KOMMUNIKATIONSUTSKOTTETS BETÄNKANDE 19/2008 rd

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

INLEDNING

Remiss

Riksdagen remitterade den 29 april 2008 en proposition med förslag till lag om ändring av lagen om dataskydd vid elektronisk kommunikation och vissa lagar som har samband med den (RP 48/2008 rd) till kommunikationsutskottet för beredning.

Utlåtanden

I enlighet med riksdagens beslut har grundlagsutskottet, förvaltningsutskottet och arbetslivs- och jämställdhetsutskottet lämnat utlåtanden i ärendet. Utlåtandena (GrUU 29/2008 rd, FvUU 32/2008 rd, AjUU 14/2008 rd) återges efter betänkandet.

Sakkunniga

Utskottet har hört

- grundlagsutskottets ordförande, riksdagsledamot Kimmo Sasi
- utskottsråd Petri Helander, riksdagen
- konsultativ tjänsteman Sanna Helopuro, kommunikationsministeriet
- lagstiftningsråd Helena Hynynen, justitieministeriet
- regeringsråd Raila Kangasperko, arbets- och näringsministeriet
- dataombudsman Reijo Aarnio, Dataombudsmannens byrå
- jurist Antti Innanen, Kommunikationsverket
- kriminalöverinspektör Marko Viitanen, Centralkriminalpolisen
- jurist Mikko Niva, Nokia Abp
- verkställande direktör Petteri Järvinen, Petteri Järvinen Oy
- jurist Paula Ilveskivi, Akava rf
- expert Mikko Nyyssölä, Finlands Näringsliv
- chefsjurist Timo Koskinen, Finlands Fackförbunds Centralorganisation FFC
- direktör Satu Kangas, Mediernas Centralförbund
- vice ordförande Ville Oksanen, Electronic Frontier Finland - EFFI ry
- juridisk chef Marko Lahtinen, FiCom
- advokat Klaus Nyblin.

Dessutom har skriftligt utlåtande lämnats av

— inrikesministeriet
— Elisa Abp
— TeleSonera Abp
— Finnet-förbundet rf
— Tjänstemannacentralorganisationen FTFC rf
— Helsingforsregionens handelskammare.

PROPOSITIONEN

I propositionen föreslår regeringen att lagen om dataskydd vid elektronisk kommunikation ska ändras. Dessutom föreslås vissa ändringar av främst teknisk karaktär 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. Sammanslutningsabonnenter ska få behandla uppgifter om bland annat avsändaren och mottagaren av elektronisk post och tidpunkten för kommunikationen, men inte innehållet i meddelandet.

Genom förslaget förbättras möjligheterna för teleföretag, leverantörer av mervärdestjänster och sammanslutningsabonnenter att ha hand om datasäkerheten för kommunikationsnät och kommunikationstjänster.

Dataombudsmannen ska övervaka sammanslutningsabonnenternas behandling av identifieringsuppgifter i missbrukssituationer. Dessutom föreslås Kommunikationsverket få mer omfattande rättigheter att lämna ut uppgifter i syfte att förebygga och utreda kränkningar av dataskyddet.

Lagarna avses träda i kraft den 1 januari 2009.

UTSKOTTETS ÖVERVÄGANDEN

Allmän motivering

Utskottet finner propositionen behövlig och lämplig. Följaktligen tillstyrker utskottet lagförslagen, men med följande anmärkningar och ändringsförslag.

Allmänt. Lagen om dataskydd vid elektronisk kommunikation antogs av riksdagen i juni 2004. Den syftar till att garantera konfidentialitet och integritet vid elektronisk kommunikation, men också att förbättra dataskyddet vid elektronisk kommunikation och medverka till en balanserad utveckling av flera olika elektroniska kommunikationstjänster. I 13 § föreskrivs det om behandlingen av meddelanden och identifieringsuppgifter i fall av missbruk. Ett teleföretag, den som tillhandahåller mervärdestjänster och sammanslutningsabonnenter får enligt paragrafen behandla identifieringsuppgifter för att upptäcka, förhindra och utreda gratisanvändning av en avgiftsbelagd tjänst inom nättjänsten, kommunikationstjänsten eller mervärdestjänsten eller annat jämförbart missbruk av en tjänst och för att göra missbruket föremål för förundersökning.

I betänkande KoUB 13/2004 rd framhåller kommunikationsutskottet bland annat att momentet i fråga avser åtgärder för att upptäcka och förhindra missbruk, men överlåter förundersökning av brott uteslutande till förundersökningsmyndigheterna. I praktiken går det dock att upptäcka missbruk bara med hjälp av t.ex. automatisk mätning av kapacitetsutnyttjandet och intrångsskydd, framhöll utskottet. 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 det går att bedöma om det varit fråga om missbruk eller fel. För att upptäcka missbruk måste identifieringsuppgifter behandlas, och så-

ledes är behandling nödvändig för att missbruk ska kunna upptäckas.

I propositionen gör regeringen en utvärdering av hur den gällande lagstiftningen har utfallit. Bland annat 13 § i lagen om dataskydd vid elektronisk kommunikation är så snävt formulerad att den inte ger sammanslutningsabonnenter tillräckligt stort svängrum, konstateras det i propositionen. Den gällande lagen tillåter inte att sammanslutningsabonnenter själva samlar in bevis för missbruk. I de flesta fall är dessutom teleövervakning inte tillåten. Bestämmelserna om rätten att behandla meddelanden och identifieringsuppgifter i fall av missbruk är tvetydiga i den gällande lagen och tillåter redan nu åtminstone delvis att identifieringsuppgifter behandlas, påpekar utskottet.

I undersökningar om underrättelseverksamhet och företagssäkerhet uppger ungefär 10 procent av de svarande företagen att de har upptäckt och 18 procent att de har misstänkt olagligt förvärv av information de senaste två åren. Det har brustit i företagens möjligheter att låta polisen undersöka olovligt röjande av företagshemligheter om de har getts ut elektroniskt. På grund av det oklara rättsläget har företagens försök att utreda frågan till och med kunnat leda till åtal för olaglig verksamhet.

Propositionen ger företagen bättre möjligheter att handla i och med att den täpper till den lucka i lagstiftningen som nu finns i den elektroniska omgivningen i skyddet av företagshemligheter. Den förtydligar det rådande oklara läget, lägger fast stränga villkor för behandling av identifieringsuppgifter och ger sammanslutningsabonnenterna bättre dataskydd, framhåller utskottet.

I 13 § i den gällande lagen krävs inga som helst föreberedande åtgärder för att uppgifter ska få behandlas. De med sanktion förknippade skyldigheterna att informera både före och efter är enligt utskottet en stor förbättring också i dataskyddet för användarna och deras rättssäkerhet.

Sett i ett internationellt perspektiv är vår reglering av dataskyddet vid elektronisk kommunikation mycket sträng, bland annat i jämförelse med övriga EU-medlemsstater. De föreslagna ändringarna innebär framför allt att bestämmelserna förtydligas beträffande både sammanslutningsabonnenter och användare, och undergräver inte dataskyddet som det har påstått offentligt.

