Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi sähköisen viestinnän tietosuojalakia. Yksityisyyden suojasta työelämässä annettuun lakiin, yhteistoiminnasta yrityksissä annettuun lakiin sekä yhteistoiminnasta valtion virastoissa ja laitoksissa annettuun lakiin ehdotetaan lisäksi eräitä lähinnä teknisiä muutoksia.

Yhteisötilaajien oikeuksia käsitellä tunnistamistietoja teknistä kehittämistä varten sekä maksullisten tietoyhteiskunnan palvelujen ja viestintäverkkojen luvattoman käytön tai viestintäpalvelujen ohjeiden vastaisen käytön selvittämiseksi selkeytettäisiin. Teleyrityksille, lisäarvopalvelun tarjoajille ja yhteisötilaajille annettaisiin tietyin edellytyksin oikeus käsitellä tunnistamistietoja automaattisen tietojenkäsittelyn avulla tilastollista analyysiä varten.

Yhteisötilaajille annettaisiin tietyin edellytyksin oikeus käsitellä tunnistamistietoja, jos epäillään elinkeinotoiminnan kannalta keskeisten yrityssalaisuuksien luvatonta paljastamista. Yhteisötilaajat saisivat käsitellä tietoa muun muassa sähköpostiviestien lähettäjästä ja vastaanottajasta sekä lähetysajasta, mutta eivät viestin sisältöä.

Ehdotuksella parannettaisiin teleyritysten, lisäarvopalvelun tarjoajien ja yhteisötilaajien mahdollisuutta huolehtia viestintäverkkojen ja -palvelujen tietoturvasta.

Tietosuojavaltuutettu valvoisi yhteisötilaajien tunnistamistietojen käsittelyä väärinkäytöstilanteissa. Lisäksi Viestintävirastolla olisi aikaisempaa laajempi oikeus luovuttaa tietoja tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi.

Lait on tarkoitettu tulemaan voimaan 1 päivänä tammikuuta 2009.

SISÄLLYS

YLEISPERUSTELUT

1 Nykytila

1.1 Lainsäädäntö ja käytäntö

Sähköisen viestinnän tietosuojalaissa (516/2004) on säädetty sähköisten viestien välittäjien velvollisuuksista, joilla taataan viestinnän luottamuksellisuus ja viestintäverkkojen käyttäjien yksityisyys tavallisen lain tasolla. Perustuslain tasolla yksityiselämän eli yksityisyyden suojasta säädetään perustuslain 10 §:ssä. Yksityisyyden suojaan kuuluu myös viestinnän luottamuksellisuus, mikä tarkoittaa sitä, että viestin sisällön suojan lisäksi suoja ulottuu myös niihin tunnistamistietoihin, joista voidaan tunnistaa luonnollinen henkilö. Sähköisen viestinnän tietosuojalaissa viestinnän luottamuksellisuuden takaava sääntely ulotettiin koskemaan teleyrityksien lisäksi myös yhteisötilaajia. Yhteisötilaajia ovat viestintäpalvelun tai lisäarvopalvelun tilaajana olevat yritykset tai yhteisöt, jotka käsittelevät viestintäverkossaan käyttäjien luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja.

Sähköisen viestinnän tietosuojalain 4 §:n 1 momentin mukaan viesti, tunnistamistiedot ja paikkatiedot ovat luottamuksellisia, jollei sähköisen viestinnän tietosuojalaissa tai muussa laissa toisin säädetä. Sähköisen viestinnän tietosuojalain 9–14 §:ssä on säädetty niistä tilanteista, joissa joku muu kuin viestinnän osapuoli voi käsitellä tunnistamistietoja.

Lain 2 §:n määritelmän mukaan tunnistamistiedoilla tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Tunnistamistietoihin voi kuulua tietoja, jotka viittaavat muun muassa viestinnän reititykseen, kestoon, ajankohtaan tai siirrettävän tiedon määrään, käytettyyn protokollaan, lähettäjän tai vastaanottajan päätelaitteen sijaintiin tietyn tukiaseman alueella, lähettävään tai vastaanottavaan verkkoon ja yhteyden alkuun, loppuun tai kestoon. Tiedot voivat myös koskea muotoa, jossa viesti välitetään verkossa.

Perinteiseen postitoimintaan verrattaessa sähköisen viestinnän tunnistamistiedot ovat rinnastettavissa kirjeen tai postipaketin osoite- ja postileimatietoihin sekä kirjeen tai paketin kokoon ja muotoon.

