanser i andra stater som koordinerar åtgärderna för att utreda kränkningar av dataskyddet. De kan då informera teleföretagen och sammanslutningsabonnenterna i sin stat om hoten och de system som kopplats till kränkningar av dataskyddet.

Utgångspunkten är att samtycke till utlämnande av uppgifter skall begäras av den finländska kommunikationsparten, t.ex. samtycke av den organisation som utsatts för kränkning av dataskyddet. I vissa fall är det dock nödvändigt att också annars lämna ut uppgifter ur system som förmedlar kommunikation. Exempelvis med automatiska system för observation av intrång kan man samla in uppgifter utifrån vilka det är omöjligt att entydigt identifiera den avsedda mottagaren. Det kan också vara frågan om sådana uppgifter om källadresser för kränkningar av dataskyddet som samlats i utrustning som

används för tillhandahållande av teleföretagets allmänna kommunikationstjänster. Inte heller då kan de uppgifter som lämnas ut identifieras så att de gäller en finländare. Det är vanligen inte nödvändigt att lämna ut uppgifter om föremålet för angreppet utan om dess källa.

I det föreslagna 4 mom. tas in en bestämmelse om att också den i 3 mom. avsedda rätten att lämna ut identifieringsuppgifter till sin omfattning skall begränsas så att den gäller endast sådant utlämnande som är nödvändigt för att förebygga och utreda kränkningar av dataskyddet. Utlämnandet av uppgifter skall inte heller få begränsa skyddet av konfidentiella meddelanden mer än nödvändigt.

42 §. *Straffbestämmelser.* Enligt förslaget skall det till 1 mom. i lagens straffbestämmelser fogas en bestämmelse enligt vilken straff för brott mot i 13 g § 3 mom. avsedd arbetstagares tystnadsplikt utdöms enligt 38 kap. 2 § 2 mom. i strafflagen, om inte strängare straff för gärningen föreskrivs någon annanstans än i 38 kap. 1 § i strafflagen.

Det föreslås att en ny 9 punkt fogas till 2 mom. Enligt den nya bestämmelsen skall det vara straffbart som dataskyddsförseelse vid elektronisk kommunikation att försumma de efterföljande skyldigheter som garanterar att behandlingen av identifieringsuppgifterna är lagenlig.

Sammanslutningsabonnenter skall fullgöra skyldigheterna endast om de behandlar identifieringsuppgifter på det sätt som avses i 13 a–13 j §. Sammanslutningsabonnenter som inte behandlar identifieringsuppgifter behöver inte heller fullgöra skyldigheterna enligt 13 a–13 j §, och det är då inte straffbart att försumma dem.

Enligt den föreslagna 9 punkten skall det vara straffbart att underlåta utarbeta eller lämna in en sådan redogörelse som avses i 13 f §.

Det skall också vara straffbart att underlåta att till företrädaren för arbetstagarna lämna en sådan redogörelse om behandlingen av identifieringsuppgifter som avses i 13 g § samt att underlåta att till dataombudsmannen lämna in en förhandsanmälan enligt 13 h § 1 punkten och en årlig redogörelse enligt 2 mom.

Försummelse av skyldigheter som garanterar lagenligheten i fråga om identifieringsuppgifter skall vara straffbar endast när skyldigheterna försummas uppsåtligen.

1.2 Lagen om integritetsskydd i arbetslivet

2 §. *Tillämpningsområde.* Det föreslås att en förtydligande hänvisning till lagen om dataskydd vid elektronisk kommunikation tas in i bestämmelsen om lagens tillämpningsområde.

21 §. *Samarbete vid ordnande av teknisk övervakning och användning av datanät.* Det föreslås att förteckningen över ärenden som skall behandlas i ett samarbetsförfarande kompletteras med ett omnämnande av behandling av uppgifter som gäller e-post och annan elektronisk kommunikation så som föreslås i de nya 13 a–13 j § i lagen om dataskydd vid elektronisk kommunikation. I 13 a–13 j § i lagen om dataskydd vid elektronisk kommunikation avsedda anvisningar för användningen av kommunikationsnät och tjänster och behandlingen av företagshemligheter, situationer där behandling är möjlig, de allmänna principerna för automatisk sökning och de arbetsuppgifter som innebär att identifieringsuppgifter får behandlas skall omfattas av samarbetsförfarande och information.

I samarbetsförfarandet bör också behandlas de centrala principer och förfaranden som skall tillämpas på åtgärder för att trygga informationssäkerheten enligt 20 §.

Det föreslås dessutom att en hänvisning till lagen om samarbete mellan kommunala arbetsgivare och arbetstagare fogas till paragrafen. Hänvisningen behövs för att det skall bli klart att det att de ovan beskrivna omständigheterna i anslutning till behandling av identifieringsuppgifter skall behandlas i ett samarbetsförfarande också gäller kommunerna.

1.3 Lagen om samarbete inom företag

19 §. *Behandling av planer, principer och praxis som grundar sig på annan lagstiftning.* Det föreslås att 4 punkten kompletteras med ett omnämnande av behandling av uppgifter som gäller e-post och annan elektro-

nisk kommunikation så som föreslås i de nya 13 a–13 j § i lagen om dataskydd vid elektronisk kommunikation.

I samarbetsförfarandet bör också behandlas de centrala principer och förfaranden som skall tillämpas på åtgärder för att trygga informationssäkerheten enligt 20 §.

1.4 Lagen om samarbete inom statens ämbetsverk och inrättningar

7 §. *Ärenden som omfattas av samarbetsförfarandet.* Det föreslås att 11 a-punkten kompletteras med ett omnämnande av behandling av uppgifter som gäller e-post och annan elektronisk kommunikation så som föreslås i de nya 13 a–13 j § i lagen om dataskydd vid elektronisk kommunikation.

I samarbetsförfarandet bör också behandlas de centrala principer och förfaranden som skall tillämpas på åtgärder för att trygga informationssäkerheten enligt 20 §.

2 Ikraftträdande

Lagarna föreslås träda i kraft den 1 januari 2009. I denna proposition föreslås ändringar av den reglering som gäller teleföretagen, sammanslutningsabonnenterna och dem som tillhandahåller mervärdestjänster. Dessa bör reserveras tillräckligt lång tid för att utbilda personalen och ge personalen anvisningar samt gå igenom behövliga förfaranden.

3 Förhållande till grundlagen samt lagstiftningsordning

De föreslagna bestämmelserna bör granskas ur perspektivet för de grundläggande frioch rättigheterna enligt grundlagen. Sådana bestämmelser i lagförslaget som gäller hemligheten i fråga om förtroliga meddelanden och integritetsskydd finns i de föreslagna 9, 12, 12 a, 13, 13 a–13 j och 14 §, där det bestäms om behandling av identifieringsuppgifter, och i 20 §, där det bestäms om rätten att genomföra vissa åtgärder för att sörja för dataskyddet. Av de föreslagna bestämmelserna bör de nya 13 a–13 j §, som gäller sammanslutningsabonnenternas behandling av identifieringsuppgifter, och 20 §, som gäller dataskydd, granskas i detalj med tanke på de grundläggande fri- och rättigheterna.

I 10 § 1 mom. i grundlagen sägs att vars och ens privatliv, heder och hemfrid är tryggade 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 momentet är brev- och telefonhemligheten samt hemligheten i fråga om andra förtroliga meddelanden okränkbar.

Dessa rättsliga intressen som skyddas är dock inte absoluta, eftersom det i vissa situationer är nödvändigt att begränsa dem. 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 skall kunna tryggas och för att brott skall 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. I samband med grundrättsreformen avsågs att förteckningen över dessa möjligheter att begränsa skyddet för konfidentiell kommunikation skulle vara uttömmande (RP 309/1993 rd, s. 54).

Bestämmelserna i 10 § 3 mom. i grundlagen är ett lagförbehåll av fullmaktstyp som samtidigt innehåller bestämmelser som inskränker lagstiftarens befogenheter. I momentet ges lagstiftaren rätt att genom vanlig lag bestämma om sådana begränsningar i bl.a. kommunikationshemligheten som är nödvändiga för ändamål i anslutning till utredning av i begränsningsklausulen nämnda brott som äventyrar individens eller samhällets säkerhet.

Det primära syftet med 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 skall förbli konfidentiellt. I motiveringen har som exem-

pel nämnts identifieringsuppgifter om samtal (RP 309/1993 rd, s. 53).

Grundlagsutskottet har i sin vedertagna praxis ansett att identifieringsuppgifterna för meddelanden inte ingår i kärnområdet i den grundläggande fri- och rättigheten för hemlighet i fråga om förtroliga meddelanden (GrUU 47/1996 rd, s. 4, GrUU 7/1997 rd, s. 2, GrUU 26/2001 rd, s. 3, GrUU 9/2004 rd, s. 4, GrUU 10/2004 rd, s. 4, GrUU 16/2004 rd, s. 6, GrUU 23/2006 rd, s. 3).

Förhållandet mellan lagförbehållet i 10 § 3 mom. i grundlagen och identifieringsuppgifterna för meddelanden är inte ovillkorligt. Enligt regeringens uppfattning har grundlagsutskottet ansett att rätten att ta del av identifieringsuppgifterna för meddelanden inte bör bedömas i ljuset av lagförbehållet i 10 § 3 mom. i grundlagen utan i ljuset av de allmänna villkoren för begränsningar i de grundläggande fri- och rättigheterna.

Grundlagsutskottet bedömde i sitt utlåtande om ändring av telemarknadslagen (GrUU 47/1996 rd, s. 4), i ljuset av de allmänna grunderna för att inskränka de grundläggande fri- och rättigheterna, frågan om den rätt att ta del av identifieringsuppgifterna som gäller för den som är skyldig att betala teleräkning. Enligt utskottet skulle förslaget inte bedömas i direkt förhållande till de begränsningsgrunder som tilläts enligt 8 § 3 mom. i den då gällande regeringsformen och som åtminstone i första hand hänför sig till ingrepp från den offentliga maktens sida. När utskottet behandlade förslaget till lag om integritetsskydd i arbetslivet bedömde det arbetsgivarens rätt att ta reda på om arbetstagaren i sin frånvaro har mottagit eller omedelbart före frånvaron har skickat eller mottagit meddelanden som hör till arbetsgivaren och som det är nödvändigt att arbetsgivaren får vetskap om för att kunna ordna sin verksamhet eller trygga sina funktioner. Utskottet ansåg att arbetsgivaren inte kan betraktas som en utomstående mot vilken bestämmelserna om hemligheten i fråga om förtroliga meddelanden i grundlagens 10 § är tänkta att ge skydd (GrUU 10/2004 rd, s. 5). Enligt utskottet måste de begränsningar i meddelandehemligheten som föreslogs i propositionen bedömas utifrån de generella villkoren för begränsningar i de grundläggande fri- och rättigheterna.

En sammanslutningsabonnent, som ofta också är arbetsgivare, skall enligt de föreslagna 13 a–13 j § på vissa villkor få utreda en grundad misstanke om att sammanslutningsabonnentens kommunikationsnät har använts olovligen eller att nätet har använts för att olovligen lämna uppgifter om företagshemligheter som är väsentliga för näringsverksamheten. En sammanslutningsabonnent äger sina egna kommunikationsnät och kommunikationstjänster och är i fråga om den kommunikation som förmedlas genom dess nät inte en utomstående på det sätt som t.ex. ett teleföretag eller polisen, som utövar offentlig makt.

Sammanslutningsabonnenten tillhandahåller kommunikationstjänster för sina användare, t.ex. arbetstagarna. När det gäller sammanslutningsabonnenter hör tillhandahållandet av kommunikationstjänster för användarna mycket nära samman med möjliggörandet av sammanslutningsabonnentens huvudsakliga verksamhet. Om sammanslutningsabonnenten är t.ex. ett företag, hänger en betydande del av den kommunikation som sammanslutningsabonnenten förmedlar samman med företagets verksamhet. I detta fall är det företaget självt som är den ena parten i kommunikationen. Sammanslutningsabonnenten får inte heller identifieringsuppgifter av en utomstående, eftersom uppgifterna samlas i sammanslutningsabonnentens utrustning. Grundlagsutskottet har konstaterat att lagen om dataskydd vid elektronisk kommunikation i första hand reglerar relationerna mellan privata aktörer (GrUU 9/2004 rd, s. 2). Därmed anser regeringen att den rätt att behandla identifieringsuppgifter som föreslås i 13 a–13 j § inte behöver bindas vid vissa brottsrekvisit. Begränsningar i skyddet för förtroliga meddelanden som inte riktar sig till kärnområdet bör granskas utifrån de generella villkoren för begränsningar i de grundläggande fri- och rättigheterna.

När en sammanslutningsabonnents kommunikationsnät eller kommunikationstjänst störs krävs det en behandling av identifieringsuppgifterna för att utreda om det är fråga om en funktionsstörning eller ett funktionsfel i systemet eller om någon har miss-

brukat sammanslutningsabonnentens kommunikationsnät eller kommunikationstjänster. Om sammanslutningsabonnenten har utsatts för ett brott är det motiverat att tillåta behandling av identifieringsuppgifter så att en eventuell begäran om utredning kan utarbetas på ändamålsenligt sätt och så att en så störningsfri verksamhet som möjligt under förundersökningen garanteras. Brott som gäller företagshemligheter och olovligt brukande är så kallade målsägandebrott. Enligt 28 kap. 15 § och 30 kap. 12 § i strafflagen får allmänna åklagaren inte väcka åtal om inte målsäganden anmäler brottet till åtal eller ett synnerligen viktigt allmänt intresse kräver att åtal väcks. Enligt 2 § i förundersökningslagen (449/1987) skall polisen eller någon annan förundersökningsmyndighet göra förundersökning när det på grund av anmälan till den eller annars finns skäl att misstänka att ett brott har begåtts. Enligt lagen om rättegång i brottmål (689/1997) har målsägande en oberoende, sekundär rätt att väcka åtal för ett brott som riktats mot denne.