Överlag har utskottet en positiv, men kritisk inställning till propositionen. Samtidigt vill utskottet framhålla att förslaget öppnar för möjligheter att missbruka befogenheterna. Det uppvägs dock delvis av klara och tydliga sanktioner för missbruk. Utskottet har i synnerhet behandlat möjligheterna att begränsa begreppet sammanslutningsabonnent, studerat innebörden av begreppen företagshemlighet och betydande men och funderat över hur revideringen påverkar möjligheterna till fortsatt anställning. Det är angeläget att dataskyddet förbättras och att behandling av identifieringsuppgifter endast blir en sista utväg. Vidare är det viktigt att tvångsmedelslagen ses över och att dataombudsmannen har resurser för att fullfölja sitt övervakningsuppdrag.

Utlåtandet från grundlagsutskottet. Grundlagsutskottet anser att lagförslagen kan behandlas i vanlig lagstiftningsordning. I sin praxis har grundlagsutskottet ansett att identifieringsuppgifter för meddelanden inte ingår i det kärnområde av de grundläggande fri- och rättigheterna som skyddar hemligheten i fråga om förtroliga meddelanden (GrUU 23/2006 rd, s. 2—3 och - GrUU 3/2008 rd, s. 2/I). Men också regler som ingriper i hemligheten i fråga om identifieringsuppgifter måste uppfylla de allmänna kraven på rätt att införa begränsningar i de grundläggande fri- och rättigheterna (GrUU 23/2006 rd, s. 3). Viktiga företagshemligheter kan ha så stor företagsekonomisk betydelse för företagets värde och de ekonomiska villkoren för näringsverksamheten att de måste betraktas som godtagbara och tungt vägande skäl för att begränsa kommunikationen via nätet, framhåller grundlagsutskottet. Med avseende på proportionalitetsprincipen är det viktigt att medel som inte gör ingrepp i användarnas konfidentiella kommunikation både enligt 13 a—13 h § och enligt 8 § 3

mom. är primära för att trygga konfidentialiteten i företagshemligheter.

Samtidigt vill grundlagsutskottet i fråga om sammanslutningsabonnenters rätt att behandla uppgifter understryka att behandling av identifieringsuppgifter på grund av kraven i 8 § 3 mom. bara är tilllåten i den omfattning som syftet kräver och att det inte är tilllåtet att begränsa skyddet för förtroliga meddelanden mer än nödvändigt. Identifieringsuppgifter får alltså till exempel bara behandlas så mycket att sammanslutningsabonnenten på ett adekvat sätt kan specificera en anmälan eller begäran om utredning till polisen. Med denna tolkning och tilllämpning är bestämmelserna inget problem med avseende på proportionalitetsprincipen.

Grundlagsutskottet föreslår vissa ändringar i lagen om dataskydd vid elektronisk kommunikation. I 13 b § bör plikten att ha adekvat datasäkerhet preciseras. I 13 d § bör villkoren delas upp i villkor som gäller rätt att behandla identifieringsuppgifter vid röjande av företagshemligheter och i villkor som gäller vid misstanke om annat missbruk. Vidare anser grundlagsutskottet att manuell behandling av identifieringsuppgifter vid misstanke om att en företagshemlighet har röjts i enlighet med 13 d § 2 mom. bara ska vara tillåten när det också finns grundad anledning att misstänka att en företagshemlighet har röjts via kommunikationsnätet. Dessutom vill grundlagsutskottet precisera begreppet företagshemlighet och även olovlig användning av kommunikationsnätet och användning i strid med anvisningarna enligt 13 a § samt göra en del språkliga preciseringar i 13 a och 13 d §.

Det är viktigt att den uppföljningsgrupp som enligt propositionen ska tillsättas vid kommunikationsministeriet också utvärderar tillämpningen av lagen med avseende på de grundläggande fri- och rättigheterna. Då bör det undersökas i vilken omfattning arbetsgivarna har utnyttjat de rättigheter som lagen ger dem, hur dataombudsmannens tillsynsuppdrag har utfallit och hur hemligheten i fråga om personalens meddelanden har tillgodosetts, säger grundlagsutskottet.

Heltäckande bevakning av hur lagen utfaller är ett måste, anser kommunikationsutskottet och föreslår ett uttalande om detta *(Utskottets förslag till uttalande 1)*.

Definition på sammanslutningsabonnent. Begreppet sammanslutningsabonnent kom till när lagen om dataskydd vid elektronisk kommunikation stiftades. Där avser ordet ett företag eller en sammanslutning 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 täcker in dels företag, dels universitet och olika typer av sammanslutningar inom den offentliga förvaltningen, bland andra näringsutövare, andelslag, aktiebolag, föreningar, universitet och statliga myndigheter.

Den gällande lagen utgår från att kommunikationen ska vara förtrolig och att teleföretag, leverantörer av mervärdestjänster och sammanslutningsabonnenter bara i vissa fall ska få behandla identifieringsuppgifter. I 3 kap. ges dessa vissa rättigheter och skyldigheter att behandla identifieringsuppgifter. Sammanslutningsabonnenter får behandla identifieringsuppgifter för att utföra och använda tjänster och för att se till dataskyddet (9 §), för fakturering (10 §), för teknisk utveckling (12 §), i fall av missbruk (13 §) och för att upptäcka tekniska fel eller brister (14 §). Alla sammanslutningsabonnenter har samma rättigheter på lika villkor, men samtidigt också samma skyldigheter när de utövar dessa rättigheter. Det finns till exempel inga begränsningar beroende på abonnenternas storlek, utan alla, från de minsta till de största, har rätt att bli behandlade på samma sätt och är därmed bundna av samma skyldigheter.

I betänkande KoUB 13/2004 rd framhåller kommunikationsutskottet att sammanslutningsabonnenter i likhet med teleföretagen är utomstående i relation till kommunikationsparterna. Sammanslutningsabonnenten abonnerar på kommunikationstjänsten eller mervärdestjänsten för sina användare, till exempel sina anställda. Då administrerar sammanslutningsabonnenten samtidigt det system där konfidentiella identifieringsuppgifter och lokaliseringsuppgifter om an-

vändarna behandlas med olika typer av servrar och terminalutrustning. I en sammanslutningsabonnents tekniska system samlas det konfidentiella identifieringsuppgifter om användarna och i till exempel e-postsystem också konfidentiella meddelanden. Sammanslutningsabonnenter, som företag och universitet, behandlar exakt samma konfidentiella uppgifter och med likadana tekniska system som teleföretagen. Det betyder att sammanslutningsabonnenterna har samma möjligheter till missbruk och samma behov av samordnade rättigheter och skyldigheter som teleföretag, ansåg utskottet då.

