

KOMMUNIKATIONSUTSKOTTETS BETÄNKANDE 13/2004 rd

Regeringens proposition med förslag till lag om dataskydd vid elektronisk kommunikation och om ändring av vissa till den anslutna lagar

INLEDNING

Remiss

Riksdagen remitterade den 11 november 2003 en proposition med förslag till lag om dataskydd vid elektronisk kommunikation och om ändring av vissa till den anslutna lagar (RP 125/2003 rd) till kommunikationsutskottet för beredning.

Utlåtande

I enlighet med riksdagens beslut har grundlagsutskottet och förvaltningsutskottet lämnat utlåtanden i ärendet. Utlåtandena (GrUU 9/2004 rd och FvUU 9/2004 rd) ingår som bilaga till detta betänkande.

Sakkunniga

Utskottet har hört

- riksdagsledamot Jyrki Kasvi, riksdagen
- konsultativ tjänsteman Juhapekka Ristola, kommunikationsministeriet
- lagstiftningsråd Leena Vettenranta, justitieministeriet
- lagstiftningsråd Kimmo Hakonen och konsultativ tjänsteman Kaarlo Korvola, inrikesministeriet
- dataombudsman Reijo Aarnio, Dataombudsmannens byrå
- jurist Miina Ojajärvi, Konsumentverket
- direktör Tapani Rantanen och chef för datasäkerhetsenheten Timo Lehtimäki, Kommunikationsverket
- kriminalinspektör Ari Määttä, centralkriminalpolisen

- jurist Heli Malmi, skyddspolisen
- datasäkerhetschef Antti Järvinen, Rundradion
- avdelningsdirektör Kari Wirman, Elisa Communications
- teknologidirektör Ari Hyppönen, F-Secure Abp
- dataadministrationsdirektör Jouni Keronen, Fortum Abp
- verkställande direktör Kari Taskinen, Hand Held Systems Ab
- direktör för informationssamhälle Mikael Jungner, Microsoft Ab
- director corporate relations, chief security officer Urho Ilmonen, Nokia Abp
- bankjurist Esa Kainulainen, Nordea Bank Finland Abp
- bankjurist Taina Kallio-Miettinen, Andelsbankscentralen
- utvecklingsdirektör Marja-Liisa Virtanen, TeliaSonera Finland Abp
- jurist Eeva Laatikainen, FiCom
- jurist Minna Aalto-Setälä, Finnet-förbundet rf
- verkställande direktör Jari Perko, Suomen Suoramarkkinointiliitto
- juridisk ombudsman Riikka Tähtivuori, Företagarna i Finland
- projektchef Antti Kotilainen och internetinspektör Ilkka Vuorenmaa, Upphovsrättens informations- och övervakningscentral
- avdelningschef Hannele Pohjola, Industrins och Arbetsgivarnas Centralförbund TT rf
- direktör Valtteri Niiranen, Mediernas Centralförbund

- jurist Elli Myllylä, Bankföreningen i Finland
- styrelseordförande Arto Kangas, Tietoturva ry
- professor Arto Karila
- JD, docent i familjerätt Kirsti Kurki-Suonio

- diplomingenjör Hannu Haaranen.

Dessutom har utskottet fått ett skriftligt utlåtande från

— Reklam-TV Ab.

PROPOSITIONEN

Propositionen

Regeringen föreslår att en ny lag om dataskydd vid elektronisk kommunikation stiftas och att vissa andra lagar ändras. Genom den föreslagna lagen upphävs lagen om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet, och med stöd av denna lag utfärdade förordningar. Genom den föreslagna lagen implementeras Europaparlamentets och rådets direktiv om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation samt artikel 10 i Europaparlamentets och rådets direktiv om distansförsäljning av finansiella tjänster till konsumenter.

Genom propositionen genomförs en totalreform av integritetsskyddet vid elektronisk kommunikation. Propositionens syfte är att trygga konfidentialitet och integritetsskydd vid elektronisk kommunikation, samt att befrämja dataskydd vid sådan kommunikation och en balanserad utveckling av varierade elektroniska kommunikationstjänster.

Propositionen eftersträvar att precisera och klargöra bestämmelserna om behandlingen av identifieringstjänster, med bibehållande av de centrala principerna i gällande lag om dataskydd inom televerksamhet. I propositionen föreslås att rättigheterna och förpliktelserna vid behandling av identifieringsuppgifter också ska gälla sammanslutningsabonnenter, varmed avses en sammanslutning som är abonnent på kommunikations- och mervärdestjänster och som i sitt kommunikationsnät behandlar användarnas konfidentiella meddelanden samt identifierings- och lokaliseringssuppgifter om dem. Precisering av sammanslutningsabonnenternas ställning reducerar inte juridiska personers rättigheter som kommunikationspartner. Dessutom före-

slås att ett teleföretag under två års tid ska lagra detaljerade uppgifter om behandlingen av identifieringsuppgifter.

I propositionen föreslås nya bestämmelser om registrering på användarens terminalutrustning av cookies eller andra uppgifter om användningen av tjänster samt om användningen av dessa uppgifter.

Nya bestämmelser föreslås om behandlingen av lokaliseringssuppgifter. Användaren ska ha möjlighet att förbjuda att lokaliseringssuppgifter behandlas för tjänster som kan förknippas med en abonnent eller användare och dessutom ska samtycke per tjänst till behandlingen av lokaliseringstjänster inhämtas av den som ska lokaliseras.

Enligt propositionen ska ett teleföretag, den som tillhandahåller mervärdestjänster, eller en sammanslutningsabonnent ha rätt att under vissa förutsättningar vidta nödvändiga åtgärder för att avvärja kränkningar och eliminera störningar av dataskydd och för att säkra dataskydd genom att hindra mottagandet av elektronisk post, textmeddelanden och andra motsvarande meddelanden, genom att avlägsna de skadliga programmen ur kommunikationerna samt genom att vidta andra nödvändiga åtgärder.

Enligt propositionen ska ett teleföretag på begäran av användaren ge en detaljerad specifikation av en räkning.

I propositionen föreslås att flera bestämmelser om direktmarknadsföring ska preciseras. Samtidigt föreslås att ett teleföretag och en sammanslutningsabonnent med användarens samtycke ska ha rätt att hindra mottagandet av oönskad direktmarknadsföring.

Användaren ska få rätt att av ett teleföretag få sådana identifieringsuppgifter om anslutningen

eller terminalutrustningen som anger position vid en viss tidpunkt.

I propositionen föreslås att teleföretag som utövar sin verksamhet med stöd av anmälan eller koncession ska vara skyldiga att till Kommunikationsverket betala en årlig dataskyddsavgift.

I propositionen föreslås att den som tillhandahåller informationssamhällets tjänster ska kunna behandla identifieringsuppgifter som är nödvändiga för att fakturera bild- och ljudinspelningar och sina andra avgiftsbelagda tjänster, som förmedlats genom av ett teleföretag administrerat kommunikationsnät, samt andra för faktureringen nödvändiga uppgifter, om den abonnent eller användare som uppgifterna gäller har gett sitt samtycke. Enligt den föreslagna bestämmelsen har den som tillhandahåller informationssamhällets tjänster rätt att av teleföretaget få ovannämnda uppgifter. Bestämmelserna om den som tillhandahåller mervärdestjänster ska tillämpas på behandlingen av uppgifterna.

Det föreslås att polislagens paragraf om rätten att få uppgifter kompletteras. I tillägg till de nuvarande hemliga telefonnumren ska polisen ha rätt att av teleföretag och sammanslutningsabonnenter få uppgifter som individualiserar terminalutrustning och anslutningar, om uppgifterna i enskilda fall behövs för att polisen ska kunna fullgöra sina uppgifter.

I propositionen föreslås att de författningstekniska ändringarna ska göras i strafflagen, kommunikationsmarknadslagen, lagen om nödcentraler, lagen om kommunikationsförvaltningen, sjöräddningslagen och lagen om behandling av personuppgifter i polisens verksamhet som namnet på den föreslagna lagen kräver.

De föreslagna lagarna avses träda i kraft snarast möjligt efter det att de har blivit godkända och stadfästa. Direktivet om integritet och elektronisk kommunikation ska implementeras den 31 oktober 2003.

UTSKOTTETS ÖVERVÄGANDEN

Allmän motivering

Med hänvisning till propositionens motivering och annan utredning anser utskottet att propositionen behövs och är angelägen. Utskottet tillstyrker lagförslaget men med följande anmärkningar och ändringsförslag.