I samband med beredningen av propositionen gjordes en ingående bedömning av möjligheten att ge polisen i uppdrag att utreda samtliga fall av missbruk. På grund av antalet sammanslutningsabonnenter, de många olika formerna av missbruk, de stora olikheterna mellan systemen och de resurser dessa uppgifter skulle kräva ansågs detta alternativ överhuvudtaget inte vara genomförbart. Det är fråga om uppgifter som hänger samman med det dagliga underhållet av sammanslutningsabonnenternas egna kommunikationssystem, som det är nödvändigt att varje sammanslutningsabonnent själv ansvarar för. Samtidigt avses det bli möjligt för sammanslutningsabonnenten att avgränsa en eventuell begäran om förundersökning hos polisen så att förundersökningen (inklusive de datorer och servrar som överlåts till polisen för den tid då undersökningen pågår) inte äventyrar kontinuiteten av hela företagets verksamhet. Det är polisen som avses genomföra förundersökningen. Propositionen syftar inte till att överföra polisens uppgifter på företag.

Det bör dock noteras att om en sammanslutningsabonnent i samband med uppgifter som hänför sig till underhåll av sina kommunikationsnät och kommunikationstjänster eller annars behandlar identifieringsuppgifter i strid med lagen, har polisen laglig behörighet att genomföra en förundersökning i ärendet. Dessutom skall dataombudsmannen övervaka hur sammanslutningsabonnenterna behandlar identifieringsuppgifter. Dataombudsmannen avses ha rätt att ålägga den som gjort sig skyldig till en överträdelse att rätta sitt fel eller sin försummelse eller ha rätt att förstärka åläggandet med vite eller hot om att den försummade åtgärden vidtas på den försumliges bekostnad.

Regleringen enligt de föreslagna 13 a–13 j § påverkar närmast det inbördes förhållandet mellan enskilda rättssubjekt. Vid bedömningen av de grundläggande fri- och rättigheterna accentueras då 22 § i grundlagen, där det bestäms om det allmännas skyldighet att se till att de grundläggande fri- och rättigheterna tillgodoses. I det här fallet anknyter tillgodoseendeskyldigheten till en regleringslösning som på ett balanserat sätt sammanjämkar rättigheterna för dem som använder kommunikationsnäten och kommunikationstjänsterna samt sammanslutningsabonnenternas rättigheter. Bedömningen av sammanjämkningen av olika grundläggande fri- och rättigheter ingår i bedömningen av de föreslagna ändringarnas godtagbarhet med tanke på de generella villkoren för begränsningar i de grundläggande fri- och rättigheterna.

När det gäller de grundläggande fri- och rättigheterna är det i propositionen fråga om en sammanjämkning av egendomsskyddet enligt 15 § och näringsfriheten enligt 18 § i grundlagen med hemligheten för användarnas förtroliga meddelanden. Tryggandet av användningen av elektroniska kommunikationsnät och kommunikationstjänster kan bedömas som en fördel med förmögenhetsvärde som i dagens kommunikationscentrerade omvärld hänförs till egendomsskyddet enligt 15 § i grundlagen. Säkerställandet av konfidentialiteten för företagshemligheter och resultaten av utvecklingsarbete vilka är centrala för sammanslutningsabonnentens näringsverksamhet kan likaså anses omfattas av egendomsskyddet och näringsfriheten. Grundlagsutskottet har behandlat frågorna gällande egendomsskydd bl.a. i samband med behandlingen av en proposition med

förslag till ändring av telelagen (GrUU 1/1996 rd), propositioner med förslag till ändring av telemarknadslagen (GrUU 47/1996 rd, GrUU 34/2000 rd och GrUU 5/2001 rd) och en proposition med förslag till ändring av lagstiftningen om kommunikationsmarknaden (GrUU 8/2002 rd).

Utskottets praxis hittills kan sammanfattas som att de olika förpliktelserna i fråga om egendomsskydd stämmer överens med grundlagen med hänsyn till egendomens speciella karaktär, om skyldigheterna finns inskrivna i tydliga lagbestämmelser och är skäliga med avseende på ägaren. Regeringen anser att grundlagsutskottet i sin utlåtandepraxis har funnit det vara viktigt att skyldigheterna för ägaren begränsas av ägarens befintliga behov och skäliga framtida behov. Den skyldighet som garanterar konfidentiell kommunikation som fastställs i 4 § i lagen om dataskydd vid elektronisk kommunikation kan även ses som en skyldighet som begränsar sammanslutningsabonnenternas egendomsskydd.

Det föreslås att rätten att behandla identifieringsuppgifter som gäller elektronisk kommunikation skall regleras i lag. Det föreslås att bestämmelser som säkerställer sådana situationer som berättigar till behandling av identifieringsuppgifter, gränserna för behandlingsrätten och lagenligheten hos behandlingen tas in i lagen om dataskydd vid elektronisk kommunikation. Förslagen uppfyller således kravet på reglering i lag.

En förutsättning för rätten att behandla identifieringsuppgifter är att användningen av kommunikationsnätet och företagshemligheternas konfidentiella läge i första hand bör tryggas genom åtgärder där man överhuvudtaget inte ingriper i kommunikationens identifieringsuppgifter. Sådana metoder är användarhantering och dataskydd samt anvisningar till användarna.

De föreslagna 13 a–13 j § berättigar sammanslutningsabonnenten att behandla identifieringsuppgifter för att utreda olovligt brukande av avgiftsbelagda informationssamhällstjänster och kommunikationsnät eller brukande av en kommunikationstjänst som strider mot anvisningarna. Incidenten eller gärningen skall sannolikt orsaka betydande men eller skada för sammanslutningsabonnenten. I bestämmelserna har man försökt förutse de mest typiska situationerna med användning av kommunikationsnätet eller en kommunikationstjänst som strider mot anvisningarna eller med olovligt brukande. På grund av den snabba kommunikationstekniska utvecklingen är det omöjligt att ge en uttömmande förteckning över alla situationer med olovligt brukande. Det är därför nödvändigt att i bestämmelsen ta in ett omnämnande av behandling av identifieringsuppgifter för att upptäcka annat olovligt brukande av ett kommunikationsnät eller användning av en kommunikationstjänst som strider mot anvisningarna som kan jämföras med de exempelfall som nämns.

Enligt förslaget skall de sammanslutningsabonnenter som är i arbetsgivarställning i förhållande till användarna få rätt att behandla identifieringsuppgifter för att utreda röjande av företagshemligheter. Det misstänkta röjandet av en företagshemlighet skall gälla för sammanslutningsabonnenten eller dennes samarbetspartner centrala företagshemligheter eller resultaten av tekniskt eller annat utvecklingsarbete som är viktiga med tanke på att påbörja eller utöva näringsverksamhet.

Begreppet företagshemlighet enligt de föreslagna 13 a–13 j § sammanfaller med begreppet företagshemlighet i 30 kap. 11 § i strafflagen. Identifieringsuppgifter skall kunna behandlas bara om det är fråga om företagshemligheter eller resultaten av tekniskt eller annat utvecklingsarbete som är centrala med tanke på att påbörja eller utöva näringsverksamhet. I detaljmotiveringen till bestämmelsen har som exempel nämnts bl.a. uppgifter som ger företaget konkurrensfördelar och som inte kan klarläggas på basis av offentliga källor samt uppgifter i fråga om vilkas behandling och skydd näringsidkaren har meddelat särskilda anvisningar och utformat skyddsförfaranden. I den föreslagna bestämmelsen har begreppet företagshemlighet getts en högre relevansnivå än i strafflagen. I förarbetena till strafflagen har det konstaterats att det inte behövs någon närmare avgränsning av innehållet i begreppet företagshemlighet än den avgränsning som tillägnats i lagen, eftersom de mest varierande slags uppgifter inom näringsverksamhet bör

skyddas från konkurrenterna (RP 66/1988 rd, s. 92).

I fråga om företagshemlighet skall behandlingsrätten gälla bara sådana personers identifieringsuppgifter som har tillgång till företagshemligheter på ett sätt som godkänts av sammanslutningsabonnenten. För att identifieringsuppgifterna skall få behandlas förutsätts att det utarbetas särskilda anvisningar för behandlingen av företagshemligheter. Den föreslagna behandlingsrätten blir därmed tillämplig endast i fråga om sammanslutningsabonnenter vilkas normala verksamhet omfattar behandling av företagshemligheter som avses i paragrafen.

Rätten att behandla identifieringsuppgifter i de föreslagna 13 a–13 j § har begränsats till att enbart gälla hot som väsentligt äventyrar sammanslutningsabonnenternas verksamhet. Endast sådana uppgifter som är nödvändiga för att utreda missbruk får tas till behandling. I princip skall identifieringsuppgifter få behandlas med hjälp av en automatisk sökfunktion enligt på förhand fastställda sökkriterier. I en automatisk sökning skall ingen utomstående person få kännedom om identifieringsuppgifterna för meddelanden som hänför sig till enskilda användare av kommunikationsnätet. Syftet med en automatisk sökning är att endast de identifieringsuppgifter som gäller meddelanden som har samband med missbruk skall avskiljas för manuell behandling. Identifieringsuppgifterna för sedvanliga meddelanden skulle härvid inte utsättas för en behandling. En behandling av identifieringsuppgifter som görs enbart med hjälp av en automatisk sökfunktion kan inte anses ingripa i skyddet av konfidentiella meddelanden för dem som idkar kommunikation, om identifieringsuppgifterna för deras meddelanden inte behandlas manuellt av en fysisk person.

Identifieringsuppgifter får i enskilda fall tas till manuell behandling endast om det finns grundad anledning att misstänka missbruk. En grundad anledning är en avvikelse i de tillåtna sökkriterierna som har uppdagats med hjälp av den automatiska sökfunktionen eller en sådan omständighet som fastställs i 13 d §.

Den föreslagna behandlingsrätten riktas endast till de identifieringsuppgifter som ackumuleras i sammanslutningsabonnentens egna system. När skyddade e-post- och nätbankstjänster på Internet har använts skall endast adressen på den tjänst som använts, tidpunkten för användningen och hur länge tjänsten har använts framgå. Om sammanslutningsabonnenterna så önskar kan de förhindra att tjänster som tillhandahålls av utomstående används från sammanslutningsabonnenternas system. Identifieringsuppgifter som gäller telefonitjänster omfattas inte av behandlingsrätten. Behandlingsrätten ger inte rätt att göra ingrepp i meddelandets innehåll.

I samband med behandlingen av propositionen med förslag till lag om dataskydd vid elektronisk kommunikation fäste grundlagsutskottet avseende vid att definitionen av begreppet behandling omfattar ett mycket stort område (bl.a. GrUU 9/2004 rd, s. 3). Utskottet konstaterade dock att problemet med den mycket breda definitionen lindras något av kravet i 8 § 3 mom. att behandlingen måste vara förknippad med ändamålet. Det nämnda momentet begränsar och styr också behandlingen av identifieringsuppgifter med stöd av de föreslagna bestämmelserna. Med hänsyn till det sakkomplex som regleringen gäller kan den föreslagna regleringen på det hela taget anses vara noggrant avgränsad.

Målet med den rätt att behandla identifieringsuppgifter som föreslås i 13 a–13 j § är att trygga att sammanslutningsabonnenternas kommunikationsnät och tjänster används för det planerade ändamålet. Tryggandet av användningen av elektroniska kommunikationsnät och tjänster kan antagligen bedömas som en fördel med förmögenhetsvärde som i dagens kommunikationscentrerade omvärld hänförs till egendomsskyddet enligt 15 § i grundlagen. För de flesta sammanslutningsabonnenter är möjligheten att använda sitt kommunikationsnät och sina kommunikationstjänster en förutsättning för verksamheten. Olovligt brukande eller användning i strid med anvisningarna som orsakar ringa men skall inte berättiga till behandling av identifieringsuppgifter, utan behandlingsrätten är begränsad endast till sådant missbruk som orsakar sammanslutningsabonnenten betydande men. Missbruket skall äventyra, försvåra eller fördröja möjligheterna att använda

kommunikationsnätet eller kommunikationstjänsterna för det planerade ändamålet. I en situation där det är fråga om olovligt brukande av ett nät som hör till sammanslutningsabonnentens tillgångar kan sammanslutningsabonnenten anses ha ett med tanke på de grundläggande fri- och rättigheterna godtagbart intresse att skydda sin egendom mot olovligt brukande.

Syftet med rätten att behandla identifieringsuppgifter i de föreslagna 13 a–13 j § är även att skydda resultaten av tekniskt eller annat utvecklingsarbete samt företagshemligheter som är centrala för näringsverksamheten. Säkerställandet av konfidentialiteten för företagshemligheter och resultaten av utvecklingsarbete vilka är centrala för sammanslutningsabonnentens näringsverksamhet kan likaså anses omfattas av egendomsskyddet enligt 15 § och näringsfriheten enligt 18 § i grundlagen. Obehörigt röjande av för ett företags näringsverksamhet betydande resultat av utvecklingsarbete eller centrala företagshemligheter kan ha mycket långtgående följder för företaget och i extrema fall leda till att verksamheten upphör. Röjande av företagshemligheter kan indirekt påverka hela samhällsekonomins utveckling negativt. Tryggandet av konfidentialiteten vad gäller företagshemligheter kan anses vara ett godtagbart intresse med tanke på de grundläggande fri- och rättigheterna.

De ändrade rättigheter att behandla identifieringsuppgifter som i 13 a–13 j § föreslås för sammanslutningsabonnenterna berättigar inte till att ta reda på innehållet i meddelanden. Behandlingsrätt som inskränks enbart till identifieringsuppgifter som gäller meddelanden utsträcks inte till kärnområdet för sekretess i fråga om konfidentiella meddelanden.