Utskottet har rett ut vad begreppet sammanslutningsabonnent avser i propositionen och undersökt möjligheten att begränsa begreppet i det här fallet. Enligt vissa källor bör man skilja mellan att utreda om företagshemligheter har läckts ut och att utreda olovlig användning. Alla sammanslutningsabonnenter berörs inte av bestämmelserna om att utreda om företagshemligheter har röjts av den enkla anledningen att de inte har företagshemligheter som kräver skydd. Ändå kan det vara en mycket stor sak också för de allra minsta företagen och organisationerna att utreda olaglig användning. Det bör dock observeras att såväl universitet och bibliotek som husbolag kan utsättas för missbruk, det vill säga deras kommunikationsnät och tjänster kan missbrukas. Då handlar det alltså om olovligt brukande.

I detta läge går det inte att dela upp sammanslutningsabonnenterna i olika grupper, men de föreslagna bestämmelserna skärper avsevärt möjligheterna att ingripa vid olovligt brukande av kommunikationsnät och tjänster. Innan universitet, bibliotek och husbolag över huvud taget får börja behandla identifieringsuppgifter måste de se till att ha ordentlig informationssäkerhet, lägga fast regler bl.a. om hur kommunikationsnät och tjänster får användas, upprätta skriftliga anvisningar för användarna, ha namngivna personer som svarar för uppdatering, datasäkerhet och annan säkerhet och har rätt att behandla identifieringsuppgifter, informera om procedurer och praxis, upplysa dataombudsmannen om att identifieringsuppgifter har börjat behandlas och lämna dataombudsmannen en årlig rapport om behandlingen. Alla sammanslutningsabonnenter måste uppfylla dessa omfattande rättssäkerhetsgarantier.

Utskottet håller med arbetslivs- och jämställdhetsutskottet som framhåller att propositionen är ett led i den rätt till informationssäkerhet som är nödvändig för den dagliga utvecklingen i informationssamhället. Eftersom Finland är ett av de ledande länderna inom produktutveckling och högteknologi har vi ett särskilt nationellt intresse av att också skydda affärshemligheter.

Företagshemlighet. Av propositionsmotiven framgår det att man med företagshemlighet i den nya 13 a § avser definitionen i 30 kap. 11 § i strafflagen. Med affärshemlighet avser strafflagen "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". Utskottet förtydligar lagförslaget genom att i paragrafen lägga till en direkt laghänvisning.

Företagshemlighet har ansetts vara det mest lämpliga begreppet i sammanhanget eftersom det har ett nära samband med näringsutövarens sekretessintresse och bestämmelserna gäller relationerna mellan enskilda parter. Det skulle bara vara förvirrande för den som ska tolka och tillämpa lagen, om det infördes ett helt nytt begrepp med samma innebörd som företagshemlighet i strafflagen.

Propositionen ställer tydliga krav på den som har rätt att behandla företagshemligheter. Behandlingen måste de facto vara skyddad för utomstående och det är i praktiken bara vissa användare som kommer åt företagshemligheter inom en organisation. Sammanslutningsabonnenten måste ange hur företagshemligheter får flyttas, lämnas ut eller överlag behandlas och till vilka destinationsadresser de behöriga personerna inte får skicka meddelanden. Allt detta ger användarna information om vad sammanslutningsabonnenten anser vara de viktigaste företagshemligheterna.

Betydande men. I 13 d § 3 mom. är betydande men ett villkor för både automatisk och manuell behandling av identifieringsuppgifter. Kravet ska specifikt gälla olovligt brukande, det vill säga användning som strider mot sammanslutningsabonnentens anvisningar. I propositionen anger regeringen bland annat att betydande men kan avse ökade kostnader eller sådan ökad användning av dataöverföringskapaciteten, ett sådant hot mot informationssäkerheten eller någonting liknande som äventyrar, försvårar eller fördröjer möjligheterna att använda kommunikationsnätet eller tjänsterna för det planerade ändamålet.

Villkoret för att betydande men ska kunna avses ha uppstått konkretiseras genom de anvisningar som avses i 13 b § och genom det som sammanslutningsabonnenten föreskriver i sina anvisningar. Innan identifieringsuppgifter behandlas måste sammanslutningsabonnenterna: 1) begränsa tillträdet till sitt kommunikationsnät och sin kommunikationstjänst och användningen av dem och 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 kommunikationsnätet, hur kommunikationsnätet och kommunikationstjänsterna i övrigt får användas och till vilka destinationsadresser kommunikation inte får riktas.

Det finns många olika typer av sammanslutningsabonnenter, och kommunikationsnäten och tjänsterna används på många olika sätt. Olovlig användning och dess betydelse för sammanslutningsabonnenten definieras utifrån abonnentens agerande.

Bättre dataskydd samt behandling av identifieringsuppgifter som sista utväg. De primära metoderna för att säkerställa att kommunikationsnät och kommunikationstjänster används på behörigt sätt är att satsa på bra dataskydd, att ge användarna anvisningar och att per automatik bevaka att de följs, framhåller utskottet. I 13 b § 1 mom. räknas de omfattande åtgärder upp som sammanslutningsabonnenter måste vidta innan de börjar behandla identifieringsuppgifter. De kan enligt utskottets uppfattning medverka till betydligt bättre dataskydd i våra företag och organisationer. Vid utfrågningen av de sakkunniga nämndes EG-kommissionens enkät, Eurobarometer, om dataskydd. Den visar att 23 % av de registeransvariga i Finland (företag och organisationer) inte ens har hört talas om tekniska metoder för dataskydd.

Det är särskilt viktigt att man på arbetsplatserna behandlar behovet av informationssäkerhet och spelreglerna för kommunikation så öppet som möjligt, som samarbetslagstiftningen avser, och tillsammans med alla berörda arbetstagare, framhåller arbetslivs- och jämställdhetsutskottet. Om man behandlar informationssäkerheten på bred front och utformar spelreglerna tillsammans med personalen underlättar man för personalen att känna till reglerna och följa dem. Då uppstår inget behov av att utreda missbruk.

Både för arbetsgivaren och för medarbetarna är det viktigt att först öppet och förbehållslöst fundera över vilka för- och nackdelarna är med att de anställda använder arbetsgivarens arbetsredskap också för att uträtta egna ärenden och att därefter lägga fast reglerna utifrån företagets och medarbetarnas behov. Lagen gäller små och stora företag och alla branscher på lika villkor. Följaktligen kan inte alla regler tillämpas på alla situationer.

Det är angeläget att olika aktörer går ut med tydlig information om lagstiftningen på bred bas och särskilt lyfter fram att behandling av identifieringsuppgifter är en sista utväg, menar kommunikationsutskottet.

Reformens tekniska räckvidd. Revideringen innebär att sammanslutningsabonnenter på vissa villkor får rätt att behandla identifieringsuppgifter vid elektronisk kommunikation för att utreda om deras kommunikationsnät och avgiftsbelagda informationssamhällstjänster används utan lov och kommunikationstjänster i strid med anvisningarna. Sammanslutningsabonnenter ska också på vissa villkor få behandla identifieringsuppgifter när de misstänker att någon obehörigen har röjt företagshemligheter av stor betydel-

se för deras näringsverksamhet. Uppgifterna ska i första hand behandlas automatiskt utifrån förbestämda faktorer.