Lain 9 §:n mukaan tunnistamistietoja saa käsitellä siinä määrin kuin se on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun toteuttamiseksi ja käyttämiseksi sekä näiden tietoturvasta huolehtimiseksi. Lisäksi tunnistamistietoja saa käsitellä laskutusta, markkinointia, teknistä kehittämistä ja palvelun käyttöä koskevien väärinkäytösten sekä vika- ja häiriötilanteiden havaitsemiseksi.

Lain 12 § sallii teleyritysten, lisäarvopalvelun tarjoajien ja yhteisötilaajien käsitellä tunnistamistietoja palvelujen teknistä kehittämistä varten. Laki ei salli tunnistamistietojen käsittelyä tilastollista analyysiä varten.

Lain 8 §:n 3 momentin mukaan tunnistamistietojen käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa, eikä sillä saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Tunnistamistietoja on sallittua luovuttaa ainoastaan niille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa. Käsittelyn jälkeen viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä.

Sellaiset tunnistamistiedot, joista on tunnistettavissa luonnollinen henkilö, ovat myös henkilötietoja. Lain 3 §:n soveltamisalasäännöksen mukaan henkilötietojen käsittelyyn sovelletaan, mitä henkilötietolaissa (523/1999) säädetään, jollei tästä laista muuta johdu.

Viestintäverkkojen väärinkäytösten ja yrityssalaisuuksien oikeudettoman paljastamisen selvittämisessä ovat käytettävissä tietohallinnolliset keinot, kuten käyttäjätietolokien tarkastaminen, pääsyä rajoittaviin järjestelmiin kirjautuvien tietojen tarkastaminen sekä järjestelmien teknisessä ylläpidossa kerätyt tiedot. Näiden tietojen käsittelylle ei sähköisen viestinnän tietosuojalaissa aseteta rajoituksia. Toisaalta näiden tietojen avulla pystytään vain poikkeuksellisesti selvittämään väärinkäytökset kokonaisuudessaan.

Toisin sanoen tietojärjestelmiä voidaan seurata vapaasti muun muassa väärinkäytöksiä selvitettäessä erilaisten käyttäjä-, tallennus- ja muiden sellaisten lokitietojen avulla.

Yksityisyyden suojasta työelämässä annetun lain (759/2004) 6 luvussa on säädetty työnantajalle kuuluvien sähköpostien esille hakemisesta ja avaamisesta sekä tähän liittyvästä menettelystä työntekijän ollessa estynyt hoitamaan työtehtäviään. Lain 18 §:n mukaan työnantajalla on oikeus hakea esille ja avata työntekijän käyttöön osoittaman sähköpostin viestejä vain, jos työnantaja on toteuttanut sanottujen viestien suojaksi laissa määritellyt tarpeelliset toimenpiteet.

Yksityisyyden suojasta työelämässä annetun lain 19 §:ssä on tarkemmin säädetty niistä perusteista, jolloin työnantaja voi hakea esille otsikkotietojen avulla työntekijän sähköpostiosoitteeseen saapuneet tai siitä lähetetyt viestit, joista työnantajan on välttämätöntä saada tieto toimintaansa liittyvien neuvottelujen loppuun saattamiseksi, asiakkaiden palvelemiseksi tai muutoin toimintojensa turvaamiseksi.

Yksityisyyden suojasta työelämässä annetun lain 20 §:n mukaan työnantaja saa myös avata hänelle kuuluvat viestit, jos on ilmeistä, että viestin otsikkotiedon perusteella viesti on tarkoitettu työnantajalle ja tiedon saaminen siitä on välttämätöntä, eikä viestin lähettäjään tai vastaanottajaan saada yhteyttä viestin sisällön selvittämiseksi eikä viestiä voida toimittaa toiseen osoitteeseen.

Viestin esille hakemisesta ja avaamisesta on laadittava siihen osallistuneiden henkilöiden allekirjoittama selvitys, josta ilmenee, mikä viesti on avattu, miksi viesti on avattu, avaamisen ajankohta, avaamisen suorittajat sekä kenelle avatun viestin sisällöstä on annettu tieto. Selvitys on ilman aiheetonta viivytystä toimitettava työntekijälle.

Rikoslain (39/1889) 38 luvun 3 ja 4 §:ssä viestintäsalaisuuden loukkaus on säädetty rangaistavaksi teoksi. Rikoslain 38 luvun 3 §:ssä säädetään rangaistus sille, joka oikeudettomasti avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä tai hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta. Luvun 4 §:ssä törkeän tekomuodon tunnusmerkeiksi on säädetty erityisen luottamusaseman käyttö, erikoislaitteen tai ohjelman käyttö taikka suunnitelmallisuus tai teon kohdistuminen erityisen luottamukselliseen viestiin tai huomattava yksityisyyden suojan loukkaus.