Sammanslutningsabonnenterna har grundad anledning att säkerställa att deras kommunikationsnät och kommunikationstjänster är användbara för deras egna behov. Sammanslutningsabonnenterna har också grundad anledning att säkerställa konfidentialiteten för sina egna och sina samarbetspartners företagshemligheter. Immateriell egendom, såsom produkter och tjänster som håller på att utvecklas, verksamhetssätt som grundar sig på know-how och övriga företagshemligheter, utgör en betydande del av i synnerhet högteknologiska företags egendom.

Enligt den föreslagna regleringen är de primära metoderna för skyddande av kommunikationsnäten och kommunikationstjänsterna samt tryggande av konfidentialiteten för företagshemligheter sådana som inte ingriper i användarnas kommunikation. Sådana metoder är anvisningar för dem som använder näten och åtgärder för att genomföra dataskyddet. I princip skall identifieringsuppgifter få behandlas med hjälp av en automatisk sökfunktion. På basis av sökfunktionens definition skulle endast identifieringsuppgifterna för meddelanden som till sin storlek, typ eller annars är avvikande avskiljas till att behandlas av fysiska personer.

Genom informationsadministrativa åtgärder kan man bara delvis säkerställa att kommunikationsnäten och kommunikationstjänsterna används i enlighet med anvisningarna. För utredning av missbruk förutsätts det likväl också att identifieringsuppgifter behandlas.

Vid utredning av obehörigt röjande av företagshemligheter står också informationsadministrativa metoder till förfogande, såsom kontroll av logguppgifter om användarna, kontroll av uppgifterna om dem som loggar in i system som begränsar åtkomst samt uppgifter som samlats in i samband med tekniskt underhåll av systemen. Av dessa uppgifter framgår vem som har infört vilka uppgifter, i vilken form, när och till vilket medium, såsom hårddisk eller ett flyttbart medium. Flyttbara är t.ex. minnespinnar och cd-skivor. Även uppgifter om annan behandling av materialet, såsom uppgifter om utskrifter, kan sparas. I lagen om dataskydd vid elektronisk kommunikation uppställs inte några begränsningar för behandlingen av sådana uppgifter. Med hjälp av uppgifterna är det å andra sidan bara i undantagsfall möjligt att utreda röjanden av företagshemligheter i deras helhet.

Det föreslås ett flertal skyldigheter för sammanslutningsabonnenterna, vilka säkerställer att identifieringsuppgifterna behandlas lagenligt och att det därmed blir fråga om så obetydliga ingrepp i konfidentialiteten vid kommunikation som möjligt. Genom att begränsa rätten att behandla identifieringsuppgifter har behandlingsrätten inriktats endast

på identifieringsuppgifter för meddelanden som anknyter till missbruk. När identifieringsuppgifter behandlas avslöjas även information om vem som är meddelandets mottagare. Grundlagsutskottet ansåg att den omständighet som nämns i motiveringen till propositionen om integritetsskydd i arbetslivet (RP 162/2003 rd, s. 74) inte var problematisk, dvs. att parterna i och rubriken för avsända och mottagna meddelanden som är avsedda att vara konfidentiella framgår vid särskiljandet av de meddelanden som är avsedda för arbetsgivaren. Enligt denna proposition får sammanslutningabonnenten endast kännedom om uppgifterna för parterna i meddelanden som hänger samman med missbruk som tas upp till manuell behandling.

Användarna skall underrättas om förfaranden och praxis vid behandlingen av identifieringsuppgifter. På basis av den information som ges till användarna kan de själva påverka om informationen om meddelandets mottagare eventuellt utsätts för behandling.

De förfaranden som anknyter till den föreslagna behandlingsrätten och det att dataombudsmannens övervakningsprestationer är avgiftsbelagda styr även sammanslutningsabonnenterna till att utnyttja behandlingsrätten endast när det är nödvändigt.

Den föreslagna rätten att behandla identifieringsuppgifter är nödvändig för att sammanslutningsabonnenterna snabbt skall kunna utreda misstankar om olovligt brukande eller brukande som strider mot anvisningarna för brukandet av sina kommunikationssystem samt olovligt röjande av företagshemligheter. När det gäller företagshemligheter är det möjligt att med hjälp av informationsadministrativa åtgärder preliminärt avgränsa kretsen av misstänkta genom att utreda vem som har behandlat uppgifterna. Det är nödvändigt att behandla identifieringsuppgifter för att få reda på om någon har haft kontakt med t.ex. den part som olovligen delgetts en företagshemlighet. Samtidigt kan sammanslutningsabonnenten avgränsa kretsen av misstänkta och på så sätt trygga fortsatt verksamhet för egen del.

Utan den föreslagna behandlingsrätten kan sammanslutningsabonnenterna inte vidta nödvändiga åtgärder för att upptäcka missbruk i anslutning till företagshemligheter eller för att avvärja eller begränsa skadorna till följd av missbruk. Enligt förslaget skall identifieringsuppgifter endast få behandlas i situationer som kan skada för den privata näringsverksamheten viktiga företagshemligheter eller informationssystemens funktion. Inskränkningarna är således påkallade av ett vägande samhällsbehov samt till sin omfattning proportionella med tanke på de rättsliga intressen som skyddas av de grundläggande fri- och rättigheterna och till betydelsen av de samhällsintressen som ligger till grund för inskränkningarna.

Vid manuell behandling av identifieringsuppgifter tar de som behandlar identifieringsuppgifterna del av dem. I fråga om en sådan behandling skall det alltid upprättas en i 13 f § avsedd redogörelse som undertecknas av dem som tagit del i behandlingen och av vilken framgår grunden för behandlingen och orsaken till att identifieringsuppgifterna har behandlats manuellt. Av redogörelsen skall dessutom framgå tidpunkten för behandlingen, dess varaktighet, vem som har behandlat uppgifterna samt den person som har beslutat om behandlingen. Redogörelsen skall ges till användaren av kommunikationsnätet eller kommunikationstjänsten så snart det är möjligt utan att syftet med behandlingen äventyras. De som deltar i behandlingen av identifieringsuppgifter omfattas av tystnadsplikten och förbudet mot utnyttjande enligt 5 §.

Sammanslutningsabonnenterna skall också årligen till dataombudsmannen lämna en redogörelse för manuell behandling av identifieringsuppgifterna, av vilken det skall framgå hur många gånger identifieringsuppgifterna har behandlats manuellt under ett år och på vilka grunder behandlingen har inletts. Samma information delges företrädarna för personalgrupperna på arbetsplatserna.

Dataombudsmannen, som övervakar den föreslagna behandlingsrätten, handlar under tjänsteansvar. Dataombudsmannen kan enligt 41 § ålägga den som brutit mot lagen att rätta sitt fel eller sin försummelse eller förena åläggandet med vite eller hot om att den försummade åtgärden vidtas på bekostnad av den som saken gäller. Om förseelsen är allvarlig, kan hotet också innebära att verksamheten avbryts helt eller delvis. Dataombuds-

mannen kan även överföra ärenden som han behandlar till förundersökning.

Behandling av identifieringsuppgifter i strid med behandlingsreglerna i 13 a–13 j och 8 § uppfyller brottsrekvisitet för kränkning av kommunikationshemlighet och grov kränkning av kommunikationshemlighet enligt 38 kap. 3 och 4 § i strafflagen. Försummelse att fullgöra de föregripande förpliktelser som avses i 13 b–13 c § och som garanterar tillbörligheten uppfyller rekvisitet för dataskyddsförseelse vid elektronisk kommunikation som avses i 42 § 2 mom. 5 punkten. Genom den föreslagna nya 9 punkten till 42 § 2 mom. skall det bli straffbart som dataskyddsförseelse vid elektronisk kommunikation att underlåta att fullgöra de förpliktelser i efterhand som garanterar att behandlingen av identifieringsuppgifter är lagenlig.

Vid behandlingen av identifieringsuppgifter enligt de föreslagna 13 a–13 j § är det fråga om liknande situationer som vid kameraövervakning och hämtning och öppnande av arbetstagares elektroniska meddelanden enligt lagen om integritetsskydd i arbetslivet. I de föreslagna bestämmelserna tar man inte upp meddelandets innehåll. I fråga om lagen om integritetsskydd i arbetslivet ansåg grundlagsutskottet att ett samarbetsförfarande, myndighetstillsyn och straffbarhet vid missbruk var tillräckliga garantier ur rättssäkerhetsperspektiv (GrUU 10/2004 rd, s. 4 och 5). Garantierna för rättssäkerhet i fråga om den föreslagna behandlingen av identifieringsuppgifter kan antas vara jämförbara med rättssäkerhetsarrangemangen enligt lagen om integritetsskydd i arbetslivet.

De föreslagna ändringarna är förenliga med de internationella människorättsförpliktelser som är bindande för Finland. I Europarådets människorättskonvention och i Europarådets dataskyddskonvention uppställs inte några restriktioner för de föreslagna ändringarna. Reglering i likhet med förslaget är tillåten också enligt artikel 15.1 i EG:s direktiv och integritet och elektronisk kommunikation. Europeiska domstolen för mänskliga rättigheter har tagit ställning till kontroll av kommunikation i sin dom av den 3 april 2007 i målet Copland mot Förenade Kungariket. I fallet hade telefonsamtal, e-post och användningen av Internet kontrollerats i fråga om en anställd vid en offentlig läroanstalt. Lagstiftning som tillåter sådan verksamhet trädde i kraft i Förenade Kungariket efter det att den aktuella kommunikationen hade kontrollerats. Domstolen uteslöt inte direkt möjligheten att det under vissa omständigheter kan vara på ett i Europarådets människorättskonvention avsett sätt nödvändigt att för ett godtagbart mål i ett demokratiskt samhälle övervaka hur anställda använder telefon, e-post och Internet.

När det gäller dataskyddet har grundlagsutskottet konstaterat att i dagsläget kan det betraktas som en risk för den enskildes och samhällets säkerhet i vid bemärkelse, om någon äventyrar datakommunikationen och datasäkerheten (GrUU 9/2004 rd, s. 4). De föreslagna ändringarna av 20 § innebär att dataskyddsbestämmelserna svarar mot dagens behov. Ändringarna är nödvändiga för att teleföretagen, de som tillhandahåller mervärdestjänster och sammanslutningsabonnenterna skall kunna undanröja störningar, trygga kommunikationsmöjligheterna och förebygga betalningsmedelsbedrägerier på ett ändamålsenligt sätt.

Grundlagsutskottet har ansett det vara möjligt att på vissa villkor som gäller noggrann avgränsning ingripa i innehållet i meddelanden för att säkra dataskyddet (GrUU 9/2004 rd, s. 4). Informationssäkra kommunikationsförbindelser är en nödvändig förutsättning för att trygga livsviktiga samhällsfunktioner. Det är nödvändigt att säkerställa tillräckliga verksamhetsmöjligheter med tanke på tryggande av yttrandefriheten, skyddet av liv och hälsa samt egendomsskyddet. När hoten mot dataskyddet ständigt förändras och konsekvenserna av problemen breder ut sig blir det oundvikligt att ompröva effektiviteten för de disponibla åtgärderna.

För att dataskyddet skall kunna skötas effektivt förutsätts det att meddelanden kan analyseras automatiskt. Meddelandena granskas då automatiskt enligt faktorer som slagits fast på förhand, och innehållet i meddelandena röjs inte för utomstående fysiska personer. Största delen av all e-posttrafik antas bestå av s.k. skräppost. Därför bör åtgärder för att genomföra dataskyddet baserade på automatisk databehandling stå till förfogande på ett smidigare sätt än tidigare för att

kommunikationsmöjligheterna för dem som använder kommunikationsnäten skall kunna tryggas.

Enligt det föreslagna 20 § 3 mom. skall innehållet i meddelanden få behandlas även manuellt i de allra grövsta fallen som äventyrar dataskyddet. Avsändaren och mottagaren skall underrättas om den manuella behandlingen, om underrättelsen inte äventyrar genomförandet av dataskyddet. Manuell behandling aktualiseras i samband med skadliga meddelanden som kan innehålla t.ex. ett nytt program eller ett skadligt kommando som den automatiska filtreringen inte identifierar.

Om man inte lyckas avlägsna de skadliga meddelandena, kan de skadliga program de innehåller äventyra kommunikationsmöjligheterna för alla som använder nätet och äventyra konfidentialiteten för data som sparats i datorerna. Meddelanden bör behandlas manuellt för att källan till hotet mot dataskyddet eller angreppets funktion och struktur skall kunna utredas. De skadliga programmens anknytning till strafflagen bör slopas, eftersom t.ex. avsaknad av uppsåtlighet då kan skapa osäkerhet i fråga om huruvida åtgärderna skall vidtas.

En automatisk analys av innehållet i meddelandena skulle inte utsätta informationen i meddelandena för utomstående personers granskning. En automatisk analys är ett effektivt sätt att sköta dataskyddet med så små ingrepp i kommunikationen som möjligt.

De föreslagna ändringarna av dataskyddsbestämmelserna behövs för att det skall vara möjligt att sörja för dataskyddet på ett ändamålsenligt sätt och för att användarnas kommunikationsmöjligheter och dataskydd skall kunna tryggas. Ingrepp i innehållet i meddelanden på något annat sätt än med metoder för automatisk databehandling har avgränsats till situationer där det är uppenbart att ett meddelande innehåller ett skadligt program eller ett skadligt kommando. Det finns inte skäl att föreskriva att det i alla situationer skall krävas en anmälan om granskning av innehållet i ett meddelande. Ett meddelande kan till exempel innehålla en skadlig kod som lamslår datasystem. Underrättelse om kodens skadlighet gagnar inte tryggandet av dataskyddet i näten eller tjänsterna eller tryggandet av mottagarens kommunikationsmöjligheter eller hemligheten för ett förtroligt meddelande. Underrättelsen kan i stället medföra ytterligare problemsituationer.