Sammanslutningsabonnenterna får inte reda på något annat än identifieringsuppgifterna för meddelanden som har skickats och tagits emot i deras egna kommunikationstjänster. För kommersiella tjänster som e-post, webbank och andra tekniskt skyddade kommersiella tjänster avslöjar identifieringsuppgifterna bara adressen, tidpunkten och hur länge tjänsten används. Rättten att behandla identifieringsuppgifter gäller inte telefonsamtal, sms eller andra liknande meddelanden i det fasta och mobila telefonnätet. Innehållet i meddelanden får över huvud taget inte behandlas vid misstanke om missbruk och identifieringsuppgifter får inte behandlas för att bryta källskyddet.

Redan nu tillåter den gällande lagstiftningen till stor del övervakning av vad användarna gör på nätet. För att utreda om företagshemligheter har röjts obehörigen har arbetsgivarna datatekniska medel till sitt förfogande, till exempel att kontrollera användarloggen, uppgifter om de som loggar in sig på åtkomstskyddade system och information som samlas i de tekniska systemen. Uppgifterna visar vem som sparat viss information, i vilket format, när och på vilket medium, till exempel hårddisk eller flyttbart medium. USB-minnen och cd-skivor är exempel på flyttbara medier. Också information om annan behandling, bland annat utskrift, kan lagras. Lagen om dataskydd vid elektronisk kommunikation anger inga begränsningar för behandlingen av sådana uppgifter. En del arbetsplatser har rentav kameraövervakning.

Hur påverkas anställningens fortbestånd? Lagen föreskriver inga påföljder för att röja företagshemligheter. Den reglerar inte påföljderna vid brott mot företagshemligheten, vare sig arbetsrättsligt eller straffrättsligt, och säger ingenting om mottagarens ansvar.

Hur anställnings- och tjänsteförhållanden får avslutas och varningar ges regleras arbets- och tjänsterättsligt utifrån en samlad prövning. Bestämmelser om bland annat uppsägningsgrunder som har samband med arbetstagarens person samt varning och grunder för att häva ett arbetsavtal ingår i 7 kap. 2 § respektive 8 kap. 1 § i arbetsavtalslagen. En samlad prövning innebär en intresseavvägning där man väger dels faktorer som talar för, dels faktorer som talar mot uppsägningskriterierna. De faktorer som kommer i fråga måste vägas mot varandra mot bakgrunden av de rådande särdragen i varje enskilt fall. Arbetsgivaren måste kunna bevisa att uppsägningsgrunder föreligger.

Utskottet noterar att de tunga centralorganisationerna på arbetsmarknaden ställer sig bakom propositionen. En del av de sakkunniga framhöll att rutinerna för dataskydd varierar på arbetsplatserna och att propositionen bidrar till att förtydliga det oklara läget. Lagförslaget bereddes länge och fick under processens gång ett flertal bestämmelser som förbättrar de anställdas rättssäkerhet. I yttrandena till utskottet framhålls det att lagförslaget inte får försämra anställningstryggheten. Propositionen medför inga ändringar i reglerna för att avsluta ett anställnings- eller tjänsteförhållande. Sådana ärenden kommer fortfarande att avgöras på grundval av arbets- och tjänsterättsliga regler och procedurer.

Revidering av tvångsmedelslagen. När propositionen utarbetades gjordes det en ingående bedömning av möjligheten att låta det uteslutande vara polisen som har rätt att utreda missbruk. Men det ansågs vara helt uteslutet eftersom sammanslutningsabonnenterna är så många, de tekniska felen och möjligheterna till missbruk så varierande, systemen så olika och uppdragen så resurskrävande.

Det handlar om daglig uppdatering av sammanslutningsabonnenternas kommunikationssystem som abonnenterna själva måste se till. Samtidigt kunde sammanslutningsabonnenterna avgränsa en begäran om förundersökning så att undersökningen (inklusive datorer och servrar som polisen tar hand om under tiden) inte äventyrar den fortsatta verksamheten vid företaget. Det är polisen som ska genomföra förundersökningen.

Utskottet håller med förvaltningsutskottet om att sammanslutningsabonnenter ska ha rätt att behandla identifieringsuppgifter bara i den omfattning att de tillräckligt väl ska kunna specificera en polisanmälan eller en begäran om förundersökning till polisen. Samtidigt påpekar utskottet att brott mot företagshemligheten och olovligt brukande är så kallade målsägandebrott och att bestämmelserna därför inte får förutsätta förundersökning.

I sitt yttrande framhåller inrikesministeriet att det bör göras en tydlig begreppsmässig skillnad mellan den föreslagna kontrollrätten för sammanslutningsabonnenter för att så att säga skydda sin verksamhet å ena sidan och polisens befogenheter och den anknytande kriminaliseringen å andra sidan. Det är ett av målen i propositionen.

Följaktligen överför propositionen inte polisuppdrag till företagen, anser utskottet. Också utlåtandet från grundlagsutskottet talar för detta. Om en anställd från sin e-post på jobbet skickar ut företagshemligheter får arbetsgivaren som lagstiftningen nu är utformad inte behandla e-postloggen för att ta reda på vem som läckt ut uppgifterna, framgår det av ett sakkunnigutlåtande. Dessutom kan det företag som utsätts för brottet inte lämna ut nödvändiga bevis till polisen för att brottet ska kunna utredas eftersom företaget som sammanslutningsabonnent agerar i rollen som utomstående e-postleverantör. För att få tillträde till bevisen måste polisen begära tillstånd för teleövervakning av domstol, men vid företagshemlighetsbrott uppfylls inte kriterierna för teleövervakning i 5 a kap. i tvångsmedelslagen (450/1987). För att få tillstånd måste polisen dessutom kunna precisera fallet. Enligt gällande lag får företaget inte behandla identifieringsuppgifter och kan därmed inte komma med preciserande uppgifter. Följaktligen kan inte heller polisen lägga fram de specificerade uppgifter som domstolen kräver.

De eventuella brister eller oklarheter i polisens befogenheter som lagförslaget lyfter fram, till exempel vid undersökning av missbruk och brott i samband med företagshemligheter, måste utredas skyndsamt och i förekommande fall redan före en mer genomgripande revidering av tvångsmedelslagen. Utskottet föreslår ett uttalande om detta *(Utskottets förslag till uttalande 2)*.

Övervakningsresurser. Reformen ger dataombudsmannen ett nytt resurskrävande övervakningsuppdrag. Dataombudsmannen ges i uppdrag att övervaka hur sammanslutningsabonnenter behandlar identifieringsuppgifter enligt 13 a—13 k § för att avslöja om någon olovligen har använt en avgiftsbelagd informationssamhällstjänst eller kommunikationsnätet, använt en kommunikationstjänst i strid med anvisningarna eller obehörigen röjt företagshemligheter.

Dataombudsmannen ska i enlighet med personuppgiftslagen övervaka hur personuppgifter behandlas. Dessutom utövar arbetarskyddsmyndigheterna tillsyn över lagen om integritetsskydd i arbetslivet tillsammans med dataombudsmannen. Företagen i egenskap av arbetsgivare hör till de största grupperna sammanslutningsabonnenter och det är därför naturligt att dataombudsmannen också är med och övervakar den lagen.