Allmänt

Lagförslaget handlar dels om en allmän lag inom området för elektronisk kommunikation, dels om en speciallag t.ex. om behandlingen av personuppgifter i elektronisk kommunikation. Därmed har förslaget beröringspunkter med speciallagstiftning om många områden och den spelar också en central roll för det allmännas skyldighet att tillgodose de grundläggande fri- och rättigheterna enligt 22 § i grundlagen. Lagstiftningen gäller en ny och sammansatt tekniskt-social verksamhetsmiljö där i stort sett likadana verksamheter genomförs med mycket olika tekniska redskap och tillämpningar. Dessutom utvecklas dessa

redskap och tillämpningar exceptionellt snabbt och därmed måste lagstiftningen vara så teknologineutral som möjligt. Det kan inte undvikas att detta höjer lagstiftningens abstraktionsnivå.

Lagförslagets räckvidd är mycket omfattande. Det täcker in alla slag av redskap med vilka meddelanden förmedlas eller sänds, beroende på situationen, antingen i allmänna kommunikationsnät eller också i andra nät än allmänna kommunikationsnät. Kommunikationens och identifieringsuppgifternas konfidentialitet gäller meddelanden som förmedlas i kommunikationsnäten och meddelanden som fysiskt finns i användarnas terminalutrustning, t.ex. mottagna e-postmeddelanden. Utskottet understryker att skyddet för ett konfidentiellt meddelande också omfattar meddelanden som lagrats för mottagning i terminalutrustningen. Formuleringarna i föreslagna 4 och 5 § avgränsar inte heller skyddet för ett konfidentiellt meddelande enbart till meddelanden i näten.

Merparten av begreppen och angreppssätten i propositionen är hämtade direkt ur andra lagar, som lagen om integritetsskydd vid telekommunikation och dataskydd inom televerksamhet (t.ex. tillämpningsområde, identifieringsuppgift, dataskydd, abonnent, användare, abonnentkatalog), kommunikationsmarknadslagen (som teleföretag, kommunikationstjänst, nättjänst, kommunikationsnät, allmänt kommunikationsnät), personuppgiftslagen (behandling i vidsträckt mening) och lagen om tillhandahållande av informationssamhällets tjänster (den som tillhandahåller informationssamhällets tjänster).

Genom lagstiftningen sätts direktivet om integritet och elektronisk kommunikation i kraft nationellt. Formuleringarna är ställvis mycket svårtydda och komplicerade och terminologin är delvis främmande åtminstone för normalt finskt och svenskt språkbruk. Som exempel kan nämnas att elektronisk post enligt direktivet också omfattar textmeddelande som vi i Finland brukar behandla som en annan form av kommunikation. Termen mervärdestjänst ger upphov till ett likadant problem. Enligt direktivet avses med det närmast tjänster som bygger på lokaliseringssuppgifter. När direktivet om s.k. elektronisk handel sattes i kraft genom lagen om tillhandahållande av informationssamhällets tjänster (458/2002) infördes mervärdestjänst i linje med allmänt finskt och svenskt språkbruk hos oss som informationssamhällets tjänster. På grund av det stora antalet fenomen som ska regleras i den föreliggande propositionen används i propositionen mervärdestjänst och informationssamhällets tjänster sida vid sida.

Lagens begreppsapparat

Förvaltningsutskottet påpekar i sitt utlåtande FvUU 9/2004 rd — RP 125/2003 rd att man bör vara extra noga med definitionen på begreppen i lagtexten, särskilt som orden ännu inte har fått spridning i allmänspråket. Kommunikationsutskottet framhåller att lagstiftningen gäller en teknisk helhet vars särdrag ställer höga krav på propositionens formulering. Regeringen har försökt att i detalj definiera begreppen i lagtexten

och förklara dem i motiveringen. Begreppsapparaten öppnar sig för dem som behärskar specialterminologin på området, men utskottet understryker att ambitionen bör vara att göra lagtexten klar också för gemene man. Därför anser utskottet med stöd av utlåtanden och utfrågningen av sakkunniga att vissa formuleringar i lagtexten måste preciseras och att begreppen på vissa punkter bör tydliggöras i betänkandets allmänna motivering.

Identifieringsuppgift. Identifieringsuppgift är ett av de viktigaste begreppen i propositionen. Med identifieringsuppgift avses en uppgift som kan förbindas med en abonnent eller användare och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden. Identifieringsuppgifterna kan omfatta uppgifter som bland annat anger vilken väg kommunikationen routas, dess varaktighet, tidpunkt, eller mängden överförda data, det använda protokollet, den position där avsändarens eller mottagarens terminalutrustning befinner sig på en viss basstations område, det avsändande och mottagande nätet samt kommunikationens början, slut och varaktighet. Uppgifterna kan också avse den form som meddelandet förmedlas i i nätet. Den avgörande faktorn är att uppgifterna ska kunna kopplas till en abonnent eller användare. Vad gäller begreppet identifieringsuppgift bör det observeras att den abonnent som identifieringsuppgifterna kan kopplas till kan vara både en fysisk och en juridisk person.

Begreppet identifieringsuppgift har inte avgränsats enbart till uppgifter som behandlas i kommunikationsnät utan det avser också uppgifter i näten som används för vissa ändamål som till att överföra, distribuera eller tillhandahålla meddelanden. Avgränsningen enligt ändamålet inskränker begreppet identifieringsuppgift på ett lämpligt sätt; en alltför noggrann avgränsning på denna punkt kunde eventuellt tillåta att bestämmelsen obehindrat kringgås och leda till att lagen i takt med den tekniska utvecklingen mycket snart måste ändras. Med hänsyn till att olika ändamål kan uppfyllas på en mängd olika sätt är det helt omöjligt att i samband med

begreppet identifieringsuppgift genom konkreta exempel och på ett heltäckande sätt definiera exakta gränser i förhållande till tjänster, nät och terminalutrustning. Det är nödvändigt att eftersträva teknologineutralitet och till exempel ett enskilt tekniskt genomföringssätt kan inte spela en avgörande roll för definitionen av identifieringsuppgifter. Redan efter det att propositionen lämnades har det blivit aktuellt att överväga om den nya lagen bör tillämpas på direktmarknadsföring med s.k. Blue Tooth-teknik, vilket bara är ett exempel på att nya tekniska metoder tas i bruk varje månad.

Det är ytterst svårt att ytterligare förtydliga definitionen på identifieringsuppgift i avgörande grad. Det svarar mot begreppet identifieringsuppgift i den redan gällande lagen om dataskydd inom televerksamhet som avser abonnentens eller användarens anslutningsnummer eller någon annan kod eller uppgift som uppkommer eller lagras då en uppkoppling har gjorts. I det föreliggande lagförslaget avses med identifieringsuppgift en uppgift som kan förbindas med en abonnent eller användare och som behandlas i kommunikationsnäten för att överföra, distribuera eller tillhandahålla meddelanden. I direktivet om integritet och elektronisk kommunikation har begreppet trafikuppgift definierats brett så att det omfattar alla uppgifter som behandlas i ett elektroniskt kommunikationsnät för överföring och fakturering av kommunikation. I detaljmotiveringen ges också en omfattande beskrivning av begreppet identifieringsuppgift.

Lokaliseringsuppgift. Identifieringsuppgifterna och en del av de uppgifter som anger en anslutnings eller terminalutrustnings geografiska position är nödvändiga för att utföra nät- eller kommunikationstjänster. Lokaliseringsuppgifterna är i begreppsligt hänseende identifieringsuppgifter eftersom de används för samma ändamål. Däremot är lokaliseringsuppgifter som används för något annat ändamål än för att utföra kommunikations- eller nättjänster inte identifieringsuppgifter utan lokaliseringsuppgifter på grund av att ändamålet är ett annat.

Det är mycket viktigt att göra en åtskillnad utifrån ändamålet, eftersom lokaliseringsuppgifterna är mera kritiska än identifieringsuppgifterna på grund av objektets behov av integritetsskydd. Lokaliseringsuppgifterna har ett mycket nära samband med integritetsskyddet medan identifieringsuppgifterna uttryckligen omfattas av skyddet för konfidentiell kommunikation. Tjänster som bygger på lokaliseringsuppgifter kräver nödvändigt en särskild lagstiftning för att säkerställa användarnas integritetsskydd och för att möjliggöra en utveckling av tjänsterna. I praktiken kan lagstiftningen inte genomföras om inte begreppen identifieringsuppgifter och lokaliseringssuppgifter skiljs åt. Åtskillnaden svarar också mot begreppen i direktivet om integritet och elektronisk kommunikation.