Den föreslagna ändringen kan bedömas som noggrant avgränsad. Ingripande i innehållet i skadliga meddelanden hänger samman med mycket vägande samhällsintressen. Med tanke på de grundläggande fri- och rättigheterna finns det inget vägande intresse att skydda konfidentialiteten för sådana meddelanden genom vilka man till exempel obehörigen försöker utreda användarnas uppgifter eller ta datorer i besittning för att genomföra angrepp som syftar till blockering av tjänster. Det är möjligt att ingripa i innehållet i ett meddelande endast om man inte kan se till dataskyddet med en automatisk analys. Den föreslagna regleringen står i proportion till det integritetsskydd och det skydd för hemligheten för förtroliga meddelanden som tryggats i grundlagen. Dataskyddspraxis bör tas till behandling i ett samarbetsförfarande, varvid användarna får kännedom om den praxis som sammanslutningsabonnenten tillämpar.

Bedömning av lagstiftningsordningen

Ingripandet i identifieringsuppgifterna för konfidentiella meddelanden med anledning av de föreslagna ändringarna av rättigheterna att behandla identifieringsuppgifter bör bedömas mot bakgrund av de generella villkoren för begränsningar i de grundläggande fri- och rättigheterna. Den föreslagna regleringen sker i lag och är noggrant avgränsad. Det finns ett godtagbart skäl till ingripandet i identifieringsuppgifterna och inskränkningarna utsträcks inte till kärnområdet för hemlighet i fråga om förtroliga meddelanden. Användningen av kommunikationsnät och kommunikationstjänster samt företagshemligheter bör i första hand tryggas genom att man ser till dataskyddet och genom anvisningar till användarna. Med hjälp av automatisk behandling av identifieringsuppgifter och dataadministrativa åtgärder avskiljs endast identifieringsuppgifter för meddelanden som har samband med missbruk för manuell behandling.

Användarna bör underrättas om förfaranden och praxis för behandlingen av identifieringsuppgifter. Information om manuell behandling av identifieringsuppgifter skall alltid ges till användaren, samlade uppgifter skall meddelas personalens representanter. Dataombudsmannen skall övervaka behandlingen av identifieringsuppgifter. Övervakningen grundar sig på anmälningar och dataombudsmannens behörighet. Den föreslagna regleringens rättsskyddsgarantier är ändamålsenliga och bestämmelserna är förenliga med de människorättsförpliktelser som är bindande för Finland.

Grundlagsutskottet har ansett det vara möjligt att man ingriper i meddelandenas innehåll för att säkerställa dataskyddet under vissa villkor som gäller avgränsning. Den föreslagna ändringen av dataskyddsbestämmelsen är noggrant avgränsad och står i proportion till det integritetsskydd och det skydd för hemligheten för förtroliga meddelanden som tryggas i grundlagen.

På de grunder som anförts ovan anser regeringen att lagförslagen kan behandlas i vanlig lagstiftningsordning. Regeringen anser det dock vara viktigt 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) 9, 12–14, 20 och 32 §, i 33 § 3 mom. det inledande stycket, 34 § och 42 § samt

fogas till lagen nya 12 a, 13 a–13 j och 34 a § som följer:

9 §

Behandling av identifieringsuppgifter för att utföra och använda tjänster

Identifieringsuppgifter får behandlas i den utsträckning det är nödvändigt för att utföra och använda nättjänster, kommunikationstjänster eller mervärdestjänster och för att sörja för dataskyddet på det sätt som anges nedan.

Identifieringsuppgifter får behandlas endast av fysiska personer som är anställda hos ett teleföretag, hos den som tillhandahåller mervärdestjänster, hos en sammanslutningsabonnent och hos en juridisk person som är abonnent samt av fysiska personer som handlar för deras räkning och som har i uppdrag att behandla uppgifterna för att de mål som anges särskilt i detta kapitel skall uppnås.

12 §

Behandling för teknisk utveckling

Ett teleföretag och den som tillhandahåller mervärdestjänster får behandla identifieringsuppgifter för att tekniskt utveckla nättjänsterna, kommunikationstjänsterna eller mervärdestjänsterna.

En sammanslutningsabonnent får behandla identifieringsuppgifter för att tekniskt utveckla sitt kommunikationsnät och sina tjänster som anslutits till det.

Innan behandling som avses i 1 och 2 mom. inleds skall abonnenten eller användaren underrättas om vilka identifieringsuppgifter som behandlas och hur länge behandlingen kommer att pågå. Underrättelsen kan vara av engångskaraktär.

12 a §

Behandling för statistisk analys

För statistisk analys har ett teleföretag och den som tillhandahåller mervärdestjänster rätt att med hjälp av automatisk databehandling behandla identifieringsuppgifter om en nättjänst, en kommunikationstjänst eller en mervärdestjänst och en sammanslutningsabonnent identifieringsuppgifter om sitt kommunikationsnät eller om en egen tjänst som anslutits till den, om

1) analysen inte annars kan utföras utan oskäligt besvär, och

2) enskilda fysiska personer inte kan identifieras i analysen.

Vad som bestäms i 1 mom. gäller även en juridisk persons rätt att som abonnent behandla identifieringsuppgifter om sin anslutning och sin terminalutrustning.

13 §

Rätten för teleföretag och den som tillhandahåller mervärdestjänster att behandla uppgifter i fall av missbruk

Ett teleföretag och den som tillhandahåller mervärdestjänster får behandla identifieringsuppgifter för att upptäcka, förhindra och utreda gratisanvändning av en avgiftsbelagd tjänst inom nättjänsten, kommunikationstjänsten eller mervärdestjänsten eller annat

jämförbart missbruk av användningen av en tjänst.

Kommunikationsverket kan utfärda närmare föreskrifter om hur den behandling av identifieringsuppgifter som avses i 1 mom. skall utföras tekniskt.

13 a §

Sammanslutningsabonnenters behandlingsrätt i fall av missbruk

En sammanslutningsabonnent har rätt att behandla identifieringsuppgifter för att utreda olovligt brukande av avgiftsbelagda informationssamhällstjänster eller kommunikationsnät, brukande av kommunikationstjänster som strider mot anvisningarna eller för att utreda röjande av företagshemligheter enligt vad som bestäms i 13 b–13 j §.

Olovligt brukande av kommunikationsnätet eller brukande av kommunikationstjänsten som strider mot anvisningarna är installation av anordningar, program eller tjänster i sammanslutningsabonnentens kommunikationsnät eller annan med detta jämförbar användning av kommunikationsnätet eller kommunikationstjänsten om den står i strid med de anvisningar för användningen som avses i 13 b § 3 mom.

Den rätt som avses i 1 mom. gäller inte identifieringsuppgifter för telefonitjänster i det fasta eller mobila telefonnätet.

13 b §

Sammanslutningsabonnenters omsorgsplikt i fall av missbruk

För att förebygga olovligt brukande av avgiftsbelagda informationssamhällstjänster eller kommunikationsnät eller brukande av kommunikationstjänster som strider mot anvisningarna skall en sammanslutningsabonnent innan behandlingen av identifieringsuppgifter inleds

1) begränsa tillträdet till sitt kommunikationsnät och sin kommunikationstjänst och användningen av dem samt vidta andra åtgärder för att skydda användningen av sitt kommunikationsnät och sin kommunikationstjänst med lämpliga datasäkerhetsåtgärder, och

2) bestämma hurdana meddelanden som får förmedlas och hämtas via sammanslutningsabonnentens kommunikationsnät, hur sammanslutningsabonnentens kommunikationsnät och kommunikationstjänster i övrigt får användas och till hurdana destinationsadresser kommunikation inte får riktas.

För att förebygga röjande av företagshemligheter skall en sammanslutningsabonnent innan behandlingen av identifieringsuppgifter inleds

1) begränsa tillgången till företagshemligheter och vidta andra åtgärder för att skydda uppgifterna på lämpligt sätt, och

2) bestämma på vilket sätt företagshemligheter får överföras, lämnas ut eller på annat sätt behandlas i kommunikationsnät och till hurdana destinationsadresser de personer som har rätt att behandla företagshemligheter inte får skicka meddelanden.

En sammanslutningsabonnent skall för att förebygga missbruk som avses i 1 och 2 mom. ge skriftliga anvisningar till dem som använder kommunikationsnätet eller kommunikationstjänsten.

13 c §

Sammanslutningsabonnenters planerings- och samarbetsplikt i fall av missbruk

En sammanslutningsabonnent skall innan behandling av identifieringsuppgifter enligt 13 a § 1 mom. inleds utse de personer till vilkas uppgifter behandling av identifieringsuppgifter hör eller bestämma de nämnda uppgifterna. Identifieringsuppgifter får behandlas endast av personer som svarar för driften av och informationssäkerheten i sammanslutningsabonnentens kommunikationsnät och kommunikationstjänst och för säkerheten.

Om sammanslutningsabonnenten som arbetsgivare omfattas av samarbetslagstiftningen skall sammanslutningsabonnenten

1) i ett samarbetsförfarande enligt 4 kap. i lagen om samarbete inom företag (334/2007), lagen om samarbete inom statens ämbetsverk och inrättningar (651/1988) och lagen om samarbete mellan kommunala ar-

betsgivare och arbetstagare (449/2007) behandla grunderna och praxisen för de i 13 a–13 j § avsedda förfaranden som skall tillämpas vid behandlingen av identifieringsuppgifter, och

2) på det sätt som föreskrivs i 21 § 2 mom. i lagen om integritetsskydd i arbetslivet (759/2004) informera arbetstagarna eller deras företrädare om beslut som sammanslutningsabonnenten har fattat om behandlingen av identifieringsuppgifter.

Om sammanslutningsabonnenten som arbetsgivare inte omfattas av samarbetslagstiftningen skall denne höra arbetstagarna om de omständigheter som avses i 2 mom. 1 punkten och informera arbetsgivarna om dem enligt vad som bestäms i 21 § 1 och 2 mom. i lagen om integritetsskydd i arbetslivet.

Om sammanslutningsabonnenten inte är arbetsgivare skall denne informera användarna om de förfaranden och den praxis som tillämpas på behandlingen av identifieringsuppgifter enligt 13 a–13 j §.

13 d §

Villkor för sammanslutningsabonnenters behandlingsrätt i fall av missbruk

En sammanslutningsabonnent får behandla identifieringsuppgifter med hjälp av en automatisk sökfunktion som kan basera sig på meddelandenas storlek, deras sammanlagda storlek, meddelandenas typ, antal eller uppkopplingssätt eller de destinationsadresser till vilka meddelandena skickas.

En sammanslutningsabonnent får behandla identifieringsuppgifter manuellt, om det finns grundad anledning att misstänka att kommunikationsnätet, kommunikationstjänsten eller en avgiftsbelagd informationssamhällstjänst används i strid med de anvisningar som avses i 13 b § 3 mom. eller att en företagshemlighet olovligen har röjts för en utomstående och om

1) en avvikelse i kommunikationen har upptäckts med hjälp av den automatiska sökfunktionen,

2) kostnaderna för användningen av en avgiftsbelagd informationssamhällstjänst har stigit ovanligt mycket,

3) det i kommunikationsnätet upptäckts en anordning, ett program eller en tjänst som har installerats obehörigen,

4) en företagshemlighet offentliggörs eller utnyttjas olovligen, eller

5) sammananslutningsabonnenten i ett enskilt fall på basis av annan med 1–4 punkten jämförbar allmänt konstaterbar omständighet har anledning att misstänka att kommunikationsnätet, kommunikationstjänsten eller en avgiftsbelagd informationssamhällstjänst används i strid med de anvisningar som avses i 13 b § 3 mom. eller att en företagshemlighet olovligen har röjts för en utomstående.

Villkor för behandling enligt 1 och 2 mom. är att

1) incidenten eller gärningen sannolikt orsakar betydande men eller skada för sammanslutningsabonnenten, eller

2) det misstänkta röjandet av företagshemlighet avser företagshemligheter som är väsentliga för sammanslutningsabonnentens egen eller dess samarbetsparters näringsverksamhet eller sådana resultat av tekniskt eller annat utvecklingsarbete som sannolikt är av betydelse med tanke på att starta eller utöva näringsverksamhet.

Villkor för behandling enligt 2 mom. är dessutom att uppgifterna är nödvändiga för att reda ut missbruket och de som svarar för det och för att göra slut på olovligt brukande eller brukande i strid med anvisningarna.

13 e §

Särskilda begränsningar av behandlingsrätten i fall av missbruk

Automatisk sökning får inte riktas och identifieringsuppgifter får inte hämtas eller tas till manuell behandling för att få reda på uppgifter enligt 17 kap. 24 § 2 och 3 mom. i rättegångsbalken.

För att utreda röjande av företagshemligheter kan en sammanslutningsabonnent som är arbetsgivare endast behandla sådana användares identifieringsuppgifter, åt vilka sammanslutningsabonnenten har gett eller vilka annars har tillgång till företagshemligheter på ett sådant sätt som sammanslutningsabonnenten har godkänt.

13 f §

Sammanslutningsabonnenters skyldighet att lämna uppgifter till användare i fall av missbruk

Sammanslutningsabonnenten skall lämna en redogörelse för den manuella behandling av identifieringsuppgifter som avses i 13 d § 1 och 2 mom. Av redogörelsen skall framgå

1) grunden och tidpunkten för behandlingen och dess varaktighet,

2) orsaken till att den manuella behandlingen har inletts,

3) behandlarna, samt

4) vem som har beslutat om behandlingen.

Redogörelsen skall undertecknas av de personer som har deltagit i behandlingen. Redogörelsen skall förvaras minst två år efter det att den behandling som avses i 13 d § upphörde.

De som använder det kommunikationsnät eller den kommunikationstjänst som är föremål för behandlingen skall underrättas om den redogörelse som avses i 1 mom. så snart det är möjligt utan att äventyra syftet med behandlingen. Redogörelsen behöver dock inte lämnas till sådana användare vars identifieringsuppgifter har behandlats i form av massbehandling så att behandlaren inte har tagit del av användarnas identifieringsuppgifter. Utan hinder av sekretess som baserar sig på lag eller avtal har användaren rätt att för behandlingen av ett ärende som gäller användarens intressen och rättigheter överlämna redogörelsen och de uppgifter användaren fått i samband med den.