Dataombudsmannens byrå är en liten enhet utan möjligheter att genom interna omställningar omfördela resurserna. För att klara av det nya övervakningsuppdraget måste byrån därför enligt propositionen få två nya specialsakkunniga och en kontorsanställd. Anslagsökningen uppskattas preliminärt uppgå till 260 000 euro på årsnivå.

En avgift får tas ut av sammanslutningsabonnenterna för övervakningen. Vilka åtgärder som är avgiftsbelagda och hur stor avgiften ska vara ska föreskrivas genom förordning av justitieministeriet på grundval av lagen om grunderna för avgifter till staten (150/1992). Betalningsskyldigheten måste stå i rätt proportion till abonnentens storlek och verksamhetens karaktär.

Dataombudsmannens byrå måste få ökade resurser när lagändringen ger den nya uppdrag, eftersom en hög nivå på övervakningen och adekvata resurser är viktiga kriterier för att reformen ska kunna godkännas.

Detaljmotivering

Lagförslag 1

Ingressen. Utskottet lägger till en ny 13 e § och ändrar därför också ingressen.

13 a §. Sammanslutningsabonnenters behandlingsrätt i fall av missbruk. Med anledning av utlåtandet från grundlagsutskottet kompletterar utskottet 1 mom. med en hänvisning till 30 kap. 11 § i strafflagen och ändrar de övriga paragrafhänvisningarna i överensstämmelse med de andra föreslagna ändringarna. Dessutom gör utskottet en språklig ändring i 1 och 2 mom.

I 1 mom. lägger utskottet till verbet förebygga i kombination med utreda. Automatisk behandling är tänkt att tillämpas kontinuerligt och kan införas när kriterierna är uppfyllda. Avvikelser som uppdagas vid automatisk sökning är en möjlighet att inleda manuell utredning av om företagshemligheter har röjts.

Med hänvisning till grundlagsutskottet preciserar utskottet bestämmelsen i 2 mom. om olovlig användning eller användning i strid med anvisningarna. Exempelförteckningen kompletteras dessutom med att någon obehörigen ger utomstående tillträde till sammanslutningsabonnentens kommunikationsnät eller kommunikationstjänster.

13 b §. Sammanslutningsabonnenters omsorgsplikt vid fall av missbruk. Utskottet preciserar 1 mom. med samma språkliga korrigeringar som i 13 a § 1 och 2 mom.

Med anledning av utlåtandet från grundlagsutskottet preciserar kommunikationsutskottet 2 mom. 1 punkten. Punkten ska klart och tydligt säga ut att sammanslutningsabonnenten är skyldig att ordna med behöriga informationssäkerhetsåtgärder för att skydda kommunikationsnätet, kommunikationstjänsterna och informationen.

13 c §. Sammanslutningsabonnenters planerings- och samarbetsplikt i fall av missbruk. Utskottet har ändrat paragrafhänvisningarna i 2 mom. 1 punkten och 4 mom. på grund av andra föreslagna ändringar.

13 d §. Villkor för sammanslutningsabonnenters behandlingsrätt i fall av missbruk. Som grundlagsutskottet föreslår har utskottet delat upp paragrafen på två olika paragrafer. Då föreskriver 13 d § om sammanslutningsabonnenters rätt att behandla identifieringsuppgifter för att utreda hur avgiftsbelagda informationssamhällstjänster, kommunikationsnätet eller kommunikationstjänster har använts. Den nya 13 e § gäller sammanslutningsabonnenters rätt att behandla identifieringsuppgifter för att utreda om företagshemligheter har röjts. Den nya paragrafen innehåller meningen i 2 mom. om situationer när en företagshemlighet olovligt har röjts för en utomstående, 2 mom. 4 punkten, satsen i 2 mom. 5 punkten om att en företagshemlighet olovligt har röjts för en utomstående, 3 mom. 2 punkten och satsen om att utreda missbruk och vem som är ansvarig i 4 mom.

Utskottet ändrar dessutom paragrafrubrikerna och formulerar om det nya 2 mom. 4 punkten (tidigare 5 punkten).

13 e §. Sammanslutningsabonnenters behandlingsrätt för att utreda om företagshemligheter har röjts (Ny). Som grundlagsutskottet föreslår inför kommunikationsutskottet en ny 13 e § som bygger på strukturen i 13 d §. Paragrafen reglerar sammanslutningsabonnenters rätt att behandla identifieringsuppgifter för att utreda om företagshemligheter har röjts.

Dessutom ändrar utskottet 2 mom. till att manuell behandling av identifieringsuppgifter ska vara tillåten i de fall som nämns i momentet bara under förutsättning att det finns grundad anledning att misstänka att företagshemligheter har getts ut via kommunikationsnätet. Vidare införs samma språkliga ändring i 2 mom. 3 punkten som i den nya 4 punkten i 13 d § 2 mom.

13 f §. Särskilda begränsningar i behandlingsrätten i fall av missbruk. Utskottet ändrar paragrafnumreringen på grund av ändringarna ovan.

13 g §. Sammanslutningsabonnenters skyldighet att lämna uppgifter till användare i fall av missbruk. Utskottet ändrar paragrafnumreringen och samtidigt också paragrafhänvisningarna i 1 och 2 mom. på grund av ändringarna ovan.

13 h §. Sammanslutningsabonnenters skyldighet att lämna uppgifter till företrädare för arbetstagarna i fall av missbruk. Utskottet ändrar paragrafnumreringen och samtidigt också paragrafhänvisningen i 1 mom. på grund av ändringarna ovan.

13 i §. Förhandsanmälan och årlig redogörelse till dataombudsmannen i fall av missbruk. Utskottet ändrar paragrafnumreringen och samtidigt också paragrafhänvisningen i 1 mom. på grund av ändringarna ovan.

13 j §. Sammanslutningsabonnenters rätt att lagra identifieringsuppgifter i fall av missbruk. Utskottet ändrar paragrafnumreringen och samtidigt också paragrafhänvisningen på grund av ändringarna ovan.

13 k §. Sammanslutningsabonnenters rätt att lämna ut uppgifter i fall av missbruk. Utskottet ändrar paragrafnumreringen och samtidigt också paragrafhänvisningen på grund av ändringarna ovan.

32 §. Dataombudsmannens uppgifter. Utskottet ändrar paragrafhänvisningen i 1 mom. 1 punkten på grund av ändringarna ovan.

34 §. Tillsynsmyndigheternas tystnadsplikt. Utskottet ändrar paragrafhänvisningen i 1 mom. på grund av ändringarna ovan.

42 §. Straffbestämmelser. Utskottet ändrar paragrafhänvisningarna i 1 mom. och 2 mom. 9 punkten på grund av ändringarna ovan.

Lagförslag 2

2 §. Tillämpningsområde. Utskottet ändrar 3 mom. i överensstämmelse med ändringen i 13 a § i lagförslag 1.