Sammanlutningsabonnent. Med en sammanlutningsabonnent avses ett företag eller en sammanlutning som är abonnent på kommunikations- eller mervärdestjänster och som i sitt kommunikationsnät behandlar konfidentiella meddelanden från användare, eller konfidentiella identifierings- eller lokaliseringsuppgifter om dem. Begreppet sammanlutningsabonnent i förslagen 10 § 2 mom. omfattar utöver egentliga företag också universitet och olika slag av sammanlutningar inom den offentliga förvaltningen, som har intern fakturering. Hit hör till exempel näringsidkare, andelslag, aktiebolag, föreningar, universitet eller statliga ämbetsverk.

En sammanlutningsabonnent är precis som ett teleföretag utomstående i relation till kommunikationsparterna. Sammanlutningsabonnenten abonnerar på kommunikationstjänsten eller mervärdestjänsten för sina användare, till exempel anställda. För detta ändamål administrerar sammanlutningsabonnenten samtidigt det system där konfidentiella identifieringsuppgifter och lokaliseringsuppgifter om användarna behandlas med olika slag av servrar och terminalutrustning. I en sammanlutningsabonnents tekniska system samlas konfidentiella identifieringsuppgifter om användarna och i till exempel e-postsystem också konfidentiella meddelanden. Sammanlutningsabonnenter, som företag

och universitet, behandlar exakt samma konfidentiella uppgifter och med likadana tekniska system som teleföretagen. När teleföretagen tillhandahåller kommunikationstjänster samlas det därmed i dem exakt likadana uppgifter som hos sammanslutningsabonnenten när kommunikationstjänster utnyttjas. Det betyder att en sammanslutningsabonnents möjligheter till missbruk och behov av enahanda behandlingsrättigheter och skyldigheter är likadana som för ett teleföretag. För att sammanslutningsabonnenten ska kunna bedriva sin verksamhet och för att integriteten och konfidentialiteten i kommunikationen ska kunna säkerställas måste likadana dataskyddsförpliktelser och regler för behandling av identifieringsuppgifter och lokaliseringssuppgifter ställas upp för sammanslutningsabonnenten som för teleföretagen.

Grundlagsutskottet konstaterar i sitt utlåtande (GrUU 9/2004 rd) att den förpliktelse att tillgodose de grundläggande fri- och rättigheterna och de mänskliga rättigheterna som 22 § i grundlagen ställer för det allmänna också gäller inbördes förhållanden mellan privatpersoner. Enligt förarbetena till bestämmelsen gäller förpliktelserna främst lagstiftaren, vars uppgift är att precisera de allmänt uttryckta fri- och rättigheterna i grundlagen så att deras verkningar också sträcker sig till förhållandet mellan privatpersoner (RP 309/1993 rd, s. 79—80). Lagförslaget uppfyller denna skyldighet för det allmänna framför allt när det gäller yttrandefriheten och hemligheten i fråga om förtroliga meddelanden inom sektorn för elektronisk kommunikation. Kommunikationsministeriet ansåg vid utfrågningen av sakkunniga att det var nödvändigt att reglera sammanslutningsabbonenternas verksamhet på förslaget sätt för att skyldigheten i 22 § i grundlagen ska kunna fullföljas i dagens samhälle. Utskottet noterar att inte heller grundlagsutskottet i sitt utlåtande ansett det nödvändigt att göra en åtskillnad mellan teleföretag och sammanslutningsabbonenter då det behandlade de föreslagna bestämmelserna om behandling av identifieringsuppgifter.

Registrering av identifieringsuppgifter

Förvaltningsutskottet påpekar i sitt utlåtande FvUU 9/2004 rd att förslaget till lag om dataskydd vid elektronisk kommunikation inte innefattar några allmänna bestämmelser om skyldighet att lagra identifieringsuppgifter vid elektronisk kommunikation. Vidare ansåg det att det i vilket fall som helst var befogat att ta in bestämmelser i lag utifrån en fristående beredning.

Enligt vad som kommit fram vid utfrågningen av sakkunniga omfattar en allmän registreringsskyldighet identifieringsuppgifterna i nästan all elektronisk kommunikation och beräknas under det första året i Finland ge upphov till extra investeringskostnader på 75 miljoner euro och omkring 17 miljoner euro i underhållskostnader under det första och varje därpå följande år. Man kan få en viss uppfattning om vilka mängder uppgifter som ska registreras av att huvudsidorna enbart i portalen SoneraPlaza i augusti 2003 hade 1 900 000 olika besökare, 10 000 000 olika gånger och att 111 000 000 olika sidor laddades ner från dem. Varje besökare, besök och nerladdade sida genererade identifieringsuppgifter. Likaså uppstår identifieringsuppgifter bland annat vid e-postkommunikation, textmeddelanden och samtal mellan människor. Enligt centralkriminalpolisen polisanmäldes 2002 tre fall av spridning av barnpornografi och rasistiskt material, men inte ett enda av dem ledde till åtal. I samband med att Europarådets konvention om cyberbrottslighet sätts i kraft nationellt har justitieministeriet utarbetat utkast till bestämmelser om skyldighet att arkivera uppgifter för att säkerställa utredning av cyberbrott. Denna arkiveringsskyldighet som eventuellt tas in i tvångsmedelslagen ska gälla enskilda fall och uppgifter som datasystemadministratören redan har i sin besittning och kräver därmed inga särskilda extra investeringar.

Enligt kommunikationsministeriet stannade man på dessa grunder vid beredningen av regeringens proposition för att en skyldighet att arkivera enbart existerande uppgifter enligt konventionen om cyberbrottslighet är ett väsentligt mycket bättre sätt att säkerställa att cyberbrott utreds än en allmän registreringsskyldighet.

Trots att propositionen inte innefattar någon allmän skyldighet att registrera identifieringsuppgifter kan teleföretag, tillhandahållare av mervärdestjänster och sammanslutningsabonnenter registrera identifieringsuppgifter för i lagen specificerade ändamål, som för att utreda missbruk av tjänsterna och för att möjliggöra fakturering. I de flesta fall har teleföretagen de facto haft tillgång till identifieringsuppgifter som är nödvändiga ur polisens synvinkel utan någon särskild registreringskyldighet. Enligt sakkunnigbedömningar ger förslaget goda och klarare definierade möjligheter att ingripa i sådan brottslighet som inte kan anses vara acceptabel användning av kommunikationstjänster.

Utskottet påpekar att om en allmän skyldighet att registrera identifieringsuppgifter tas in i lagen är det också viktigt att bedöma vilka konsekvenser det får för användarnas tilltro till den elektroniska kommunikationen. Hittills har användarna kunnat lita på att deras kommunikation är konfidentiell och att uppgifter inte registreras i större omfattning än vad som är absolut nödvändigt. Om en särskild registreringskyldighet tas in i lagen förändras den viktigaste principen i det gällande rättsläget och det kan få oanade effekter för människors beteende.

Vidare bör det observeras att registreringen resulterar i att först och främst inhemska och utländska teleföretag och deras multinationella underleverantörer fått tillgång till ett enormt data-material om den offentliga förvaltningens, näringslivets och enskilda personers kommunikationer hos oss. Att kunna garantera datasäkerheten i ett sådant material blir en kritisk fråga för hela samhället och därför bör den bedömas omsorgsfullt till denna del.

Kommunikationsministeriet har tillsatt en expertarbetsgrupp för att utreda vilka fördelar, kostnader och andra konsekvenser en allmän registreringskyldighet i verkligheten har. Inte bara kommunikationsministeriets särskilda arbetsgrupp utan också rådet för inrikes och rättsliga frågor i Europeiska unionen bedömer frågan. Utskottet konstaterar att det kan vara en nackdel för den nationella regleringen och inte

minst företagen i branschen om man redan på detta stadium antar ståndpunkter som står i strid med nationella eller europeiska synpunkter som formuleras först längre fram och som kan få konsekvenser för lagstiftningen. Med anledning av förvaltningsutskottets uttalande understryker utskottet att behovet av bestämmelser på lagnivå nogå bör övervägas i en separat utredning.

Dataskyddsavgift

Utskottet konstaterar att det i dagsläget är allt annat än lätt att i tekniskt hänseende hantera och behärska datasäkerheten. Det är livsviktigt att datasäkerheten är under kontroll för att näringslivet ska kunna blomstra, den internationella konkurrenskraften upprätthållas och förbättras och medborgarnas rättigheter och välfärd vara tryggade. Under expertutfrågningen påpekades det att det för de flesta bolag och privatpersoner är svårt eller i det närmaste omöjligt att behärska datasäkerheten, eftersom det handlar om synnerligen tekniska och komplicerade saker. Det är bara de största företagen, som har en lång rad experter för att upprätthålla datasäkerheten, och en liten krets av forskare och produktutvecklare inom datasäkerhetsbranschen som vet vad det faktiskt handlar om när man talar om datasäkerhet och dess underhåll och utveckling. Därför måste den myndighet som ansvarar för den nationella datasäkerheten med synnerligen kort varsel kunna sammanställa klara och tydliga anvisningar om datasäkerheten som förstås av vanliga medborgare. Anvisningarna behövs exempelvis på grund av de skadeprogram som på några dygn, ja t.o.m. på några timmar sprider sig över hela jordklotet och slår ut ett oräkneligt antal datorer.