Liikesalaisuuksien suojasta on säädetty sopimattomasta menettelystä elinkeinotoiminnassa annetun lain (1061/1978) 4 §:ssä. Rikoslain 30 luvun 4–6 §:ssä on kriminalisoitu yritysvakoilu, yrityssalaisuuden rikkominen ja yrityssalaisuuden väärinkäyttö. Rikoslaissa omaksuttu yrityssalaisuuden käsite kattaa sekä liike- että ammattisalaisuudet. Liike- ja ammattisalaisuuksien suojasta on lisäksi säädöksiä useissa muissa laeissa.

Pakkokeinolain (450/1987) 5 a luvun 3 §:n mukaan televalvonta on mahdollista muun muassa sellaisten rikosten tutkinnassa, joista ankarin rangaistus on 4 vuotta vankeutta tai jotka kohdistuvat automaattiseen tietojenkäsittelyjärjestelmään. Koska yrityssalaisuusrikoksien enimmäisrangaistukset ovat kaksi vuotta vankeutta, televalvontaa voidaan käyttää vain sellaisen yritysvakoilun tutkinnassa joka samalla täyttäisi rikoslain 38 luvun 8 §:ssä tarkoitetun tietomurron tunnusmerkit.

Yksityisyyden suojasta työelämässä annetun lain perusteella työnantaja voidaan tuomita sakkorangaistukseen, jos muualla laissa ei ole säädetty ankarampaa rangaistusta.

Voimassa oleva sähköisen viestinnän tietosuojalaki ei salli tunnistamistietojen käsittelyä yrityssalaisuuksien oikeudettoman paljastamisen selvittämiseksi.

Tietoturvasta huolehtimisesta koskevista toimintaoikeuksista säädetään sähköisen viestinnän tietosuojalain 20 §:ssä.

1.2 Euroopan unionin lainsäädäntö

Euroopan parlamentin ja neuvoston 24 päivänä lokakuuta 1995 antama direktiivi 95/46/EY yksilöiden suojelusta ja henkilötietojen käsittelystä ja näiden tietojen vapaasta liikkuvuudesta, myöhemmin henkilötietodirektiivi on pantu täytäntöön henkilötietolailla. (523/1999). Direktiivillä on pyritty turvaamaan yksilöiden perusoikeudet ja yksityisyys henkilötietoja käsiteltäessä.

Euroopan parlamentin ja neuvoston 12 päivänä heinäkuuta 2002 antama direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, myöhemmin sähköisen viestinnän tietosuojadirektiivi, pantiin kansallisesti täytäntöön sähköisen viestinnän tietosuojalailla, joka tuli voimaan syyskuussa 2004.

Direktiivin 5 artiklassa on säädetty jäsenvaltioiden velvollisuudesta varmistaa yleisessä viestintäverkossa ja sähköisten viestintäpalveluiden välityksellä tapahtuvan viestinnän luottamuksellisuus.

Direktiivin 15 artiklassa on säädetty jäsenvaltioiden mahdollisuudesta toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan muun muassa direktiivin 5 artiklan mukaisten oikeuksien ja velvollisuuksien soveltamisalaa. Rajoitusten on oltava välttämättömiä, asianmukaisia ja oikeasuhteisia demokraattisen yhteiskunnan toimenpiteitä kansallisen turvallisuuden (valtion turvallisuus) sekä puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi henkilötietodirektiivin 13 artiklan 1 kohdan mukaisesti.

1.3 Kansainvälinen kehitys sekä ulkomaiden lainsäädäntö

Yleistä

Viestinnän luottamuksellisuutta ja henkilötietojen suojaa koskevia säännöksiä sisältyy eräisiin kansainvälisiin sopimuksiin. Euroopan neuvoston ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen (SopS 19/1990; Euroopan ihmisoikeussopimus) 8 artiklassa on turvattu yksityis- ja perhe-elämän, kodin ja kirjeenvaihdon suoja.

Euroopan neuvoston yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn yleissopimuksen (SopS 35–36/1992; Euroopan neuvoston tietosuojayleissopimus) 5 artiklan mukaan automaattisessa tietojenkäsittelyssä käsiteltävien henkilötietojen tulee olla asianmukaisesti ja laillisesti hankittuja ja käsiteltyjä. Tiedot saavat olla vain määriteltyihin ja laillisiin tarkoituksiin talletettuja, eikä niitä saa käyttää tavalla, joka on ristiriidassa mainittujen tarkoitusten kanssa.