Förslag till beslut

Med stöd av det ovan anförda föreslår kommunikationsutskottet

att lagförslag 3 och 4 godkänns utan ändringar och

att lagförslag 1 och 2 godkänns med ändringar ***(Utskottets ändringsförslag)*** *och*

att två uttalanden godkänns ***(Utskottets förslag till uttalanden)****.*

Utskottets ändringsförslag

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 *k* och 34 a § som följer:

9—13 §
(Som i RP)

13 a §

Sammanslutningsabonnenters behandlingsrätt i fall av missbruk

En sammanslutningsabonnent har rätt att behandla identifieringsuppgifter för att *förebygga och utreda* olovligt brukande av avgiftsbelagda samhällstjänst*er, kommunikationsnätet eller kommunikationstjänster eller röjande av* företagshemligheter *enligt 30 kap. 11 § i strafflagen (39/1889),* enligt vad som bestäms i 13 b–13 j §.

(*Utesl.*) *Att installera* anordningar, program eller tjänster i sammanslutningsabonnentens kommunikationsnät, *att obehörigen ge utomstående tillträde till sammmanslutningsabonnentens kommunikationsnät eller kommunikationstjänster eller att på något annat jämförbart sätt använda kommunikationsnätet eller kommunikationstjänster kan vara olovligt brukande av kommunikationsnätet eller kommunikationstjänster,* om *förfarandet* står i strid med de anvisningar för användningen som avses i 13 b § 3 mom.

(3 mom. som i RP)

13 b §

Sammanslutningsabonnenters omsorgsplikt i fall av missbruk

För att förebygga olovligt brukande av avgiftsbelagda informationssamhällstjänster, (*utesl.*) *kommunikationsnätet eller kommunikationstjänster (utesl.)* skall en sammanslutningsabonnent innan behandlingen av identifieringsuppgifter inleds

(Punkt 1 och 2 som i RP)

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

1) begränsa tillträdet till företagshemligheter och vidta andra åtgärder för att skydda *användningen av sitt kommunikationsnät och sina kommunikationstjänster* och uppgifterna *genom behöriga informationssäkerhetsåtgärder*, och

(Punkt 2 som i RP)
(3 mom. som i RP)

13 c §

Sammanslutningsabonnenters planerings- och samarbetsplikt i fall av missbruk

(1 mom. som i RP)

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 *k* § avsedda förfaranden som skall tillämpas vid behandlingen av identifieringsuppgifter, och

(Punkt 2 som i RP)

(3 mom. som i RP)

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 *k* §.

13 d §

Sammanslutningsabonnenters behandlingsrätt för att utreda om avgiftsbelagda informationssamhällstjänster, kommunikationsnätet eller kommunikationstjänster har använts olovligt

(1 mom. som i RP)

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. (*utesl.*) och om

(1—3 punkten som i RP)

(Punkt 4 *utesl.*)

4) det i ett enskilt fall på basis av annan med 1–*3* punkten jämförbar allmänt konstaterbar omständighet *går att sluta sig till* att kommunikationsnätet, kommunikationstjänsten eller en avgiftsbelagd informationssamhällstjänst används i strid med de anvisningar som avses i 13 b § 3 mom. (*utesl.*).

Villkor för behandling enligt 1 och 2 mom. är att (*utesl.*) incidenten eller gärningen sannolikt orsakar betydande men eller skada för sammanslutningsabonnenten (*utesl.*).

Villkor för behandling enligt 2 mom. är dessutom att uppgifterna är nödvändiga för att reda ut *olovligt brukande* och de som svarar för det och för att göra slut på olovligt brukande (*utesl.*).

13 e § (Ny)

Sammanslutningsabonnenters behandlingsrätt för att utreda om företagshemligheter har röjts

En sammanslutningsabonnent får behandla identifieringsuppgifter med hjälp av en automatisk sökfunktion som baserar sig på meddelandenas storlek eller sammanlagda storlek, typ av meddelande, antalet meddelanden, uppkopplingssätt eller destinationsadresser.

Sammanslutningsabonnenten får behandla identifieringsuppgifter manuellt, om det finns grundad anledning att misstänka att en företagshemlighet olovligen har röjts för en utomstående via kommunikationsnätet eller en kommunikationstjänst och om

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

2) en företagshemlighet offentliggörs eller utnyttjas olovligen, eller

3) det i ett enskilt fall på grund av en annan med 1 eller 2 punkten jämförbar allmänt konstaterbar omständighet går att sluta sig till att en företagshemliget har röjts olovligen för en utomstående.

Ett villkor för behandling enligt 1 och 2 mom. är att den företagshemlighet som misstänkts ha blivit röjd gäller näringsverksamhet som är av central betydelse för sammanslutningsabonnenten eller dess samarbetspartner eller resultaten av tekniskt eller något annat utvecklingsarbete som sannolikt är viktiga för att starta eller utöva näringsverksamhet.

Villkor för behandling enligt 2 mom. är dessutom att uppgifterna är nödvändiga för att reda ut om en företagshemlighet har röjts och vem som är ansvarig.

13 *f* (e) §

Särskilda begränsningar av behandlingsrätten i fall av missbruk

(1 och 2 mom. som i RP)

13 *g (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 § (*utesl.*) 2 mom. *och 13 e § 2 mom*. Av redogörelsen skall framgå

(Punkterna 1—4 som i RP)

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 § *eller 13 e §* upphörde.

(3 mom. som i RP)

13 *h (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 *och 13 e § 2 mom.* Av redogörelsen skall det framgå på vilka grunder och hur många gånger identifieringsuppgifterna har behandlats under ett år.

(2 och 3 mom. som i RP)

13 *i* (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 § *och 13 e §* avsedda förfaranden som skall tillämpas vid behandlingen av identifieringsuppgifter,

(Punkterna 2 och 3 som i RP)

(2 mom. som i RP)

13 *j* (i) §

Sammanslutningsabonnenters rätt att lagra identifieringsuppgifter i fall av missbruk

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

13 *k* (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 *j* §.

14 och 20 §
(Som i RP)

32 §

Dataombudsmannens uppgifter

Dataombudsmannens uppgift är att övervaka

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

(Punkt 2—5 som i RP)

(2 mom. som i RP)

33 §
(Som i RP)

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 *i* § skall hållas hemliga.