Kommunikationsverket är per definition den nationella datasäkerhetsmyndigheten. Utfrågade experter har hävdade att de för den nya verksamheten anvisade resurserna inte förslagit utan bara räckt till för att statistikföra utländska och finländska anmälningar om kränkningar av datasäkerheten och utläggning på webben av varningar om dessa kränkningar. Vidare har det framhållits att Kommunikationsverket med nu-

varande organisation, resurser och målsättning inte har några möjligheter att nå de primära mål som uppställts för upprätthållandet av datasäkerheten och att det därför absolut behövs större satsningar än hittills. Utskottet vill understryka att också om experter vid utfrågningen ansett att kommunikationsverkets insatser för datasäkerheten varit utmärkta och fått tack från många olika håll, minskar det inte behovet av insatser för utveckling av datasäkerheten för att ribban fortfarande ska ligga högt. Det är ytterst viktigt, menar utskottet, att Kommunikationsverkets verksamhet och resurser, inbegripet rätten att få information, säkras för att informationssamhället faktiskt ska vara informationssäkert och medborgarna få sina grundläggande fri- och rättigheter tillgodosedda.

Regeringen gör i avsnittet om propositionens verkningar en bedömning av vilka resurser tillsynsmyndigheterna behöver. På denna punkt är det helt klart att tillsynsmyndigheterna ska ha fullgoda möjligheter att utöva sin verksamhet. Kommunikationsverket har nyss fått ett litet tillskott av personella resurser för att sköta datasäkerhetsuppgifterna, men det kan mycket väl bli aktuellt att längre fram fundera på extra resurser. Kommunikationsministeriet har planer på att efter lagens ikraftträdande låta de med tanke på lagens tillämpning viktigaste aktörerna bege sig ut på fältet. I planerna ingår bl.a. information och utbildning av olika slag. Dessutom har Kommunikationsministeriet tillsatt en grupp för att följa verkställigheten av lagen och denna grupp kommer att ta ställning till eventuella problem som uppstår vid verkställigheten.

I propositionen föreslås att teleföretag som utövar anmälningspliktig eller koncessionsberoende verksamhet ska vara skyldiga att till Kommunikationsverket betala en årlig dataskyddsavgift för finansiering av den nationella CERT-verksamheten. Betalningsskyldigheten gäller över huvud taget inte företag som bedriver allmän televerksamhet i liten skala och som inte behöver göra anmälan. Den föreslagna avgiftsbördan fördelar sig rättvisare mellan företagen i branschen och bestämmelsen tar också hänsyn till de krav som företag av olika storlek ställer på

Kommunikationsverkets verksamhet. Företag med stor omsättning bedriver normalt verksamhet av olika slag och bedriver affärsverksamhet på en geografiskt större marknad i Finland än små företag. Dessa företags verksamhet ställer följaktligen större krav på Kommunikationsverkets verksamhet än småföretagens och därför stiger avgiften när omsättningen ökar. Meningen är att den i propositionen föreslagna dataskyddsavgiften ska gå till att täcka dessa sammanlagda kostnader.

Teleföretagens avgiftsbörda kommer att vara ungefär densamma som nu. Den föreslagna dataskyddsavgiften motsvarar avgiften i lagen om datasekretess vid telekommunikation. Dataskyddsavgiften beräknas inbringa totalt ca 540 000 euro 2004.

I takt med att informationssamhället utvecklas kan det hända att också myndigheterna måste ge större akt på datasäkerheten inte bara när det gäller nät- och kommunikationstjänster utan också andra med hänsyn till denna utveckling viktiga tjänster. I det sammanhanget bör frågan vem som ska betala skatter på näringsverksamhet typ dataskyddsavgift tas upp till ny prövning. För att trenden ska kunna föregripas på behörigt sätt tillsatte Kommunikationsministeriet redan den 15 december 2003 en arbetsgrupp för att göra en sammanhållen utredning av Kommunikationsverkets alla avgifter. Arbetsgruppen ska också diskutera olika alternativ visavi dataskyddsavgiften. Gruppens mandat löper från den 1 januari till den 30 november 2004 men kan vid behov få sitta längre.

Utskottet påpekar att bestämmelserna om dataskyddsavgift strukturellt motsvarar kommunikationsmarknadsavgiften enligt kommunikationsmarknadslagen och hänvisar till grundlagsutskottets utlåtande GrUU 61/2002 rd, där avgiften ansågs ha karaktären av skatt. I det sammanhanget föreslog Kommunikationsutskottet ett uttalande där det förutsattes att de medel som inflyter genom kommunikationsmarknads- och teletreprenadavgiften oavkortade går till att täcka kostnaderna för verksamheten vid Kommunikationsverket. Utskottet ser också nu det nödvändiga i att avgiften, som intäktsförs i bud-

geten, oavkortad går till att täcka Kommunikationsverkets utgifter för dataskyddet (*Utskottets förslag till uttalande*).

Förvaltningsutskottet påpekar i sitt utlåtande att också dataombudsmannen får nya övervakningsuppgifter och att det därför är viktigt att dataombudsmannen får adekvata resurser för sina uppgifter. Kommunikationsministeriet uppger att man under beredningen av förslaget diskuterat tillsynsmyndigheternas behov av resurser. Enligt ministeriet bör frågan utredas separat för dataombudsmannens vidkommande i samband med statsbudgeten. När myndigheterna påförs nya uppgifter i lag måste de också få adekvata resurser för att kunna klara av dem på behörigt sätt, understryker utskottet. Därför bör i budgeten förutom dataskyddsavgiften också upptas annan finansiering för att andra myndigheter som svarar för dataskyddet än Kommunikationsverket ska kunna sköta sina uppgifter.

Detaljmotivering

Lagrubriken. Grundlagsutskottet påpekar i sitt utlåtande att lagrubriken i propositionen bör ses över i enlighet med kraven på god lagskrivning. Kommunikationsutskottet föreslår att det överflödiga "lag" stryks så att rubriken lyder "lag om dataskydd vid elektronisk kommunikation". Utskottet har gjort denna ändring i rubriken.

4 §. Den konfidentiella naturen hos meddelanden, identifieringsuppgifter och lokaliseringsuppgifter. Enligt grundlagsutskottets utlåtande strider 4 § 2 mom. i lagförslaget mot yttrandefrihetsbestämmelserna i 12 § 1 mom. i grundlagen när det gäller identifieringsuppgifter för publicerade meddelanden. Grundlagsutskottet kräver därför att identifieringsuppgifter stryks i bestämmelsen. Det påpekar vidare att grundlagens skydd av yttrandefriheten också gäller anonym kommunikation. Kommunikationsutskottet föreslår därför att momentet formuleras så att identifieringsuppgifter som ansluter sig till meddelanden är konfidentiella också när meddelandena är föremål för allmän mottagning. I enlighet med grundlagsutskottets utlåtande föreslår kommuni-

kationsutskottet ett tillägg om att bestämmelser om utlämnande av identifieringsuppgifter i nätmeddelanden finns i 17 § i lagen om yttrandefrihet i masskommunikation. Utskottet har ändrat 2 mom. i enlighet med detta.

7 §. Registrering på användarens terminalutrustning av uppgifter om användning av tjänster och användning av dessa uppgifter. Grundlagsutskottet har pekat på att 1 och 2 mom. är oklara. Exempelvis kan ordalydelsen i 1 mom. ge den bilden att bestämmelsen även gäller användaren själv. Kommunikationsutskottet föreslår att det uttryckligen anges att registrering och användning av uppgifter är tillåten för den som tillhandahåller tjänsten.

Enligt grundlagsutskottet är det oklart vad 2 mom. förbjuder respektive tillåter. Utskottet påpekar därför att 2 mom. måste uttryckas klarare både i fråga om hänvisningen till 1 mom. och i fråga om vem bestämmelsen gäller. På detta sätt blir det också väsentligt klarare vad 2 mom. förbjuder respektive tillåter. Således föreslår utskottet att hänvisningen till 1 mom. preciseras att gälla tjänstetillhandahållarens skyldighet att lämna uppgifter och användarens rätt att förbjuda registrering och användning av uppgifter.