13 g §

Sammanslutningsabonnenters skyldighet att lämna uppgifter till företrädare för arbetstagarna i fall av missbruk

Om sammanslutningsabonnenten är arbetsgivare skall denne årligen till företrädaren för arbetstagarna lämna en redogörelse för den manuella behandling av identifieringsuppgifterna som avses i 13 d § 2 mom. Av redogörelsen skall det framgå på vilka grunder och hur många gånger identifieringsuppgifterna har behandlats under ett år.

Den redogörelse som avses i 1 mom. skall lämnas till en förtroendeman som utsetts med stöd av ett arbets- eller tjänstekollektivavtal eller, om någon sådan inte har utsetts, till ett förtroendeombud enligt 13 kap. 3 § i arbetsavtalslagen (55/2001). Om arbetstagarna inom en personalgrupp inte har utsett någon förtroendeman eller något förtroendeombud, skall redogörelsen lämnas till ett samarbetsombud enligt 8 § i lagen om samarbete inom företag eller 3 § i lagen om samarbete mellan kommunala arbetsgivare och arbetstagare eller till en företrädare enligt 6 § 2 mom. i lagen om samarbete inom statens ämbetsverk och inrättningar. Om inte heller några sådana har utsetts skall redogörelsen lämnas till alla arbetstagare som hör till personalgruppen.

Företrädarna för arbetstagarna och de arbetstagare som avses i 2 mom. skall under hela den tid anställningsförhållandet är i kraft hemlighålla de kränkningar av företagshemligheten och de misstänkta fall av kränkning av företagshemligheten som de tagit del av. I fråga om tystnadsplikten för tjänstemän och andra anställda hos myndigheter gäller vad som bestäms i lagen om offentlighet i myndigheternas verksamhet (621/1999) och någon annanstans i lag. Det som föreskrivs ovan hindrar inte att uppgifter lämnas ut till tillsynsmyndigheterna.

13 h §

Förhandsanmälan och årlig redogörelse till dataombudsmannen i fall av missbruk

En sammanslutningsabonnent skall på förhand meddela dataombudsmannen att behandling av identifieringsuppgifter inleds. Av förhandsanmälan skall framgå

1) grunderna och praxisen för de i 13 d § avsedda förfaranden som skall tillämpas vid behandlingen av identifieringsuppgifter,

2) de uppgifter som avses i 13 c § 1 mom., och

3) hur sammanslutningsabonnenten har fullgjort den informationsskyldighet enligt 13 c § 2 mom. 2 punkten eller 3 mom. som föreligger innan behandlingen inleds.

Sammanslutningsabonnenten skall årligen i efterhand lämna dataombudsmannen en re-

dogörelse för den manuella behandlingen av identifieringsuppgifterna. Av redogörelsen skall framgå på vilka grunder och hur många gånger identifieringsuppgifterna har behandlats under ett år.

13 i §

Sammanslutningsabonnenters rätt att lagra identifieringsuppgifter i fall av missbruk

Bestämmelserna i 13 a–13 h § ger inte sammanslutningsabonnenten rätt att lagra identifieringsuppgifter i registret längre än vad som annars är tillåtet enligt lag.

13 j §

Sammanslutningsabonnenters rätt att lämna ut uppgifter i fall av missbruk

Utan hinder av 8 § 3 mom. har en sammanslutningsabonnent rätt att i samband med polisanmälan eller begäran om utredning i egenskap av målsägande överlämna till polisen för behandling sådana identifieringsuppgifter om meddelanden avseende användare av sammanslutningsabonnentens kommunikationsnät eller kommunikationstjänst som sammanslutningsabonnenten fått i enlighet med 13 a–13 i §.

14 §

Behandling för att upptäcka tekniska fel eller brister

Ett teleföretag, den som tillhandahåller mervärdestjänster och en sammanslutningsabonnent får behandla identifieringsuppgifter, om det behövs för att upptäcka, förhindra eller utreda tekniska fel eller brister vid förmedlingen av kommunikationen.

20 §

Åtgärder för att genomföra dataskyddet

Ett teleföretag, den som tillhandahåller mervärdestjänster och en sammanslutningsabonnent samt de som handlar för dessas räkning har rätt att vidta nödvändiga åtgärder för att handha dataskyddet enligt 2 mom.

1) för att upptäcka, förhindra och utreda åtgärder som kan inverka menligt på dataskyddet i kommunikationsnäten eller på de tjänster som anslutits till dem och för att göra störningarna föremål för förundersökning,

2) för att trygga kommunikationsmöjligheterna för den som sänder eller tar emot ett meddelande, eller

3) för att förhindra förberedelse till betalningsmedelsbedrägerier enligt 37 kap. 11 § i strafflagen (39/1889), vilka planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna.

De åtgärder som avses i 1 mom. kan omfatta

1) en automatisk analys av innehållet i meddelanden,

2) automatiskt förhindrande eller automatisk begränsning av förmedling och mottagande av meddelanden,

3) automatiskt avlägsnande av sådana skadliga datorprogram ur meddelandena som kan äventyra dataskyddet, samt

4) andra jämförbara åtgärder av teknisk natur.

Om det på basis av typen av meddelande, meddelandets form eller någon annan omständighet är uppenbart att ett meddelande innehåller ett skadligt datorprogram eller ett skadligt kommando och uppnåendet av målen enligt 1 mom. inte kan säkerställas genom en automatisk analys av innehållet, får innehållet i det enskilda meddelandet behandlas manuellt. Avsändaren och mottagaren av ett meddelande skall underrättas om den manuella behandlingen av innehållet i meddelandet, om det är sannolikt att underrättelsen inte äventyrar uppnåendet av målen enligt 1 mom.

Åtgärderna enligt denna paragraf skall utföras omsorgsfullt och de skall stå i rätt proportion till den störning som skall avvärjas. Åtgärderna skall utföras utan att yttrandefriheten eller skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än nödvändigt med tanke på säkerställandet av möjligheterna att uppnå målen enligt 1 mom. Åtgärderna skall avbrytas, om det inte

längre finns i denna paragraf nämnda förutsättningar för att vidta dem.

Kommunikationsverket kan meddela teleföretagen och dem som tillhandahåller mervärdestjänster närmare föreskrifter om hur åtgärderna enligt denna paragraf skall genomföras tekniskt.

32 §

Dataombudsmannens uppgifter

Dataombudsmannens uppgift är att övervaka

1) i 13 a–13 j § avsedd behandling av identifieringsuppgifter som en sammanslutningsabonnent genomför,

2) i 4 kap. avsedd behandling av lokaliseringsuppgifter,

3) tillämpningen av bestämmelserna om telefonkataloger, abonnentkataloger och nummerupplysning som avses i 25 §,

4) tillämpningen av bestämmelserna om direktmarknadsföring i 7 kap.,

5) bestämmelserna om rätt att få uppgifter och om tystnadsplikt i 9 kap., till den del det är fråga om lokaliseringsuppgifter.

För de tillsynsuppgifter som avses i 1 mom. 1 punkten får en avgift tas ut av sammanslutningsabonnenten. Beslut om avgiftsbelagda åtgärder och avgiftens storlek fattas genom förordning av justitie-ministeriet enligt de grunder som föreskrivs i lagen om grunderna för avgifter till staten (150/1992).

33 §

Styrnings- och övervakningsmyndigheternas rätt att få uppgifter

— — — — — — — — — — — — — —

För att utföra sina i denna lag föreskrivna uppgifter har Kommunikationsverket och dataombudsmannen rätt att få identifierings- och lokaliseringsuppgifter och meddelanden, om det behövs för att övervaka bestämmelserna om behandling, användning av i 7 § avsedda uppgifter eller direktmarknadsföring eller för att utreda betydande kränkningar av och hot mot dataskyddet. Dessutom krävs det att det enligt Kommunikationsverkets eller dataombudsmannens bedömning är skäl att misstänka att något av följande rekvisit är uppfyllda:

— — — — — — — — — — — — — —

34 §

Tillsynsmyndigheternas tystnadsplikt

Uppgifter som Kommunikationsverket och dataombudsmannen med stöd av 33 § 3 mom. erhållit om konfidentiella meddelanden, identifieringsuppgifter och lokaliseringsuppgifter samt uppgifter som dataombudsmannen erhållit med stöd av 13 h § skall hållas hemliga.

I övrigt föreskrivs det om sekretess för tillsynsmyndigheternas uppgifter i lagen om offentlighet i myndigheternas verksamhet.

34 a §

Utlämnande av tillsynsmyndigheternas uppgifter

Utan hinder av någon annan än den tystnadsplikt som föreskrivs i 34 § 1 mom. eller utan hinder av andra begränsningar som gäller utlämnande av uppgifter har Kommunikationsverket och dataombudsmannen rätt att till kommunikationsministeriet lämna ut i 33 § 1 mom. avsedda uppgifter som de erhållit vid utförandet av i denna lag föreskrivna uppgifter.

Utan hinder av den tystnadsplikt som föreskrivs i 34 § 1 mom. eller utan hinder av andra begränsningar som gäller utlämnande av uppgifter har Kommunikationsverket rätt att till de teleföretag, dem som tillhandahåller mervärdestjänster och de sammanslutningsabonnenter som har utnyttjats vid kränkning av dataskydd, som har blivit föremål för sådan kränkning eller som sannolikt kan utsättas för kränkning av dataskydd lämna ut identifieringsuppgifter som verket erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskydd, om det enligt Kommunikationsverkets be-

dömning finns skäl att misstänka att något av de rekvisit som anges i 33 § 3 mom. 1–10 punkten har blivit uppfyllt.

Utan hinder av den tystnadsplikt som föreskrivs i 34 § 1 mom. har Kommunikationsverket rätt att till sådana myndigheter eller andra instanser som är verksamma i andra stater och som har till uppgift att förebygga eller utreda kränkningar av dataskydd riktade mot kommunikationsnät och kommunikationstjänster lämna ut identifieringsuppgifter som verket erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskydd.

Kommunikationsverket har rätt att lämna ut i 2 och 3 mom. avsedda identifieringsuppgifter endast i den omfattning som behövs för att förebygga och utreda kränkningar av dataskydd. Utlämnandet av uppgifter får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt.

42 §

Straffbestämmelser

Bestämmelser om straff för kränkning av kommunikationshemlighet och för grov kränkning av kommunikationshemlighet finns i 38 kap. 3 och 4 § i strafflagen samt för dataintrång i 38 kap. 8 § i strafflagen. Straff för brott mot i 5 § föreskriven tystnadsplikt utdöms enligt 38 kap. 1 eller 2 § i strafflagen, om gärningen inte utgör brott enligt 40 kap. 5 § i strafflagen eller om inte strängare straff föreskrivs någon annanstans. Straff för brott mot i 13 d § 3 mom. föreskriven tystnadsplikt utdöms enligt 38 kap. 2 § 2 mom. i strafflagen, om inte strängare straff för gärningen föreskrivs någon annanstans än i 38 kap. 1 § i strafflagen.

Den som uppsåtligen

1) bryter mot det i 6 § 2 mom. föreskrivna förbudet mot innehav, import, tillverkning eller distribution av system för avkodning av det tekniska skyddet vid elektronisk kommunikation eller av en del av ett sådant system,

2) försummar de förpliktelser som föreskrivs i 7 §,

3) försummar den i 19 § föreskrivna skyldigheten att handha dataskyddet för sina tjänster eller för identifierings- och lokaliseringsuppgifter,

4) försummar den i 21 § 2 mom. eller 35 § 4 mom. föreskrivna anmälningsplikten,

5) behandlar identifierings- eller lokaliseringsuppgifter i strid med bestämmelserna i 3 och 4 kap.,

6) underlåter att iaktta vad som i 24 § bestäms om specificering av en räkning,

7) underlåter att iaktta vad som i 25 § bestäms om behandling av personuppgifter som ingår i en telefonkatalog eller i en annan abonnentkatalog, om anmälning till abonnenten om ändamålet med och användningen av katalogen, om avlägsnande och rättelse av uppgifter, om förbud eller om juridiska personers rättigheter,

8) bedriver direktmarknadsföring i strid med bestämmelserna i 7 kap., eller

9) underlåter att iaktta vad som i 13 f–13 h § bestäms om att utarbeta en redogörelse eller förhandsanmälan och att lämna den till användarna, arbetstagarnas företrädare eller dataombudsmannen,

skall, om inte strängare straff för gärningen föreskrivs någon annanstans i lag, för dataskyddsförseelse vid elektronisk kommunikation dömas till böter.

Straff döms inte ut om förseelsen är ringa.

Denna lag träder i kraft den 20 .

2.