(2 mom. som i RP)

34 a §
(Som i RP)

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 *h* § 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
(Punkt 1—8 som i RP)
9) underlåter att iaktta vad som i 13 f–13 *i* § 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.
(3 mom. som i RP)

Ikraftträdandebestämmelsen

(Som i RP)

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 §

Tillämpningsområde

— — — — — — — — — — — — — —

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 (*utesl.*) en kommunikationstjänst och (*utesl.*) 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 §
(Som i RP)

Ikraftträdandebestämmelsen

(Som i RP)

Utskottets förslag till uttalanden

1. *Utskottet förutsätter att tillämpningen av och målen med lagreformen bevakas och utvärderas heltäckande, bland annat av sammanslutningsabonnenterna. Kommunikationsministeriet ska rapportera resultaten till kommunikationsutskottet före den 1 januari 2011.*

2. *Riksdagen förutsätter att de eventuella brister och oklarheter i polisens befogenheter som kommer fram genom lagförslaget, till exempel när missbruk och brott relaterade till företagshemligheter undersöks, snabbt utreds, i förekommande fall redan före en genomgripande revidering av tvångsmedelslagen.*

Helsingfors den 12 december 2008

I den avgörande behandlingen deltog

ordf. Martti Korhonen /vänst
vordf. Saara Karhu /sd
medl. Mikko Alatalo /cent
Leena Harkimo /saml
Lauri Kähkönen /sd
Mats Nylund /sv
Reijo Paajanen /saml
Markku Pakkanen /cent
Lyly Rajala /saml
Tero Rönni /sd
Janne Seurujärvi /cent
Johanna Sumuvuori /gröna
Anne-Mari Virolainen /saml
ers. Pentti Tiusanen /vänst
Mirja Vehkaperä /cent
Henna Virkkunen /saml (delvis).

Sekreterare var

utskottsråd Kaj Laine.

RESERVATION 1

Motivering

I vårt moderna informationssamhälle är missbruk av elektronisk kommunikation, till exempel för att lägga ut företagshemligheter, ett verkligt problem som man måste försöka lösa. När man vill förhindra och utreda missbruk ska man ändå i så liten utsträckning som möjligt ingripa i de grundläggande fri- och rättigheterna, där integritetsskyddet och skyddet för förtroliga meddelanden är centrala inslag. Lagreformen är inte tillräckligt exakt avgränsad ens efter behandlingen i utskottet.

Vid ingrepp i de grundläggande fri- och rättigheterna måste man noga väga nyttan mot ingreppen. Det framgår inte av motiven till propositionen vilka fördelar som talar för att sammanslutningsabonnenter ska få rätt att behandla identifieringsuppgifter vid fall av "olagligt brukande av avgiftsbelagda informationssamhällstjänster, kommunikationsnätet eller kommunikationstjänster" i relation till de inskränkningar i de grundläggande fri- och rättigheterna som denna rättighet medför. Åtminstone i princip öppnar lagförslaget för att till exempel husbolag, bibliotek och läroanstalter får laglig rätt att behandla identifieringsuppgifter, förutsatt att vissa kriterier är uppfyllda. Bland annat det faktum att dataombudsmannen har rätt att ta ut en avgift av sammanslutningsabonnenten för övervakningsåtgärderna kan dock höja ribban för övervakning i större skala.

Följaktligen är det motiverat att åtminstone begränsa lagen så att sammanslutningsabonnenter får rätt att behandla identifieringsuppgifter förmeddelanden uteslutande för att utreda om företagshemligheter har läckt ut. Kommunikationsutskottet tog fasta på utlåtandet från grundlagsutskottet och lade till en bestämmelse som betyder att företagshemligheter som röjs måste gälla uppgifter som avses i 30 kap. 11 § i strafflagen (39/1889). I 13 e § sägs det vidare att det måste gälla företagshemligheter som är av central betydelse för sammanslutningsabonnentens egen eller samarbetspartnernas näringsverksamhet. Passusen om sammanslutningsabonnenters rätt att behandla identifieringsuppgifter för att utreda "olagligt brukande av avgiftsbelagda informationssamhällstjänster, kommunikationsnätet eller kommunikationstjänster" ströks alltså.

Också med den här avgränsningen finns det anledning att betvivla att lagen fungerar. Det är mycket osannolikt att välutbildade experter läcker ut företagshemligheter via sin e-post på jobbet, när det finns webbaserade e-posttjänster, USB-minnen och cd-brännare och andra verktyg för att kopiera och vidarebefordra information. Dessutom måste man fråga sig om det räcker med identifieringsuppgifter för att förundersökning ska inledas.

Företagshemligheter kunde skyddas genom att ge polisen större befogenheter i samband med revideringen av tvångsmedelslagen. Så skulle behandling av identifieringsuppgifter tydligare ingå i laglighetsövervakningen.

Förslag

Vi föreslår

> *att lagförslagen godkänns enligt betänkandet utom 13 a §, 13 b, 13 c § och 13 i § med ändringar och 13 d § med uteslutning i lagförslag 1 och 2 § 3 mom. i lagförslag 2 med ändringar.*

Reservationens ändringsförslag

Lagförslag 1

13 a §

Sammanslutningsabonnenters behandlingsrätt i fall av missbruk

En sammanslutningsabonnent har rätt att behandla identifieringsuppgifter för att utreda (*utesl.*) röjande av företagshemligheter enligt 30 kap. 11 § i strafflagen (39/1889) *(utesl.)* enligt vad som bestäms i 13 b–13 j §.

(2 mom. *utesl.*)

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

13 b §

Sammanslutningsabonnenters omsorgsplikt i fall av missbruk

(1 mom. *utesl.*)

(2 mom. som i KoUB)

En sammanslutningsabonnet skall för att förebygga missbruk som avses ovan (*utesl.*) ge skriftliga anvisningar till dem som använder kommunikationsnätet eller kommunikationstjänsten.

13 c §

Sammanslutningsabonnenters planerings- och samarbetsplikt i fall av missbruk

(1–3 mom. som i KoUB)

(4 mom. *utesl.*)

13 d §

(Utesl.)

13 i §

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 e § (*utesl.*) avsedda förfaranden som skall tillämpas vid behandlingen av identifieringsuppgifter,

(2 och 3 punkten som i KoUB)

(2 mom. som i KoUB)

Lagförslag 2

2 §

Tillämpningsområde

— — — — — — — — — — — — — —

Om arbetsgivarens rätt att i egenskap av abonnent för utredning av avgiftsskyldigheten få identifieringsuppgifter om en anslutning som ställts till arbetstagarens förfogande och om rättten att behandla identifieringsuppgifter som gäller arbetstagarens elektroniska kommunikation (*utesl.*) för att skydda företagshemligheter föreskrivs i lagen om dataskydd vid elektronisk kommunikation (516/2004). Vad som i nämnda lag bestäms om användare av lokaliseringstjänster tilllämpas 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.

— — — — — — — — — — — — — —

Helsingfors den 12 december 2008

Johanna Sumuvuori /gröna

RESERVATION 2

Motivering

I propositionen ges arbetsgivaren och andra sammanslutningsabonnenter rätt att övervaka och behandla identifieringsuppgifter i de anställdas e-posttrafik, när de misstänker att någon arbetstagare har röjt eller har för avsikt att röja företagshemligheter via e-posten. I debatten har man alltför lite fokuserat på att sammanslutningsabonnent är ett mycket omfattande begrepp. Inte bara företag, utan också universitet, ämbetsverk, bibliotek och rentav husbolag med eget kommunikationsnät ska i vissa situationer ha rätt att kontrollera e-posttrafiken.