Grundlagsutskottet anser att 3 mom. bör ses över, eftersom formuleringen "utan att integritetsskyddet äventyras mer än nödvändigt" anmars med sitt motsatsförhållande pekar mot möjligheten till nödvändigt äventyrande av rättigheter. Kommunikationsutskottet föreslår därför att momentet formuleras så att sådan registrering och användning som avses i paragrafen inte får begränsa skyddet mer än vad som är nödvändigt.

Utskottet har ändrat paragrafen i enlighet med detta.

8 §. Allmänna bestämmelser om behandlingen. Grundlagsutskottet anser att problemet med den mycket breda definitionen lindras något av kravet i 8 § 3 mom. att behandlingen måste vara förknippad med ändamålet. Behandling enligt 9—14 § är enligt paragrafen tillåten bara i den omfattning som behandlingens ändamål kräver. I 5 § ingår relevanta bestämmelser om tystnads-

plikt och förbud mot utnyttjande av uppgifter. Ett problem är ändå att definitionen på behandling också innehåller utlämnande av uppgifter. Enligt motiven till propositionen kan uppgifter på grund av 8 § 3 mom. bara lämnas ut till de som har rätt att behandla uppgifterna i relevanta situationer. På grund av kravet på exakthet anser grundlagsutskottet det viktigt att lagen får en bestämmelse om detta. Kommunikationsutskottet anser att 3 mom. dels behöver preciseras, dels behöver en uttrycklig bestämmelse om utlämnande. Utskottet föreslår därför tillägg av en mening enligt vilken det är tillåtet att lämna ut identifieringsuppgifter endast till dem som i den berörda situationen har rätt att behandla uppgifter.

Den första meningen i 3 mom. bör enligt grundlagsutskottet ses över, eftersom formuleringen "utan att skyddet ... äventyras mer än nödvändigt" annars med sitt motsatsförhållande pekar mot möjligheten till nödvändigt äventyrande av rättigheter. Kommunikationsutskottet föreslår därför att momentet formuleras så att behandling inte får begränsa skyddet av konfidentiella meddelanden och integritetsskyddet mer än vad som är nödvändigt.

Utskottet har ändrat momentet i enlighet med detta.

10 §. Behandling för fakturering. Det föreslagna 3 mom. ger dem som tillhandahåller informationssamhällets tjänster möjlighet att få identifieringsuppgifter från teleforetag och att behandla uppgifter för fakturering. Den gällande lagen har inte tillåtit att den som tillhandahåller informationssamhällets tjänster får dessa uppgifter från teleforetag, utan faktureringen har skett via teleforetagen. Bestämmelsen erbjuder således aktörerna nya tillvägagångssätt och begränsar på intet sätt dessa tjänsteproducenters övriga behandling av identifieringsuppgifter. I övrigt gäller den föreslagna lagens bestämmelser om behandlingen av identifieringsuppgifter bara teleforetag, tillhandahållare av mervärdestjänster (i snäv bemärkelse enligt lagen) och sammanslutningsabonnenter. Utskottet noterar att en kommunikationspart dessutom får behandla identifieringsuppgifter när de har sam-

band med den egna kommunikationen. Även en tillhandahållare av informationsamhällets tjänster kan vara part i kommunikationen vid en beställning av en tjänst, varvid tillhandahållaren även får behandla den andra partens (den som beställt tjänsten) identifieringsuppgifter för andra ändamål än fakturering. Utskottet understryker att denna reglering inte på något sätt försvårar eller komplicerar den nuvarande verksamheten för att erbjuda eller tillhandahålla tjänster. Tagen ur sitt sammanhang torde bestämmelsen ändå gå att förstå så att den även begränsar behandlingen av andra identifieringsuppgifter än de som teleforetag lämnar ut. Enligt sakkunnigutfrågningen är detta emellertid inte avsikten med den föreslagna bestämmelsen.

Med beaktande av bestämmelsens syfte anser utskottet att det finns skäl att uttrycka 3 mom. mer exakt: den rätt som tillhandahållare av informationssamhällets tjänster har att behandla nödvändiga identifieringsuppgifter och andra uppgifter som är nödvändiga för faktureringen begränsas att gälla uppgifter från teleforetaget. Därför föreslår utskottet att momentet ändras i enlighet med detta.

Utskottet har följaktligen formulerat om momentet.

13 §. Behandling i fall av missbruk. Enligt den föreslagna paragrafen får teleforetag, tillhandahållare av mervärdestjänster och sammanslutningsabonnenter behandla identifieringsuppgifter, "om det är behövligt för att upptäcka, förhindra och utreda sådant missbruk som gäller användningen av nättjänsten, kommunikationstjänsten eller mervärdestjänsten samt för att inleda förundersökning av missbruket". Ett exempel på sådant missbruk som gäller användning kan vara uppkoppling till en avgiftsbelagd tjänst med hjälp av ett obehörigt erhållit lösenord eller användning av en avgiftsfri tjänst för ett ändamål som väsentligt avviker från vad som avtalats med den som tillhandahåller tjänsten. Detta gäller ändå inte ett eventuellt avtalsbrott som hör samman med tjänsteinnehållet, såsom genom strafflagen straffbelagd ärekränkning per telefon, även om detta skulle vara förbjudet enligt

avtalet mellan teleföretaget och abonnenten. Det föreslagna momentet ger rätt att behandla uppgifter för att upptäcka och förhindra missbruk, men förundersökningen avseende brott ska handhas av förundersökningsmyndigheterna.

I praktiken går det dock att upptäcka missbruk enbart med hjälp av t.ex. automatisk mätning av kapacitetsutnyttjandet och intrångsskydd. Med hjälp av dessa går det t.ex. att se om någon olovligen börjat använda hela den datakommunikationskapacitet som reserverats för ett höghus så att andra anslutningar inte fungerar som de ska. Dessa tekniska tillämpningar används också för automatiskt uppdagande av fel och störningar. Det är först när man går in för att mer exakt utreda orsaken som man kan bedöma om det varit fråga om missbruk eller fel. Upp-täckande av missbruk förutsätter behandling av identifieringsuppgifter, som således är nödvändig för att missbruk ska kunna upptäckas i förväg. Därför behövs rätt att lämna ut identifieringsuppgifter i vissa fall. Exempelvis i fall där missbruket gäller flera tjänsteproducenters tjänster och kommunikationsnät eller sammanslutningsabbonnents interna nät kan tjänsteproducenterna och sammanslutningsabbonnenterna i praktiken bekämpa missbruket endast genom gemensamma åtgärder. Det bör dock observeras att identifieringsuppgifter i dessa situationer kan utlämnas endast till dem som har rätt att behandla identifieringsuppgifter i den aktuella situationen. Det är särskilt viktigt att notera att behandlingen i den föreslagna paragrafen begränsas till det ändamål som paragrafen tillåter och att utlämningen av uppgifter således också är begränsad till det ändamålet. Den som behandlar uppgifter måste se till behandlingen i enlighet med 8 § 3 mom. inte begränsar integritetsskyddet mer än vad som är nödvändigt.

Eftersom bestämmelsen är oklart formulerad och kan ge upphov till missförstånd, föreslår utskottet att missbruk som gäller användningen mer klart anges gälla obehörig gratisanvändning av avgiftsbelagda tjänster eller motsvarande missbruk.

Utskottet har ändrat paragrafen i enlighet med detta.

16 §. Behandling och utlämnande av lokaliseringsuppgifter. Enligt grundlagsutskottets utlåtande bör den första meningen i 3 mom. ses över, eftersom formuleringen ("utan att i onödan äventyra integritetsskyddet") annars med sitt motsatsförhållande pekar mot möjligheten till nödvändigt äventyrande av rättigheter. Kommunikationsutskottet föreslår därför att momentet formuleras så att behandling inte får begränsa integritetsskyddet mer än vad som är nödvändigt. Utskottet har ändrat momentet i enlighet med detta.

19 §. Skyldighet att handha dataskyddet. Enligt grundlagsutskottet kan de administrativa och tekniska åtgärder som behövs för att handha dataskyddet enligt propositionens motiv gälla säkerhet för verksamheten, datatrafiken, datorutrustningen, programmen och datamaterialet. Denna typ av bestämmelser som dels preciserar skyldighetens innehåll, dels begränsar Kommunikationsverkets normgivningsbefogenhet bör enligt utlåtandet lämpligen tas in i lagen. Därför föreslår Kommunikationsutskottet att paragrafen preciseras så att handhavandet av dataskyddet för tjänster och behandling avser åtgärder för att trygga säkerheten för verksamheten, datatrafiken, utrustningen och programmen samt för datamaterialet. Utskottet har ändrat momentet i enlighet med detta.