Lag

om ändring av 2 och 21 § i lagen om integritetsskydd i arbetslivet

I enlighet med riksdagens beslut

ändras i lagen av den 13 augusti 2004 om integritetsskydd i arbetslivet (759/2004) 2 § 3 mom. och 21 § 1 mom., av dem det sist nämnda sådant det lyder i lag 457/2007, som följer:

2 §	21 §
Tillämpningsområde	*Samarbete vid ordnande av teknisk övervakning och användning av datanät*
— — — — — — — — — — — — — — —	
Om arbetsgivarens rätt att i egenskap av abonnent för utredning av avgiftsskyldigheten få identifieringsuppgifter om en anslutning som ställts till arbetstagarens förfogande och om rätten att behandla identifieringsuppgifter som gäller arbetstagarens elektroniska kommunikation i situationer av olovligt brukande av ett kommunikationsnät eller brukande av en kommunikationstjänst som strider mot anvisningarna och för att skydda företagshemligheter föreskrivs i lagen om dataskydd vid elektronisk kommunikation (516/2004). Vad som i nämnda lag bestäms om användare av lokaliseringstjänster tillämpas på arbetstagare till vars förfogande arbetsgivaren har ställt en lokaliseringstjänst. På behandling av personuppgifter tillämpas personuppgiftslagen (523/1999), om inte något annat bestäms i denna lag.	Syftet med kameraövervakning, passerkontroll och annan övervakning med tekniska metoder av arbetstagarna, ibruktagandet av dem och de metoder som används i övervakningen samt användningen av elektronisk post och andra datanät samt behandlingen av uppgifter som gäller en arbetstagares elektroniska post och annan elektronisk kommunikation omfattas av samarbetsförfarandet enligt lagen om samarbete inom företag, lagen om samarbete inom statens ämbetsverk och inrättningar samt lagen om samarbete mellan kommunala arbetsgivare och arbetstagare. I andra företag och offentligrättsliga sammanslutningar än sådana som omfattas av samarbetslagstiftningen skall arbetsgivaren före beslutsfattandet bereda arbetstagarna eller deras representanter tillfälle att bli hörda i de angelägenheter som nämns ovan.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .

3.

Lag

om ändring av 19 § i lagen om samarbete inom företag

I enlighet med riksdagens beslut

ändras i lagen av den 30 mars 2007 om samarbete inom företag (334/2007) 19 § 4 punkten som följer:

19 §	4) principerna för användningen av elektronisk post och datanät och behandlingen av uppgifter som gäller en arbetstagares elektroniska post och annan elektronisk kommunikation,
Behandling av planer, principer och praxis som grundar sig på annan lagstiftning	— — — — — — — — — — — — — — — — — — — —
Vid samarbetsförhandlingar skall behandlas	Denna lag träder i kraft den 20 .
— — — — — — — — — — — — — — — — — — — —	

4.

Lag

om ändring av 7 § i lagen om samarbete inom statens ämbetsverk och inrättningar

I enlighet med riksdagens beslut

ändras i lagen av den 1 juli 1988 om samarbete inom statens ämbetsverk och inrättningar (651/1988) 7 § 11 a-punkten, sådan den lyder i lag 762/2004, som följer:

7 §

Ärenden som omfattas av samarbetsförfarandet

Samarbetsförfarandet omfattar

— — — — — — — — — — — — — — —

11 a) syftet med, ibruktagandet av och metoderna för kameraövervakning, passerkontroll och annan övervakning med tekniska metoder av personalen, användningen av elektronisk post och datanät samt behandlingen av uppgifter som gäller en tjänstemans och arbetstagares elektroniska post och annan elektronisk kommunikation,

— — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

Helsingfors den 28 mars 2008

Republikens President

TARJA HALONEN

Kommunikationsminister *Suvi Lindén*

Bilaga
Parallelltext

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) 9, 12–14, 20 och 32 §, i 33 § 3 mom. det inledande stycket, 34 § och 42 § samt

fogas till lagen nya 12 a, 13 a–13 j och 34 a § som följer:

Gällande lydelse	*Föreslagen lydelse*
9 §	9 §
Behandling av identifieringsuppgifter för att utföra och använda tjänster	*Behandling av identifieringsuppgifter för att utföra och använda tjänster*
Identifieringsuppgifter får 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.	Identifieringsuppgifter får behandlas i den utsträckning det är nödvändigt för att utföra och använda nättjänster, kommunikationstjänster eller mervärdestjänster och för att sörja för dataskyddet *på det sätt som anges nedan.*
Identifieringsuppgifter får behandlas endast av fysiska personer som är anställda hos ett teleföretag, hos den som tillhandahåller mervärdestjänster eller hos en sammanslutningsabonnent samt av fysiska personer som handlar för deras räkning och vilkas uppgift är att behandla information för att uppnå de mål som anges särskilt i 1 mom. och i 10–14 §.	Identifieringsuppgifter får behandlas endast av fysiska personer som är anställda hos ett teleföretag, hos den som tillhandahåller mervärdestjänster, hos en sammanslutningsabonnent *och hos en juridisk person som är abonnent samt av fysiska personer som handlar för deras räkning och som skall behandla uppgifterna för att de mål som anges särskilt i detta kapitel skall uppnås.*
12 §	12 §
Behandling för teknisk utveckling	*Behandling för teknisk utveckling*
Ett teleföretag och den som tillhandahåller mervärdestjänster får behandla identifieringsuppgifter för att tekniskt utveckla tjänsterna.	Ett teleföretag och den som tillhandahåller mervärdestjänster får behandla identifieringsuppgifter för att tekniskt utveckla *nättjänsterna, kommunikationstjänsterna eller mervärdestjänsterna.*
Innan den i 1 mom. avsedda behandlingen påbörjas skall teleföretaget och den som tillhandahåller mervärdestjänster meddela abonnenten eller användaren vilka identifieringsuppgifter som behandlas och hur länge be-	*En sammanslutningsabonnent får behandla identifieringsuppgifter för att tekniskt utveckla sitt kommunikationsnät och sina tjänster som anslutits till det.*

Gällande lydelse

handlingen räcker.

En sammanslutningsabonnent får behandla identifieringsuppgifter för att tekniskt utveckla sin egen verksamhet.

13 §

Behandling i fall av missbruk

Ett teleföretag, den som tillhandahåller mervärdestjänster och en sammanslutningsabonnent får behandla identifieringsuppgifter, om det är behövligt för att upptäcka, förhindra och utreda missbruk som omfattar gratisanvändning av enstaka avgiftsbelagda tjänster eller av andra med dem jämförbara tjänster inom nättjänsten, kommunikationstjänsten eller mervärdestjänsten samt för att göra missbruket föremål för förundersökning.

Föreslagen lydelse

Innan den i 1 och 2 mom. avsedda behandlingen inleds skall abonnenten eller användaren underrättas om vilka identifieringsuppgifter som behandlas och hur länge behandlingen räcker. Underrättelsen kan vara av engångskaraktär.

12 a §

Behandling för statistisk analys

För statistisk analys har ett teleföretag och den som tillhandahåller mervärdestjänster rätt att med hjälp av automatisk databehandling behandla identifieringsuppgifter om en nättjänst, en kommunikationstjänst eller en mervärdestjänst och en sammanslutningsabonnent identifieringsuppgifter om sitt kommunikationsnät eller om en egen tjänst som anslutits till den, om

1) analysen inte annars kan utföras utan oskäligt besvär, och

2) enskilda fysiska personer inte kan identifieras i analysen.

Vad som bestäms i 1 mom. gäller även en juridisk persons rätt att som abonnent behandla identifieringsuppgifter om sin anslutning och sin terminalutrustning.

13 §

Rätten för teleföretag och den som tillhandahåller mervärdestjänster att behandla uppgifter i fall av missbruk

Ett teleföretag och den som tillhandahåller mervärdestjänster får behandla identifieringsuppgifter för att upptäcka, förhindra och utreda gratisanvändning av en avgiftsbelagd tjänst inom nättjänsten, kommunikationstjänsten eller mervärdestjänsten *eller annat jämförbart missbruk av användningen av en tjänst.*

Kommunikationsverket kan utfärda närmare föreskrifter om hur den behandling av identifieringsuppgifter som avses i 1 mom. skall utföras tekniskt.

Gällande lydelse

Föreslagen lydelse

13 a §

Sammanslutningsabonnenters behandlingsrätt i fall av missbruk

En sammanslutningsabonnent har rätt att behandla identifieringsuppgifter för att utreda olovligt brukande av avgiftsbelagda informationssamhällstjänster eller kommunikationsnät, brukande av kommunikationstjänster som strider mot anvisningarna eller för att utreda röjande av företagshemligheter enligt vad som bestäms i 13 b–13 j §.

Olovligt brukande av kommunikationsnätet eller brukande av kommunikationstjänsten som strider mot anvisningarna är installation av anordningar, program eller tjänster i sammanslutningsabonnentens kommunikationsnät eller annan med detta jämförbar användning av kommunikationsnätet eller kommunikationstjänsten om den står i strid med de anvisningar för användningen som avses i 13 b § 3 mom.

Den rätt som avses i 1 mom. gäller inte identifieringsuppgifter för telefonitjänster i det fasta eller mobila telefonnätet.

13 b §

Sammanslutningsabonnenters omsorgsplikt i fall av missbruk

För att förebygga olovligt brukande av avgiftsbelagda informationssamhällstjänster eller kommunikationsnät eller brukande av kommunikationstjänster som strider mot anvisningarna skall en sammanslutningsabonnent innan behandlingen av identifieringsuppgifter inleds

1) begränsa tillträdet till sitt kommunikationsnät och sin kommunikationstjänst och användningen av dem samt vidta andra åtgärder för att skydda användningen av sitt kommunikationsnät och sin kommunikationstjänst med lämpliga datasäkerhetsåtgärder, och

2) bestämma hurdana meddelanden som får förmedlas och hämtas via sammanslutningsabonnentens kommunikationsnät, hur sammanslutningsabonnentens kommunikationsnät och kommunikationstjänster i övrigt får användas och till hurdana destinations-

Gällande lydelse *Föreslagen lydelse*

adresser kommunikation inte får riktas.

För att förebygga röjande av företagshemligheter skall en sammanslutningsabonnent innan behandlingen av identifieringsuppgifter inleds

1) begränsa tillgången till företagshemligheter och vidta andra åtgärder för att skydda uppgifterna på lämpligt sätt, och

2) bestämma på vilket sätt företagshemligheter får överföras, lämnas ut eller på annat sätt behandlas i kommunikationsnät och till hurdana destinationsadresser de personer som har rätt att behandla företagshemligheter inte får skicka meddelanden.

En sammanslutningsabonnent skall för att förebygga missbruk som avses i 1 och 2 mom. ge skriftliga anvisningar till dem som använder kommunikationsnätet eller kommunikationstjänsten.

13 c §

Sammanslutningsabonnenters planerings- och samarbetsplikt i fall av missbruk

En sammanslutningsabonnent skall innan behandling av identifieringsuppgifter enligt 13 a § 1 mom. inleds utse de personer till vilkas uppgifter behandling av identifieringsuppgifter hör eller bestämma de nämnda uppgifterna. Identifieringsuppgifter får behandlas endast av personer som svarar för driften av och informationssäkerheten i sammanslutningsabonnentens kommunikationsnät och kommunikationstjänst och för säkerheten.

Om sammanslutningsabonnenten som arbetsgivare omfattas av samarbetslagstiftningen skall sammanslutningsabonnenten

1) i ett samarbetsförfarande enligt 4 kap. i lagen om samarbete inom företag (334/2007), lagen om samarbete inom statens ämbetsverk och inrättningar (651/1988) och lagen om samarbete mellan kommunala arbetsgivare och arbetstagare (449/2007) behandla grunderna och praxisen för de i 13 a–13 j § avsedda förfaranden som skall tillämpas vid behandlingen av identifieringsuppgifter, och

2) på det sätt som föreskrivs i 21 § 2 mom. i lagen om integritetsskydd i arbetslivet

Gällande lydelse | *Föreslagen lydelse*

(759/2004) informera arbetstagarna eller deras företrädare om beslut som sammanslutningsabonnenten har fattat om behandlingen av identifieringsuppgifter.

Om sammanslutningsabonnenten som arbetsgivare inte omfattas av samarbetslagstiftningen skall denne höra arbetstagarna om de omständigheter som avses i 2 mom. 1 punkten och informera arbetsgivarna om dem enligt vad som bestäms i 21 § 1 och 2 mom. i lagen om integritetsskydd i arbetslivet.

Om sammanslutningsabonnenten inte är arbetsgivare skall denne informera användarna om de förfaranden och den praxis som tillämpas på behandlingen av identifieringsuppgifter enligt 13 a–13 j §.

13 d §

Villkor för sammanslutningsabonnenters behandlingsrätt i fall av missbruk

En sammanslutningsabonnent får behandla identifieringsuppgifter med hjälp av en automatisk sökfunktion som kan basera sig på meddelandenas storlek, deras sammanlagda storlek, meddelandenas typ, antal eller uppkopplingssätt eller de destinationsadresser till vilka meddelandena skickas.

En sammanslutningsabonnent får behandla identifieringsuppgifter manuellt om det finns grundad anledning att misstänka att kommunikationsnätet, kommunikationstjänsten eller en avgiftsbelagd informationssamhällstjänst används i strid med de anvisningar som avses i 13 b § 3 mom. eller att en företagshemlighet olovligen har röjts för en utomstående och om

1) en avvikelse i kommunikationen har upptäckts med hjälp av den automatiska sökfunktionen,

2) kostnaderna för användningen av en avgiftsbelagd informationssamhällstjänst har stigit ovanligt mycket,

3) det i kommunikationsnätet upptäckts en anordning, ett program eller en tjänst som har installerats obehörigen,

4) en företagshemlighet offentliggörs eller utnyttjas olovligen, eller

Gällande lydelse *Föreslagen lydelse*

5) sammananslutningsabonnenten i ett enskilt fall på basis av annan med 1–4 punkten jämförbar allmänt konstaterbar omständighet har anledning att misstänka att kommunikationsnätet, kommunikationstjänsten eller en avgiftsbelagd informationssamhällstjänst används i strid med de anvisningar som avses i 13 b § 3 mom. eller att en företagshemlighet olovligen har röjts för en utomstående.

Villkor för behandling enligt 1 och 2 mom. är att

1) incidenten eller gärningen sannolikt orsakar betydande men eller skada för sammanslutningsabonnenten, eller

2) det misstänkta röjandet av företagshemlighet avser företagshemligheter som är väsentliga för sammanslutningsabonnentens egen eller dess samarbetsparters näringsverksamhet eller sådana resultat av tekniskt eller annat utvecklingsarbete som sannolikt är av betydelse med tanke på att starta eller utöva näringsverksamhet.