En annan sak som har kommit i skymundan är att lagen också kommer att gälla all IT-baserad trafik, till exempel webbtelefoni och snabbmeddelandetjänster. Det utvidgar tillämpningsområdet. Den gällande lagstiftningen har ansetts vara otydlig och ge rum för tolkning. Ett annat problem har varit att det inte går att få hjälp från myndigheterna när det behövs. Den föreslagna ändringen avser att förtydliga situationen.

Målet att förbättra informationssäkerheten är bra. Extra viktigt är det också att få verktyg för att skydda företagshemligheter. Varje företag skall ha rätt till resultaten av sitt arbete och sitt materiella och immateriella kapital. Kriminalitet och företagsspionerі är i inga händelser acceptabelt. Företagen har ansett att e-posten kommer till korta i den nuvarande lagstiftningen om dataskydd. Men den föreslagna lagen löser inte problemet, tycker vi, eftersom oärliga människor har många metoder till sitt förfogande.

Också själva utgångspunkten i lagen är ett problem för en misstanke om brott är en polissak, och polisen måste ha adekvata resurser och befogenheter för att ta tag i sådant. I dagsläget måste polisen ha tillstånd från domstol för att få övervaka identifieringsuppgifter. Propositionen ger alltså sammanslutningsabonnenter exceptionella befogenheter betydligt lättare än polisen har rätt att få.

När dessutom begreppet betydande men i alltför hög grad får bedömas av sammanslutningsabonnenterna själva, får de mycket omfattande rättigheter att agera och övervaka kommunikationsnätet, förutsatt att de lagstadgade kriterierna är uppfyllda. Vi har all anledning att fråga vem som övervakar övervakaren. Propositionen öppnar för nya otydligheter i lagstiftningen och inbjuder till missbruk av befogenheterna. Dessutom har dataombudsmannen begränsade möjligheter att utöva tillsyn över den nya lagstiftningen.

Arbetsmarknadsorganisationerna har godtagit propositionen och kommit överens om spelreglerna i ett samrådsförfarande. Men arbetsgivaren och arbetstagarna har ett särskilt förhållande till varandra som avviker från de övriga sammanslutningsabonnenterna. Inom ramen för dessa gemensamma spelregler måste man på arbetsplatserna också kunna komma överens om hur identifieringsuppgifter i den e-posttrafik som arbetsgivaren tillhandahåller får övervakas utan att det inkräktar på skyddet för hemligheten i fråga om arbetstagarnas förtroliga meddelanden.

Vi anser att propositionen bara borde ha gällt den e-postuppkoppling som arbetsgivaren tillhandahåller på arbetsplatsen. Däremot är det inte motiverat att lagen också gäller övriga sammanslutningsabonnenter. På den punkten krävs det en ny och omsorgsfullare beredning av dataskyddet.

Kommunikationsutskottet ansåg det dock inte möjligt att dela upp sammanslutningsabonnenterna i olika grupper. Under behandlingen i utskottet har det kommit fram att både lagförslaget och begreppen där är diffusa. Lagförslaget kan inte godtas i den form som det nu har, utan det finns all anledning att bereda lagen på nytt. Slutresultatet måste vara en tydligare och mer lättförståelig lag där de viktigaste begreppen är tydligt avgränsade, vilket gör det lättare att tillämpa lagen på rätt sätt.

Förslag

Vi föreslår

att lagförslagen förkastas och

att ett uttalande godkänns ***(Reservationens förslag till uttalande).***

Reservationens förslag till uttalande

Riksdagen förutsätter att regeringen bereder tydliga bestämmelser om skydd för företagshemligheter och begränsar dem till att bara gälla den e-postuppkoppling som arbetsgivaren tillhandahåller på arbetsplatsen utifrån arbetsmarknadsorganisationernas gemensamt godkända principer.

Helsingfors den 12 december 2008

Saara Karhu /sd
Lauri Kähkönen /sd
Tero Rönni /sd

RESERVATION 3

Motivering

Det är tydligt att lagstiftningen om elektronisk kommunikation och övervakningen av den behöver ses över. De gällande bestämmelserna om behandling av identifieringsuppgifter är alltför generellt formulerade och medför tolkningsproblem. E-posttrafiken har blivit en gråzon som varken företagen som arbetsgivare eller myndigheterna, till exempel polisen har kunnat undersöka när det har funnits anledning att misstänka att företagshemligheter har läckt ut. Varje företag har rätt till resultaten av sitt arbete och sitt materiella och immateriella kapital. Men i vissa fall har det varit svårt att skydda kapitalet mot missbruk.

Propositionen ger en möjlighet att förhindra olovlig användning av kommunikationsnätet och användning av kommunikationstjänster i strid med anvisningarna i och med att den tillåter att identifieringsuppgifter behandlas. Dessutom ger den en möjlighet att förhindra att företagshemligheter som är av central betydelse för näringsverksamheten röjs olovligt, om det görs via elektronisk kommunikation.

Också universitet, ämbetsverk, bibliotek och rent av husbolag med eget kommunikationsnät ska få rätt att observera e-posttrafiken. Dessutom ska rätten gälla IT-trafik, till exempel webbtelefoni och snabbmeddelandetjänster. Enligt lagförslaget ska arbetsgivaren ha rätt att observera och behandla identifieringsuppgifter i arbetstagarnas e-posttrafik. Automatisk behandling är tillåten utan misstanke om att en företagshemlighet har röjts.

Redan textutformningen och begreppen i propositionen visar tydligt att elektronisk kommunikation tekniskt sett och med avseende på den juridiska regleringen är ett ytterst känsligt område på arbetsplatser där parterna har starka rättigheter och skyldigheter.

Av allt att döma utgår propositionen i stor utsträckning från företagens behov. Även om de gott och väl kan vara motiverade bör man fundera om samma mål hade kunnat nås på något annat sätt och utan att äventyra integritet i ett läge då tekniken, systemen och arbetslivet är stadda i snabb förändring. Vid utfrågningen av de sakkunniga fick vi inget uttömmande svar på frågan vem som övervakar övervakaren. Exempelvis dataombudsmannens byrå har mycket knappa resurser.

Justitiekanslern och de många sakkunniga i grundlagsutskottet har varit mycket kritiska till lagförslaget. De menar att lagen alltför mycket inkräktar på de grundläggande fri- och rättigheterna och sammanslutningsabonnenter, det vill säga arbetsgivarna, alltför stora befogenheter. Vi talar alltså om att ge privata aktörer betydande rätt att använda tvångsmedel, större befogenheter än polisen, utan att det ges tillstånd.

Det hade funnits två andra alternativ att satsa på som inte hade medfört så stor misstro och så betydande hot mot människors integritet som regeringens förslag. För det första hade det varit bättre med avseende på arbetslivet att lagen om integritetsskydd i arbetslivet hade fått bättre och exaktare bestämmelser om arbetsgivarens rätt att behandla identifieringsuppgifter för arbetsgivares meddelande. Det andra alternativet hade varit att ge polisen större och exaktare befogenheter för att kunna behandla identifieringsuppgifter i den här typen av situationer.

Förslag
Vi föreslår

att lagförslagen förkastas.

Helsingfors den 12 december 2008

Pentti Tiusanen /vänst
Martti Korhonen /vänst