20 §. Åtgärder för att genomföra dataskyddet. Paragrafen bör kompletteras med en bestämmelse om att åtgärderna ska vidtas med hänsyn till ett krav på omsorgsfullhet som ingår i yttrandefriheten och att åtgärderna måste stå i rätt proportion till hur allvarlig störningen är, föreslår grundlagsutskottet i sitt utlåtande. Det är en liten brist med tanke på proportionalitetskravet att bestämmelsen inte nämner att åtgärderna är tillfälliga. Å andra sidan är det inbyggt i kravet på nödvändighet att åtgärderna måste upphöra eller avbrytas så snart de inte längre behövs. Detta bör dock sägas ut i bestämmelsen, anser grundlagsutskottet.

Vidare anser grundlagsutskottet att paragrafen måste formuleras bättre. För tydlighetens

skull vore det bättre om till exempel syftena med åtgärderna inte nämndes på så många olika ställen i paragrafen.

Dessutom påpekar grundlagsutskottet att det enligt motiveringen med stöd av 1 mom. är tillåtet att dels hindra att ett meddelande kommer fram, dels hindra att ett meddelande förmedlas. På grund av kravet på exakthet måste detta skrivas ut i bestämmelsen, understryker grundlagsutskottet. Därför föreslår utskottet att 1 mom. inte bara ska föreskriva om mottagande utan också om förmedling av meddelanden.

Begreppet skadliga program kan ges många betydelser vid reglering av kommunikation, säger grundlagsutskottet. Därför är det inte helt problemfritt med avseende på exakthetskravet att en tredje part gentemot parterna i kommunikationen har rätt att ta bort skadliga program ur meddelanden. I det aktuella fallet råder det kanske ingen ovisshet om vilka skadliga program som avses. Ändå är det bäst att bestämmelsen preciseras, anser grundlagsutskottet. Utskottet föreslår att bestämmelsen om skadliga program preciseras till att omfatta skadliga program som äventyrar dataskyddet.

Kravet att bestämmelserna ska vara exakta och noga avgränsade medför att förslaget är problematiskt när det dels tillåter att en mottagare förhindras att ta emot ett meddelande och ett program i ett meddelande kan tas bort, dels att "andra nödvändiga åtgärder" vidtas. Detta framhåller grundlagsutskottet. Uttryckt är mycket tillåtande och inskränker åtgärderna bara med hjälp av kravet på nödvändighet. Utifrån formuleringen förefaller också andra åtgärder av teknisk karaktär att vara möjliga än bara sådana som är jämförliga med dem som specifikt anges i bestämmelsen. Bestämmelsen måste preciseras till exempel med en passus om jämförliga åtgärder. Annars kan lagförslaget inte behandlas i vanlig lagstiftningsordning. Grundlagsutskottet kräver en precisering vad beträffar andra nödvändiga åtgärder. Utskottet föreslår att dataskyddet ska kunna säkras också genom att andra åtgärder av teknisk karaktär får genomföras om de är jämförliga med de övriga åtgärderna.

Enligt grundlagsutskottet bör den sista meningen i 2 mom. ses över för att den kontradiktoriska slutsats som kan dras ur formuleringen "utan att ... skyddet äventyras i onödan" inte ska peka mot möjligheten till nödvändigt äventyrande av rättigheter. Utskottet föreslår att paragrafen formuleras om på det sätt som grundlagsutskottet föreslår. För tydlighetens skull föreslår utskottet dessutom att de tre meningarna i 2 mom. delas upp på tre olika moment. Då blir den tredje meningen 4 mom. med den formulering som grundlagsutskottet föreslår. Följaktligen blir 3 mom. i lagförslaget 5 mom.

Bestämmelsen i 2 mom. om rätten att göra ingrepp i innehållet i ett meddelande är enligt grundlagsutskottet inte entydigt och medför därför tolkningssvårigheter. Det är oklart om bestämmelsen avser att ett meddelande kontrolleras och raderas med hjälp av tekniska medel eller om ett meddelande med stöd av bestämmelsen får öppnas och att någon kontrollerar om det är skadligt. Utskottet föreslår att lagförslaget preciseras med att ingrepp i innehållet i ett meddelande bara får göras med hjälp av tekniska medel för att kontrollera och radera meddelandet.

Passusen om misstanke i 2 mom., "om det finns sannolika skäl att misstänka", är så formulerad att den synbarligen inte avser det brott enligt 38 kap. 5 § i strafflagen som nämns i momentet, påpekar grundlagsutskottet. Utskottet föreslår därför att formuleringen "om det finns sannolika skäl att misstänka" också nämns i samband med brottet enligt 38 kap. 5 § i strafflagen.

Vidare föreslår utskottet att hänvisningen till 1 mom. i 3 mom. utvidgas till att omfatta tekniskt avvärjande och undanröjande av störningar i dataskyddet i den mening som avses i paragrafen.

Utskottet har formulerat om paragrafen i enlighet med resonemanget ovan.

21 §. Dataskyddsanmälningar. Syftet med paragrafen är att teleföretagen och tillhandahållarna av mervärdestjänster utan dröjsmål måste underrätta abonnenten när dataskyddet är hotat. Samtidigt måste de underrätta abonnenten om vilka

åtgärder abonnenten och användaren kan vidta för att avvärja hotet och hur stora kostnaderna sannolikt är. Regeringen har inte velat lägga fast skyldigheten vid bara ett enda sätt att informera abonnenten, eftersom det kan förekomma situationer då offentliga meddelanden kan äventyra kravet på konfidentialitet. Hur abonnenten informeras måste avgöras från fall till fall. Däremot finns inte möjligheten att man avgör från fall till fall om ett meddelande över huvud taget behövs och när det i så fall ska göras. Uttrycket "utan dröjsmål" indikerar att abonnenten ska informeras så snart det är möjligt och kan göras på ett säkert sätt.

Grundlagsutskottet menar att det dessutom kan behövas bestämmelser som föreskriver att beställaren och användaren till exempel efter att en störning eller en kränkning har avvärjts måste underrättas om vilka åtgärder som vidtagits för att avvärja det särskilda hotet mot dataskyddet och vilka konsekvenser åtgärderna kan ha haft för kommunikationen.

Kommunikationsutskottet anser att en skyldighet att informera i efterhand behövs eftersom den fundamentala innebörden ingår i traditionell och normal kundtjänst. Om bestämmelser skrivs in bör det göras bara i den omfattning som är nödvändig för syftet och utan att teleföretagen åläggs skyldigheter som avviker från de normala. Utskottet menar att informationsskyldigheten måste vara generell och avse information i efterhand. Detta för att aktörerna ska kunna reagera snabbt i liknande situationer. Tanken är dock att information om åtgärderna ska gå ut i realtid i mån av möjlighet. Det är klart att skyldigheten inte får innebära att teleföretagen måste informera om saker som ingår i affärshemligheten eller om saker som kan försvåra möjligheterna att lösa det aktuella problemet. Dessutom bör det uppmärksammas att skyldigheten eventuellt bara kan gälla teleföretag. I dagsläget bör skyldigheten inte utsträckas till att omfatta tillhandahållare av mervärdestjänster och sammanslutningsabonnenter. Utskottet föreslår att ett nytt 3 mom. om detta läggs till efter 1 och 2 mom.

Då blir 3 mom. i lagförslaget 4 mom. Momentet får dessutom en hänvisning till 3 mom.

Förvaltningsutskottet anser i sitt utlåtande att lagen måste få bestämmelser som anger spelreglerna för ersättning till kunden vid direkta skador. Enligt kommunikationsministeriet lades det under beredningens gång inte fram några motiverade skäl för varför principerna för normalt skadeståndsrättsligt och avtalsrättsligt ansvar inte skulle räcka till i de aktuella situationerna. Utskottet anser därför att reglerna i det föreslagna tillägget om informationsskyldigheten på behörigt sätt säkerställer kundernas rättssäkerhet och garanterar att de får ut sin rätt vid eventuella skador.

Utskottet har ändrat paragrafen i enlighet med detta.

29 §. Hindrande av mottagande av direktmarknadsföring. Enligt grundlagsutskottet bör den sista meningen i paragrafen ses över. Detta för att den kontradiktoriska slutsatsen av uttrycket "utan att ... skyddet äventyras i onödan" inte ska peka mot möjligheten till nödvändigt äventyrande av rättigheter. Utskottet föreslår därför att bestämmelsen preciseras med att åtgärderna ska genomföras noggrant och att de inte får begränsa yttrandefriheten, skyddet för förtroliga meddelanden eller skyddet för privatlivet mer än vad som är nödvändigt. Kommunikationsutskottet har ändrat paragrafen i enlighet med detta.