Villkor för behandling enligt 2 mom. är dessutom att uppgifterna är nödvändiga för att reda ut missbruket och de som svarar för det och för att göra slut på olovligt brukande eller brukande i strid med anvisningarna.

13 e §

Särskilda begränsningar av behandlingsrätten i fall av missbruk

Automatisk sökning får inte riktas och identifieringsuppgifter får inte hämtas eller tas till manuell behandling för att få reda på uppgifter enligt 17 kap. 24 § 2 och 3 mom. i rättegångsbalken.

För att utreda röjande av företagshemligheter kan en sammanslutningsabonnent som är arbetsgivare endast behandla sådana användares identifieringsuppgifter, åt vilka sammanslutningsabonnenten har gett eller vilka annars har tillgång till företagshemligheter på ett sådant sätt som sammanslutningsabonnenten har godkänt.

Gällande lydelse

Föreslagen lydelse

13 f §

Sammanslutningsabonnenters skyldighet att lämna uppgifter till användare i fall av missbruk

Sammanslutningsabonnenten skall lämna en redogörelse för den manuella behandling av identifieringsuppgifter som avses i 13 d § 1 och 2 mom. Av redogörelsen skall framgå

1) grunden och tidpunkten för behandlingen och dess varaktighet,

2) orsaken till att den manuella behandlingen har inletts,

3) behandlarna, samt

4) vem som har beslutat om behandlingen.

Redogörelsen skall undertecknas av de personer som har deltagit i behandlingen. Redogörelsen skall förvaras minst två år efter det att den behandling som avses i 13 d § upphörde.

De som använder det kommunikationsnät eller den kommunikationstjänst som är föremål för behandlingen skall underrättas om den redogörelse som avses i 1 mom. så snart det är möjligt utan att äventyra syftet med behandlingen. Redogörelsen behöver dock däremot inte lämnas till sådana användare vars identifieringsuppgifter har behandlats i form av massbehandling så att behandlaren inte har tagit del av användarnas identifieringsuppgifter. Utan hinder av sekretess som baserar sig på lag eller avtal har användaren rätt att för behandlingen av ett ärende som gäller användarens intressen och rättigheter överlämna redogörelsen och de uppgifter användaren fått i samband med den.

13 g §

Sammanslutningsabonnenters skyldighet att lämna uppgifter till företrädare för arbetstagarna i fall av missbruk

Om sammanslutningsabonnenten är arbetsgivare skall denne årligen till företrädaren för arbetstagarna lämna en redogörelse för den manuella behandling av identifieringsuppgifterna som avses i 13 d § 2 mom. Av redogörelsen skall det framgå på vilka grunder och hur många gånger identifieringsuppgifterna har behandlats under ett år.

Gällande lydelse *Föreslagen lydelse*

Den redogörelse som avses i 1 mom. skall lämnas till en förtroendeman som utsetts med stöd av ett arbets- eller tjänstekollektivavtal eller, om någon sådan inte har utsetts, till ett förtroendeombud enligt 13 kap. 3 § i arbetsavtalslagen (55/2001). Om arbetstagarna inom en personalgrupp inte har utsett någon förtroendeman eller något förtroendeombud, skall redogörelsen lämnas till ett samarbetsombud enligt 8 § i lagen om samarbete inom företag eller 3 § i lagen om samarbete mellan kommunala arbetsgivare och arbetstagare eller till en företrädare enligt 6 § 2 mom. i lagen om samarbete inom statens ämbetsverk och inrättningar. Om inte heller några sådana har utsetts skall redogörelsen lämnas till alla arbetstagare som hör till personalgruppen.

Företrädarna för arbetstagarna och de arbetstagare som avses i 2 mom. skall under hela den tid anställningsförhållandet är i kraft hemlighålla de kränkningar av företagshemligheten och de misstänkta fall av kränkning av företagshemligheten som de tagit del av. I fråga om tystnadsplikten för tjänstemän och andra anställda hos myndigheter gäller vad som bestäms i lagen om offentlighet i myndigheternas verksamhet (621/1999) och någon annanstans i lag. Det som föreskrivs ovan hindrar inte att uppgifter lämnas ut till tillsynsmyndigheterna.

13 h §

Förhandsanmälan och årlig redogörelse till dataombudsmannen i fall av missbruk

En sammanslutningsabonnent skall på förhand meddela dataombudsmannen att behandling av identifieringsuppgifter inleds. Av förhandsanmälan skall framgå

1) grunderna och praxisen för de i 13 d § avsedda förfaranden som skall tillämpas vid behandlingen av identifieringsuppgifter,

2) de uppgifter som avses i 13 c § 1 mom., och

3) hur sammanslutningsabonnenten har fullgjort den informationsskyldighet enligt 13 c § 2 mom. 2 punkten eller 3 mom. som föreligger innan behandlingen inleds.

Sammanslutningsabonnenten skall årligen i efterhand lämna dataombudsmannen en re-

Gällande lydelse	*Föreslagen lydelse*
	dogörelse för den manuella behandlingen av identifieringsuppgifterna. Av redogörelsen skall framgå på vilka grunder och hur många gånger identifieringsuppgifterna har behandlats under ett år.
	13 i §
	Sammanslutningsabonnenters rätt att lagra identifieringsuppgifter i fall av missbruk
	Bestämmelserna i 13 a–13 h § ger inte sammanslutningsabonnenten rätt att lagra identifieringsuppgifter i registret längre än vad som annars är tillåtet enligt lag.
	13 j §
	Sammanslutningsabonnenters rätt att lämna ut uppgifter i fall av missbruk
	Utan hinder av 8 § 3 mom. har en sammanslutningsabonnent rätt att i samband med polisanmälan eller begäran om utredning i egenskap av målsägande överlämna till polisen för behandling sådana identifieringsuppgifter om meddelanden avseende användare av sammanslutningsabonnentens kommunikationsnät eller kommunikationstjänst som sammanslutningsabonnenten fått i enlighet med 13 a–13 i §.
14 §	14 §
Behandling för att upptäcka tekniska fel eller brister	*Behandling för att upptäcka tekniska fel eller brister*
Ett teleföretag, den som tillhandahåller mervärdestjänster och en sammanslutningsabonnent får behandla identifieringsuppgifter, om det är behövligt för att upptäcka tekniska fel eller brister vid förmedlingen av kommunikationen.	Ett teleföretag, den som tillhandahåller mervärdestjänster och en sammanslutningsabonnent får behandla identifieringsuppgifter, *om det behövs* för att upptäcka, *förhindra eller utreda* tekniska fel eller brister vid förmedlingen av kommunikationen.
20 §	20 §
Åtgärder för att genomföra dataskyddet	*Åtgärder för att genomföra dataskyddet*
För att avvärja kränkningar och eliminera störningar av dataskyddet har ett teleföretag, den som tillhandahåller mervärdestjänster eller en sammanslutningsabonnent samt de som	*Ett teleföretag, den som tillhandahåller mervärdestjänster och en sammanslutningsabonnent samt de som handlar för dessas räkning har rätt att vidta nödvändiga åtgär-*

Gällande lydelse	*Föreslagen lydelse*
verkar för dessas räkning rätt att vidta nödvändiga åtgärder för att säkra i 19 § avsett dataskydd genom att	*der för att handha dataskyddet enligt 2 mom.*
1) hindra förmedling och mottagande av elektronisk post, textmeddelanden och andra motsvarande meddelanden,	1) *för att upptäcka, förhindra och utreda åtgärder som kan inverka menligt på dataskyddet i kommunikationsnäten eller på de tjänster som anslutits till dem och för att göra störningarna föremål för förundersökning,*
2) ur meddelandena avlägsna skadliga program som äventyrar dataskyddet, samt genom att	2) *för att trygga kommunikationsmöjligheterna för den som sänder eller tar emot ett meddelande, eller*
3) vidta andra jämförbara åtgärder av teknisk natur.	*3) för att förhindra förberedelse till betalningsmedelsbedrägerier enligt 37 kap. 11 § i strafflagen (39/1889), vilka planeras bli genomförda i omfattande utsträckning via kommunikationstjänsterna.*
De åtgärder som avses i 1 mom. får vidtas endast om de är nödvändiga för att trygga nät- eller kommunikationstjänsterna, eller kommunikationsmöjligheterna för den som mottar ett meddelande.	De åtgärder som avses i 1 mom. *kan omfatta*
Ingrepp får göras i meddelandets innehåll endast med tekniska medel för att kontrollera och avlägsna meddelandet, om det finns sannolika skäl att misstänka att meddelandet innehåller ett sådant dataprogram eller en sådan serie av programinstruktioner som avses i 34 kap. 9 a § 1 punkten i strafflagen (39/1889) eller att meddelandet används för sådant störande av post- och teletrafik som avses i 38 kap. 5 § i strafflagen.	*1) en automatisk analys av innehållet i meddelanden,* *2) automatiskt förhindrande eller automatisk begränsning av förmedling och mottagande av meddelanden,* *3) automatiskt avlägsnande av sådana skadliga datorprogram ur meddelandena som kan äventyra dataskyddet, samt* *4) andra jämförbara åtgärder av teknisk natur.* *Om det på basis av typen av meddelande, meddelandets form eller någon annan omständighet är uppenbart att ett meddelande innehåller ett skadligt datorprogram eller ett skadligt kommando och uppnåendet av målen enligt 1 mom. inte kan säkerställas genom en automatisk analys av innehållet, får innehållet i det enskilda meddelandet behandlas manuellt. Avsändaren och mottagaren av ett meddelande skall underrättas om den manuella behandlingen av innehållet i meddelandet, om det är sannolikt att underrättelsen inte äventyrar uppnåendet av målen enligt 1 mom.*
Åtgärderna skall utföras omsorgsfullt och anpassas till den störning som skall avvärjas. Åtgärderna skall utföras utan att yttrandefriheten eller skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än nödvändigt med tanke på säkerställandet av nättjänsterna eller kommunikationstjänsterna eller kommunikationsmöjligheterna för mottagaren av ett meddelande. Åtgärderna	*Åtgärderna enligt denna paragraf skall utföras omsorgsfullt och de skall stå i rätt proportion till den störning som skall avvärjas. Åtgärderna skall utföras utan att yttrandefriheten eller skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än nödvändigt med tanke på säkerställandet av möjligheterna att uppnå målen enligt 1 mom. Åtgärderna skall avbrytas, om det inte*

Gällande lydelse	*Föreslagen lydelse*
skall avbrytas så snart det inte längre finns i denna paragraf nämnda förutsättningar för att vidta dem.	*längre finns i denna paragraf nämnda förutsättningar för att vidta dem.*
Kommunikationsverket kan meddela närmare föreskrifter om det tekniska förfarandet för att avvärja i denna paragraf avsedda kränkningar av dataskyddet samt för att eliminera störningar av dataskyddet.	*Kommunikationsverket kan meddela teleföretagen och dem som tillhandahåller mervärdestjänster närmare föreskrifter om hur åtgärderna enligt denna paragraf skall genomföras tekniskt.*
32 §	32 §
Dataombudsmannens uppgifter	*Dataombudsmannens uppgifter*
Dataombudsmannens uppgift är att övervaka	Dataombudsmannens uppgift är att övervaka
	1) i 13 a–13 j § avsedd behandling av identifieringsuppgifter som en sammanslutningsabonnent genomför,
1) i 4 kap. avsedd behandling av lokaliseringsuppgifter,	*2)* i 4 kap. avsedd behandling av lokaliseringsuppgifter,
2) tillämpningen av de i 25 § avsedda bestämmelserna om telefonkataloger, abonnentkataloger och nummerupplysning,	*3)* tillämpningen av bestämmelserna om telefonkataloger, abonnentkataloger och nummerupplysning som avses i 25 §,
3) tillämpningen av bestämmelserna om direktmarknadsföring i 7 kap., samt	*4)* tillämpningen av bestämmelserna om direktmarknadsföring i 7 kap.,
4) bestämmelserna om rätt att få uppgifter och om tystnadsplikt i 9 kap., till den del det gäller lokaliseringsuppgifter.	*5)* bestämmelserna om rätt att få uppgifter och om tystnadsplikt i 9 kap., till den del det är fråga om lokaliseringsuppgifter.
	För de tillsynsuppgifter som avses i 1 mom. 1 punkten får en avgift tas ut av sammanslutningsabonnenten. Beslut om avgiftsbelagda åtgärder och avgiftens storlek fattas genom förordning av justitie-ministeriet enligt de grunder som föreskrivs i lagen om grunderna för avgifter till staten (150/1992).
33 §	33 §
Styrnings- och övervakningsmyndigheternas rätt att få uppgifter	*Styrnings- och övervakningsmyndigheternas rätt att få uppgifter*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
För att utföra sina i denna lag föreskrivna uppgifter har Kommunikationsverket och dataombudsmannen rätt att få identifierings- och lokaliseringsuppgifter *och i 20 § 2 mom. avsedda* meddelanden, om de är behövliga för att övervaka att bestämmelserna om behandling, användning av i 7 § avsedda uppgifter	För att utföra sina i denna lag föreskrivna uppgifter har Kommunikationsverket och dataombudsmannen rätt att få identifierings- och lokaliseringsuppgifter och meddelanden, *om det behövs* för att övervaka bestämmelserna om behandling, användning av i 7 § avsedda uppgifter eller direktmarknadsföring