33 §. Styrnings- och övervakningsmyndigheterna rätt att få uppgifter. Grundlagsutskottet anser att 1 mom. vara svårbegriplig och menar att paragrafen lämpligen kunde preciseras. Samtidigt framhåller grundlagsutskottet visserligen att regleringen inte medför några problem med avseende på 10 § i grundlagen, om 1 mom. inte tolkas så att det innebär en i förhållande till bestämmelserna i 2 och 3 mom. självständig rätt att få uppgifter om konfidentiella meddelanden och innehållet i dem. Utskottet föreslår därför att "Kommunikationsverket och dataombudsmanen" läggs till i sista meningen i 1 mom. Dessutom bör paragrafen, enligt grundlagsutskottet, preciseras så att myndigheternas rätt att få up-

pgifter bara gäller uppgifter som är nödvändiga för tjänsteutövningen, trots att bestämmelsen i första hand gäller andra uppgifter än sådana som har relevans för skyddet av personuppgifter. Kommunikationsutskottet föreslår därför att "som kommunikationsministeriet behöver" i den första meningen i 1 mom. ersätts med "som är nödvändiga för att de ovan nämnda myndigheterna skall kunna utföra ...".

Grundlagsutskottet påpekar att ordet "vahingonteko" i 3 mom. 4 punkten saknas i den finska lagtexten. Utskottet lägger till ordet i den finska lagtexten.

Med tanke på konsekvent lagstiftning är det inte bra att skyldigheten att utplåna uppgifter som fåtts med stöd av 3 mom. i 5 mom. kopplas ihop med behandlingen av brott- eller civilmål och förvaltningsärenden. Utskottet föreslår att "brott- eller civilmål eller förvaltningsärenden" stryks i 5 mom.

Utskottet har ändrat paragrafen i enlighet med detta.

36 §. Rätt för vissa andra myndigheter att få uppgifter. I 36 § finns bestämmelser om vissa andra myndigheters än styr- och övervakningsmyndigheternas rätt att få uppgifter, påpekar förvaltningsutskottet i sitt utlåtande. I 2 mom. 2 punkten nämns bara rätt att få uppgifter på grundval av samtycke från abonnenten. Det händer emellertid att abonnemangskortet byts ut i mobilterminaler vid stöld. Då kan ägaren till terminalutrustningen sannolikt inte betraktas som abonnent. Förvaltningsutskottet föreslår att lagrummet ska föreskriva att ägaren till en terminalutrustning har samma rättigheter som abonnenten.

Vid utfrågningen av de sakkunniga framhölls det att polisens rätt att få uppgifter som omfattas av telehemligheten är utspridd på många olika lagar. Bestämmelser om polisens rätt att få uppgifter finns i tvångsmedelslagen, polislagen och i den föreslagna lagen om dataskydd vid elektronisk kommunikation. I tvångsmedelslagen finns det bestämmelser om teleavlyssning, teleövervakning och rätt att inhämta lokaliseringssuppgifter för mobilapparater i syfte att utreda brott. Vid teleavlyssning utreds innehållet i

ett telemeddelande. Vid teleövervakning inhämtas identifieringsuppgifter om telemeddelanden och lokaliseringssuppgifter om mobilapparater. Dessutom ingår tillfällig stängning av teleabonnemang och teleterminaler i teleövervakning. När lokaliseringssuppgifter om mobilapparater inhämtas är det fråga om att uppgifter som inte ingår i teleövervakning inhämtas beträffande från vilken teleapparat det vid en viss tidpunkt har registrerats uppgifter i telesystemet från en basstation i närheten av en viss plats. I polislagen finns bestämmelser om teleövervakning i syfte att förhindra brott och om rätt för polisen att få kontaktuppgifter som inte finns i offentliga kataloger. I den nu föreslagna formen ingår också bestämmelser om rätt för polisen att få uppgifter som specificerar också andra teleterminaler eller teleabonnemang. Polisen får uppgifterna för tjänsteutövning. I den föreslagna lagen om dataskydd vid elektronisk kommunikation föreskrivs om polisens rätt att för utredning av brott få identifieringsuppgifter om telemeddelanden utifrån samtycke från användaren eller liknande samtycke. Vid utfrågningen av de sakkunniga kom det fram att lagsystematiken härnäst kunde vara uppbyggd så att tvångsmedelslagen har bestämmelser om teleavlyssning, rätt att få identifieringsuppgifter om telemeddelanden och inhämtande av lokaliseringssuppgifter för mobilapparater i syfte att utreda brott. Polislagen skulle då ha bestämmelser om teleavlyssning och eventuellt också om inhämtande av lokaliseringssuppgifter för mobilapparater i syfte att förebygga brott. Vidare kan bestämmelser om rätt att få andra uppgifter som omfattas av telehemligheten i syfte att förebygga och utreda brott och för annan polisiär tjänsteutövning ingå i polislagen.

Vid utfrågningen av de sakkunniga kom det fram att polisen bör få större befogenheter att få uppgifter som omfattas av telehemligheten. Utskottet påpekar dock att utvidgade befogenheter bör bedömas dels med hänsyn till polisens behov att få uppgifter i samband med utredning av enskilda brott, dels i ett större perspektiv kring frågan vilken relevans det har om brottet begås med hjälp av elektronisk kommunikation eller

om det är en annan typ av brott där det krävs uppgifter om elektronisk kommunikation för att brottet ska kunna förhindras eller utredas. Dessutom bör konsekvenserna av det faktum att användaren ger sitt samtycke eller något annat samtycke inhämtas bedömas i relation till myndigheternas rätt att få information. Utskottet påpekar dessutom att alla meddelanden inte berörs av samma konfidentialitetsnivå.

I 36 § 2 mom. 2 punkten nämns bara uppgifter som bygger på samtycke från abonnenten. I levande livet har det förekommit att abonnemangskorten byts ut i terminalutrustning vid stöld. I likhet med förvaltningsutskottet anser kommunikationsutskottet att ägaren till terminalutrustning i sådana fall sannolikt inte kan betraktas som abonnent. Därför föreslår utskottet att 2 mom. ändras till att också ägaren till en terminalutrustning kan ge sitt samtycke till de åtgärder som nämns i 2 punkten.

Med hänvisning till utfrågningen av de sakkunniga anser kommunikationsutskottet att övriga utvidgningar och ändringar i polisens rätt att få uppgifter bör genomföras utifrån en samlad bedömning av polisens rätt att få information när polislagen revideras.

Utskottet har ändrat momentet i enlighet med detta.

Förslag till beslut

Med stöd av det ovan anförda föreslår kommunikationsutskottet

att lagförslagen 2—8 godkänns utan ändringar,

att lagförslag 1 godkänns med följande ändringar (Utskottets ändringsförslag) och

att ett uttalande godkänns (Utskottets förslag till uttalande).

Utskottets ändringsförslag

1.

Lag

(utesl.) om dataskydd vid elektronisk kommunikation

I enlighet med riksdagens beslut föreskrivs:

1 kap.
Allmänna bestämmelser
1—3 §
(Som i RP)

2 kap.
Skydd av integritet och konfidentiella meddelanden
4 §

Den konfidentiella naturen hos meddelanden, identifieringsuppgifter och lokaliseringsuppgifter

(1 mom. som i RP)

Ett meddelande är inte konfidentiellt om det är föremål för allmän mottagning. Till ett meddelande anslutna identifieringsuppgifter är emellertid konfidentiella. I 17 § lagen om yttrandefrihet i masskommunikation (460/2003) föreskrivs om utlämnande av nätmeddelandes identifieringsuppgifter.

(3 mom. som i RP)

5 och 6 §
(Som i RP)

7 §

Registrering på användarens terminalutrustning av uppgifter om användning av tjänster och användning dessa uppgifter

Registrering med hjälp av kommunikationsnät på användarens terminalutrustning av cookies och andra uppgifter om användningen av tjänster samt användningen av dessa uppgifter är tillåten *för den som tillhandahåller tjänsten*, om *denne* ger användaren begripliga och fullständiga uppgifter om ändamålet med registreringen eller användningen. Samtidigt skall användaren ges möjlighet att förbjuda registrering eller användning enligt detta moment.

Bestämmelserna i 1 mom. *om skyldighet för den som tillhandahåller tjänsten att ge uppgifter och användarens rätt att förbjuda registrering eller användning* gäller inte sådan registrering eller användning av uppgifter, vars enda syfte är att förmedla meddelanden eller underlätta förmedlingen av meddelanden via kommunikationsnäten eller som är nödvändig för att tillhandahålla sådana tjänster som abonnenten eller användaren av tjänsten uttryckligen har begärt.