Gällande lydelse	*Föreslagen lydelse*
eller direktmarknadsföring *iakttas* eller för att utreda betydande kränkningar och hot av dataskyddet och om det enligt Kommunikationsverkets eller dataombudsmannens bedömning är skäl att misstänka att något av följande rekvisit är uppfyllda:	eller för att utreda betydande kränkningar av och hot mot dataskyddet. *Dessutom krävs det att* det enligt Kommunikationsverkets eller dataombudsmannens bedömning är skäl att misstänka att något av följande rekvisit är uppfyllda:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
34 §	34 §
Tillsynsmyndigheternas tystnadsplikt ***och utlämnande av uppgifter***	*Tillsynsmyndigheternas tystnadsplikt*
Uppgifter som Kommunikationsverket och dataombudsmannen med stöd av 33 § 3 mom. erhållit om konfidentiella meddelanden, identifieringsuppgifter och lokaliseringsuppgifter skall hållas hemliga.	Uppgifter som Kommunikationsverket och dataombudsmannen med stöd av 33 § 3 mom. erhållit om konfidentiella meddelanden, identifieringsuppgifter och lokaliseringsuppgifter *samt uppgifter som dataombudsmannen erhållit med stöd av 13 h §* skall hållas hemliga.
Utan hinder av någon annan än den sekretessbestämmelse som avses i 1 mom. eller utan hinder av andra begränsningar som gäller utlämnande av uppgifter har Kommunikationsverket och dataombudsmannen rätt att till kommunikationsministeriet lämna ut i 33 § 1 mom. avsedda uppgifter som de erhållit vid utförandet av i denna lag föreskrivna uppgifter.	(34 a § 1 mom.)
Utan hinder av den sekretessbestämmelse som avses i 1 mom. eller utan hinder av andra begränsningar som gäller utlämnande av uppgifter har Kommunikationsverket rätt att till de teleföretag, till dem som tillhandahåller mervärdestjänster och till de sammanslutningsabonnenter som har utnyttjats vid kränkning av dataskydd eller som har blivit föremål för sådan kränkning, lämna ut identifieringsuppgifter som verket erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskydd, om det enligt Kommunikationsverkets bedömning finns skäl att misstänka att något av de rekvisit som anges i 33 § 3 mom. 1–10 punkten har blivit uppfyllda.	(34 a § 2 mom.)
Kommunikationsverket har rätt att lämna ut ovan i 3 mom. avsedda identifieringsuppgifter endast i den omfattning som är nödvändig för att förebygga och utreda kränkningar av dataskydd.	(34 a § 3 mom.)
I övrigt gäller lagen om offentlighet i myndigheternas verksamhet (621/1999) i fråga om sekretess för tillsynsmyndigheternas upp-	I övrigt föreskrivs det om sekretess för tillsynsmyndigheternas uppgifter i lagen om offentlighet *i myndigheternas verksamhet*

Gällande lydelse	*Föreslagen lydelse*
gifter.	(621/1999).
	34 a §
	Utlämnande av tillsynsmyndigheternas uppgifter
(34 § 1 mom.)	*Utan hinder av någon annan än den tystnadsplikt som föreskrivs i 34 § 1 mom. eller utan hinder av andra begränsningar som gäller utlämnande av uppgifter har Kommunikationsverket och dataombudsmannen rätt att till kommunikationsministeriet lämna ut i 33 § 1 mom. avsedda uppgifter som de erhållit vid utförandet av i denna lag föreskrivna uppgifter.*
(34 § 2 mom.)	*Utan hinder av den tystnadsplikt som föreskrivs i 34 § 1 mom. eller utan hinder av andra begränsningar som gäller utlämnande av uppgifter har Kommunikationsverket rätt att till de teleföretag, dem som tillhandahåller mervärdestjänster och de sammanslutningsabonnenter som har utnyttjats vid kränkning av dataskydd, som har blivit föremål för sådan kränkning eller som sannolikt kan utsättas för kränkning av dataskydd, lämna ut identifieringsuppgifter som verket erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskydd, om det enligt Kommunikationsverkets bedömning finns skäl att misstänka att något av de rekvisit som anges i 33 § 3 mom. 1–10 punkten har blivit uppfyllt.*
(34 § 3 mom.)	*Utan hinder av den tystnadsplikt som föreskrivs i 34 § 1 mom. har Kommunikationsverket rätt att till sådana myndigheter eller andra instanser som är verksamma i andra stater och som har till uppgift att förebygga eller utreda kränkningar av dataskydd riktade mot kommunikationsnät och kommunikationstjänster lämna ut identifieringsuppgifter som verket erhållit i samband med insamlandet av uppgifter om och utredning av kränkningar av dataskydd.* *Kommunikationsverket har rätt att lämna ut i 2 och 3 mom. avsedda identifieringsuppgifter endast i den omfattning som behövs för att förebygga och utreda kränkningar av dataskydd. Utlämnandet av uppgifter får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nöd-*

Gällande lydelse	*Föreslagen lydelse*
	vändigt.
42 §	42 §
Straffbestämmelser	*Straffbestämmelser*
Bestämmelser om straff för kränkning av kommunikationshemlighet och för grov kränkning av kommunikationshemlighet finns i 38 kap. 3 och 4 § i strafflagen samt för dataintrång i 38 kap. 8 § i strafflagen. Straff för brott mot i 5 § föreskriven tystnadsplikt utdöms enligt 38 kap. 1 eller 2 § i strafflagen, om gärningen inte utgör brott enligt 40 kap. 5 § i strafflagen eller om inte strängare straff föreskrivs någon annanstans.	Bestämmelser om straff för kränkning av kommunikationshemlighet och för grov kränkning av kommunikationshemlighet finns i 38 kap. 3 och 4 § i strafflagen samt för dataintrång i 38 kap. 8 § i strafflagen. Straff för brott mot i 5 § föreskriven tystnadsplikt utdöms enligt 38 kap. 1 eller 2 § i strafflagen, om gärningen inte utgör brott enligt 40 kap. 5 § i strafflagen eller om inte strängare straff föreskrivs någon annanstans. *Straff för brott mot i 13 d § 3 mom. föreskriven tystnadsplikt utdöms enligt 38 kap. 2 § 2 mom. i strafflagen, om inte strängare straff för gärningen föreskrivs någon annanstans än i 38 kap. 1 § i strafflagen.*
Den som uppsåtligen 1) bryter mot det i 6 § 2 mom. föreskrivna förbudet mot innehav, import, tillverkning eller distribution av system för avkodning av det tekniska skyddet vid elektronisk kommunikation eller av en del av ett sådant system, 2) försummar de förpliktelser som föreskrivs i 7 §, 3) försummar den i 19 § föreskrivna skyldigheten att handha dataskyddet för sina tjänster eller för identifierings- och lokaliseringsuppgifter, 4) försummar den i 21 § 2 mom. eller 35 § 4 mom. föreskrivna anmälningsplikten, 5) behandlar identifierings- eller lokaliseringsuppgifter i strid med bestämmelserna i 3 och 4 kap., 6) underlåter att iaktta vad som i 24 § bestäms om specificering av en räkning, 7) underlåter att iaktta vad som i 25 § bestäms om behandling av personuppgifter som ingår i en telefonkatalog eller i en annan abonnentkatalog, om anmälning till abonnenten om ändamålet med och användningen av katalogen, om avlägsnande och rättelse av uppgifter, om förbud eller om juridiska personers rättigheter, *eller* 8) bedriver direktmarknadsföring i strid med bestämmelserna i 7 kap.,	Den som uppsåtligen 1) bryter mot det i 6 § 2 mom. föreskrivna förbudet mot innehav, import, tillverkning eller distribution av system för avkodning av det tekniska skyddet vid elektronisk kommunikation eller av en del av ett sådant system, 2) försummar de förpliktelser som föreskrivs i 7 §, 3) försummar den i 19 § föreskrivna skyldigheten att handha dataskyddet för sina tjänster eller för identifierings- och lokaliseringsuppgifter, 4) försummar den i 21 § 2 mom. eller 35 § 4 mom. föreskrivna anmälningsplikten, 5) behandlar identifierings- eller lokaliseringsuppgifter i strid med bestämmelserna i 3 och 4 kap., 6) underlåter att iaktta vad som i 24 § bestäms om specificering av en räkning, 7) underlåter att iaktta vad som i 25 § bestäms om behandling av personuppgifter som ingår i en telefonkatalog eller i en annan abonnentkatalog, om anmälning till abonnenten om ändamålet med och användningen av katalogen, om avlägsnande och rättelse av uppgifter, om förbud eller om juridiska personers rättigheter, 8) bedriver direktmarknadsföring i strid med bestämmelserna i 7 kap., *eller* *9) underlåter att iaktta vad som i 13 f–13 h*

skall, om inte strängare straff för gärningen bestäms någon annanstans i lag, för *dataskyddsförseelse vid elektronisk kommunikation* dömas till böter.

Straff döms inte ut om förseelsen är ringa.

§ bestäms om att utarbeta en redogörelse eller förhandsanmälan och att lämna den till användarna, arbetstagarnas företrädare eller dataombudsmannen,

skall, om inte strängare straff för gärningen bestäms någon annanstans i lag, för *dataskyddsförseelse vid elektronisk kommunikation* dömas till böter.

Straff döms inte ut om förseelsen är ringa.

Denna lag träder i kraft den 20 .

2.

Lag

om ändring av 2 och 21 § i lagen om integritetsskydd i arbetslivet

I enlighet med riksdagens beslut

ändras i lagen av den 13 augusti 2004 om integritetsskydd i arbetslivet (759/2004) 2 § 3 mom. och 21 § 1 mom., sådant det sist nämnda av dem lyder i lag 457/2007, som följer:

Gällande lydelse	*Föreslagen lydelse*
2 §	2 §
Tillämpningsområde	*Tillämpningsområde*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
På behandling av personuppgifter tillämpas personuppgiftslagen (523/1999) och lagen om dataskydd vid elektronisk kommunikation (516/2004), om inte något annat bestäms i denna lag.	*Om arbetsgivarens rätt att i egenskap av abonnent för utredning av avgiftsskyldigheten få identifieringsuppgifter om en anslutning som ställts till arbetstagarens förfogande och om rätten att behandla identifieringsuppgifter som gäller arbetstagarens elektroniska kommunikation i situationer av olovligt brukande av ett kommunikationsnät eller brukande av en kommunikationstjänst som strider mot anvisningarna och för att skydda företagshemligheter föreskrivs i lagen om dataskydd vid elektronisk kommunikation (516/2004). Vad som i nämnda lag bestäms om användare av lokaliseringstjänster tillämpas på arbetstagare till vars förfogande arbetsgivaren har ställt en lokaliseringstjänst.* På behandling av personuppgifter tillämpas personuppgiftslagen (523/1999), om inte något annat bestäms i denna lag.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
21 §	21 §
Samarbete vid ordnande av teknisk övervakning och användning av datanät	*Samarbete vid ordnande av teknisk övervakning och användning av datanät*
Syftet med kameraövervakning, passerkontroll och annan övervakning med tekniska metoder av arbetstagarna, ibruktagandet av dem och de metoder som används samt an-	Syftet med kameraövervakning, passerkontroll och annan övervakning med tekniska metoder av arbetstagarna, ibruktagandet av dem och de metoder som används i övervak-

Gällande lydelse	*Föreslagen lydelse*
vändningen av elektronisk post och andra datanät omfattas av samarbetsförfarandet enligt lagen om samarbete inom företag, lagen om samarbete inom statens ämbetsverk och inrättningar samt lagen om samarbete mellan kommunala arbetsgivare och arbetstagare. I andra företag och offentligrättsliga sammanslutningar än sådana som omfattas av samarbetslagstiftningen skall arbetsgivaren före beslutsfattandet bereda arbetstagarna eller deras representanter tillfälle att bli hörda i de angelägenheter som nämns ovan. (13.4.2007/457)	ningen samt användningen av elektronisk post och andra datanät *samt behandlingen av uppgifter som gäller en arbetstagares elektroniska post och annan elektronisk kommunikation* omfattas av samarbetsförfarandet enligt lagen om samarbete inom företag, lagen om samarbete inom statens ämbetsverk och inrättningar samt lagen om samarbete mellan kommunala arbetsgivare och arbetstagare I andra företag och offentligrättsliga sammanslutningar än sådana som omfattas av samarbetslagstiftningen skall arbetsgivaren före beslutsfattandet bereda arbetstagarna eller deras representanter tillfälle att bli hörda i de angelägenheter som nämns ovan.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

3.

Lag

om ändring av 19 § i lagen om samarbete inom företag

I enlighet med riksdagens beslut
ändras i lagen av den 30 mars 2007 om samarbete inom företag (334/2007) 19 § 4 punkten som följer:

Gällande lydelse	*Föreslagen lydelse*
19 §	19 §
Behandling av planer, principer och praxis som grundar sig på annan lagstiftning	*Behandling av planer, principer och praxis som grundar sig på annan lagstiftning*
Vid samarbetsförhandlingar skall behandlas	Vid samarbetsförhandlingar skall behandlas
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
4) principerna för användningen av elektronisk post och datanät,	4) principerna för användningen av elektronisk post och datanät *samt behandlingen av uppgifter som gäller en arbetstagares elektroniska post och annan elektronisk kommunikation,*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

———

Denna lag träder i kraft den 20 .

———

4.

Lag

om ändring av 7 § i lagen om samarbete inom statens ämbetsverk och inrättningar

I enlighet med riksdagens beslut

ändras i lagen av den 1 juli 1988 om samarbete inom statens ämbetsverk och inrättningar (651/1988) 7 § 11 a-punkten, sådan den lyder i lag 762/2004, som följer:

Gällande lydelse	*Föreslagen lydelse*
7 §	7 §
Ärenden som omfattas av samarbetsförfarandet	*Ärenden som omfattas av samarbetsförfarandet*
Samarbetsförfarandet omfattar	Samarbetsförfarandet omfattar
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
11 a) syftet med, ibruktagandet av och metoderna för kameraövervakning, passerkontroll och annan övervakning med tekniska metoder av personalen samt användningen av elektronisk post och datanät,	11 a) syftet med, ibruktagandet av och metoderna för kameraövervakning, passerkontroll och annan övervakning med tekniska metoder av personalen, användningen av elektronisk post och datanät *samt behandlingen av uppgifter som gäller en tjänstemans och arbetstagares elektroniska post och annan elektronisk kommunikation*,
	— — — — — — — — — — — — — — —

Denna lag träder i kraft den 20 .