Ovan i denna paragraf avsedd registrering och användning är tillåten endast i den omfattning som tjänsten kräver och *får inte begränsa integritetsskyddet (utesl.)* mer än nödvändigt.

3 kap.

Behandling av meddelanden och identifieringsuppgifter

8 §

Allmänna bestämmelser om behandlingen

(1 och 2 mom. som i RP)

Behandling enligt 9 — 14 § är tillåten endast i den omfattning som behandlingens ändamål kräver och behandlingen *får inte begränsa skyddet av konfidentiella meddelanden eller integritetsskyddet mer än nödvändigt. Identifieringsuppgifter får endast överlämnas 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 annat bestäms i lag.

9 §
(Som i RP)

10 §

Behandling för fakturering

(1 och 2 mom. som i RP)

Den som tillhandahåller informationssamhällets tjänster och som avses i lagen om tillhandahållande av informationssamhällets tjänster (458/2002) kan behandla identifieringsuppgifter *som den erhållit av ett teleföretag och* som är nödvändiga för fakturering av bild- och ljudinspelningar och andra avgiftsbelagda tjänster som förmedlas genom ett av ett teleföretag administrerat kommunikationsnät samt andra för faktureringen nödvändiga uppgifter, om den abonnent eller användare som uppgifterna gäller har gett sitt samtycke.

(4—6 mom. som i RP)

11 och 12 §
(Som i RP)

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 sådant missbruk som gäller *obehörig gratis-användning av enstaka avgiftsbelagda tjänster eller motsvarande missbruk inom nättjänsten, kommunikationstjänsten eller mervärdestjänsten* samt för att inleda förundersökning av missbruket.

14 och 15 §
(Som i RP)

4 kap.

Lokaliseringsuppgifter

16 §

Behandling och utlämnande av lokaliseringsuppgifter

(1 och 2 mom. som i RP)

Behandling är tillåten endast i den utsträckning som behandlingens ändamål kräver och *den får inte begränsa integritetsskyddet mer än nödvändigt*. Efter behandlingen skall lokaliseringsuppgifterna förstöras eller göras sådana att de inte kan förknippas med en abonnent eller användare, om inte annat bestäms i lag.

(4 mom. som i RP)

17 och 18 §
(Som i RP)

5 kap.

Dataskydd vid kommunikation

19 §

Skyldighet att handha dataskyddet

Ett teleföretag och den som tillhandahåller mervärdestjänster skall handha dataskyddet för sina tjänster. En sammanslutningsabonnent skall handha dataskyddet vid behandlingen av sina användares identifierings- och lokaliseringsuppgifter. *Handhavandet av dataskyddet för tjänster och behandling avser åtgärder för att trygga säkerheten för verksamheten, datatrafiken, utrustningen och programmen samt för datamaterialet. Åtgärderna skall anpassas till hur allvarliga hot som föreligger samt till den tekniska utvecklingens nivå och till kostnaderna.*

(2 och 3 mom. som i RP)

20 §

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 verkar för deras räkning rätt att vidta nödvändiga åtgärder för att säkra i 19 § avsett dataskydd genom att

1) *hindra förmedling och mottagande av elektronisk post, textmeddelanden och andra motsvarande meddelanden,*

2) *genom att ur meddelandena avlägsna skadliga program som äventyrar dataskyddet, samt*

3) *genom att vidta andra jämförbara åtgärder av teknisk natur*

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. *(Utesl.)*

Ingrepp får göras i meddelandets innehåll endast med tekniska medel för att kontrollera och avlägsna det 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.

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 skall avbrytas så snart det inte längre finns i denna paragraf nämnda förutsättningar för att vidta dem.

Kommunikationsverket kan ge närmare föreskrifter om det tekniska förfarandet för att avvärja i denna paragraf avsedda kränkningar av dataskyddet och för att eliminera störningar av dataskyddet.

21 §

Dataskyddsanmälningar

(1 och 2 mom. som i RP)

När ett teleföretag har avvärjt en betydande, mot dess tjänster riktad dataskyddskränkning eller ett hot om en sådan kränkning eller när det har avlägsnat en störning skall det på ett ändamålsenligt sätt informera om vilka åtgärder som vidtagits och om eventuella effekter på användningen av tjänsterna.

Kommunikationsverket kan ge närmare föreskrifter om innehållet i och utformningen av anmälningar som avses i 1 och 2 mom. samt om hur de skall ges in till Kommunikationsverket *eller anvisningar om innehållet i och formen för den information som avses i 3 mom.*

6 kap.

Samtalstjänster

22—25 §
(Som i RP)

7 kap.

Direktmarknadsföring

26—28 §

Direktmarknadsföring till fysiska personer

(Som i RP)

29 §

Hindrande av att direktmarknadsföring tas emot

På begäran av en användare har ett teleföretag och en sammanslutningsabonnent rätt att hindra att i 26 — 28 § avsedd direktmarknadsföring tas emot. Åtgärderna skall genomföras omsorgsfullt och *utan att yttrandefriheten eller skyddet av konfidentiella meddelanden eller integritetsskyddet begränsas mer än nödvändigt.*

8 kap.

Styrning och tillsyn

30—32 §
(Som i RP)

9 kap.

Rätt att få uppgifter

33 §

Styrnings- och övervakningsmyndigheternas rätt att få uppgifter

Utan hinder av sekretessbestämmelser eller av andra begränsningar som gäller utlämnande av uppgifter har kommunikationsministeriet, Kommunikationsverket och dataombudsmanen rätt att av teleföretag, av dem som tillhandahåller mervärdestjänster, av sammanslutningsabbonenter, av teleentreprenörer, av dem som tillhandahåller tjänster som behandlar uppgifter om användning av tjänster, av dem som bedriver direktmarknadsföring, av dem som tillhandahåller abonnentkatalog- eller nummerupplysnings-

tjänster samt av dem som verkar för dessa få sådana uppgifter om i denna lag avsedd, av ovan nämnda operatörer och företag bedriven verksamhet som är nödvändiga för att de ovan nämnda myndigheterna skall kunna utföra sina i denna lag föreskrivna uppgifter. *Kommunikationsministeriets, Kommunikationsverkets och dataombudsmannens rätt att få uppgifter* omfattar inte uppgifter om konfidentiella meddelanden, identifieringsuppgifter eller lokaliseringssuppgifter.

(2—4 mom. som i RP)

Kommunikationsverket och dataombudsmannen skall utplåna de uppgifter om konfidentiella meddelanden, identifierings- och lokaliseringssuppgifter som de fått med stöd av 2 och 3 mom. då uppgifterna inte mera behövs för att utföra de i 2 och 3 mom. föreskrivna uppgifterna eller för att handlägga *brottmål* som gäller dem. Uppgifter om konfidentiella meddelanden, identifierings- och lokaliseringssuppgifter skall utplånas senast inom två år eller då det är fråga om uppgifter för att utreda kränkning av dataskydd, senast inom tio år från utgången av det kalenderår under vilket uppgifterna erhöles eller då ett beslut eller en dom i ett ärende som avses i detta moment vann laga kraft.

(6 mom. som i RP)

34 och 35 §
(Som i RP)

36 §

Rätt för vissa andra myndigheter att få uppgifter

(1 mom. som i RP)

Utan hinder av den tystnadsplikt som föreskrivs i 5 § har polisen rätt att av ett teleföretag erhålla

(1 punkten som i RP)

2) med samtycke av abonnenten *eller ägaren av terminalutrustningen* identifieringsuppgifter om de meddelanden som sänts från en mobilteleapparat till den del detta är nödvändigt för att utreda brott på grund av vilket mobilteleapparat eller dess anslutning orättmätigt har kommit i någon annans besittning.

(3 mom. som i RP)

37 §
(Som i RP)

10 kap.

Dataskyddsavgift

38—40 §
(Som i RP)

11 kap.

Särskilda bestämmelser

41—44 §
(Som i RP)

Utskottets förslag till uttalande

*Riksdagen förutsätter att de medel som
inflyter genom dataskyddsavgiften an-*

*vänds oavkortade för Kommunikations-
verkets kostnader.*

Helsingfors den 19 maj 2004

I den avgörande behandlingen deltog

ordf. Markku Laukkanen /cent
vordf. Matti Kangas /vänst
medl. Leena Harkimo /saml
Saara Karhu /sd
Marjukka Karttunen /saml
Risto Kuisma /sd
Reino Ojala /sd
Erkki Pulliainen /gröna

Pertti Salovaara /cent
Arto Seppälä /sd
Timo Seppälä /saml
Harry Wallin /sd
Lasse Virén /saml
Raimo Vistbacka /saf
ers. Reijo Paajanen /saml
Lyly Rajala /saml.

Sekreterare var

utskottsråd Mika Boedeker.