Kansallinen voimassa oleva sääntely perustuu keskeisiltä osin sähköisen viestinnän tietosuojadirektiiviin. Direktiivin kansallisessa täytäntöönpanossa viestinnän luottamuksellisuuden takaavat velvoitteet ulotettiin koskemaan myös yhteisötilaajia.

Tässä ehdotuksessa esitetyt sääntelyn muutokset ovat pääosin kansallisen täytäntöönpanon yksityiskohtiin ja voimassa olevan kansallisen sääntelyn soveltamisessa ja tulkinnassa esiin tulleiden ongelmien korjaamiseen liittyviä ehdotuksia. Sähköisen viestinnän tietosuojalain yhteisötilaajan käsitettä ei ole omaksuttu muissa maissa. Tämän vuoksi kansainvälisessä vertailussa on keskitytty yleisesti yksityiselämän suojaa, yrityssalaisuuksien suojaa, henkilötietojen suojaa ja sähköisen viestinnän tietosuojaa koskevan lainsäädännön esittelyyn.

Ruotsi

Ruotsin perustuslaki koostuu neljästä säädöksestä. Näitä säädöksiä ovat hallitusmuoto (Regeringsform SFS 1974:152), perimysjärjestys, painovapausasetus (Tryckfrihetsförordning SFS 1949:105) ja sananvapauden perustuslaki (Yttrandefrihetsgrundlag SFS 991:1469). Hallitusmuodon 2 § sisältää säännöksen yksityisyyden suojasta. Hallitusmuodon 2 luvun 13 §:ssä todetaan, että ilmaisun ja tiedon liikkumisen vapautta, joita sananvapausasetus perustuslaillisesti suojaa, voidaan rajoittaa yksityiselämän koskemattomuuden suojaamiseksi. Hallitusmuodon 2 luvun 3 § turvaa lisäksi yksityiselämän koskemattomuuden, kun kyse on automaattisesta tietojenkäsittelystä.

Ruotsissa on säädetty erityinen laki yrityssalaisuuksien suojasta (Lag om skydd för företagshemligheter 1990:40). Lain 1§:n mukaan yrityssalaisuudella tarkoitetaan sellaista tietoa, jota elinkeinonharjoittaja liike- tai muussa toiminnassa pitää salaisena ja jonka paljastuminen on omiaan aiheuttamaan hänen liiketoiminnalleen vahinkoa heikentämällä kilpailun edellytyksiä. Tiedolla tarkoitetaan sekä eri tavoin dokumentoitua tietoa, mukaan lukien piirrokset, mallit ja vastaavat tekniset kuvaukset, että yksittäisten henkilöiden hallussaan pitämää tietoa jostain seikasta, vaikka sitä ei olisikaan dokumentoitu. Työntekijän, joka tahal-

laan tai huolimattomuudella käyttää hyväkseen tai paljastaa työnantajan yrityssalaisuuden, jonka on saanut tietoonsa työsuhteessa olosuhteissa, joissa hän käsitti tai hänen olisi pitänyt käsittää, ettei tietoa saa paljastaa, on korvattava toiminnastaan aiheutunut vahinko (7 §). Jos teko on tapahtunut työsuhteen päätyttyä, sovelletaan säännöstä vain, jos siihen on erityisiä syitä. Tällaiset tilanteet korostavat salassapitosopimusten merkitystä.

Ruotsin keskeinen tietosuojalaki on henkilötietolaki (Personuppgiftslag, 1998:204), jolla on pantu täytäntöön EU:n henkilötietodirektiivi. Laki sääntelee automatisoitujen henkilörekisterien käyttöä sekä julkisella että yksityisellä sektorilla. Ruotsissa ei ole erillistä lakia koskien työelämän yksityisyyden suojaa, vaan näitä kysymyksiä säännellään henkilötietolaissa. Erillinen työelämän tietosuojaa koskeva lainvalmistelu on vireillä ja lakiehdotus annettaneen vuoden 2008 alkupuolella.

Työntekijöiden henkilötietoja voidaan käsitellä vain lain sallimissa tilanteissa. Henkilötietojen käsittelyn tarkoitus on määriteltävä, eikä tietoja saa käsitellä muita tarkoituksia varten. Tarkoituksesta on informoitava niitä, joiden tietoja käsitellään. Lain sallimia tilanteita, joissa henkilötietoja voidaan käsitellä, ovat suostumukseen perustuva käsittely, sopimukseen perustuva käsittely, jolloin työntekijä ja työnantaja ovat sopineet henkilötietojen käsittelystä sopimuksen toteuttamiseksi sekä käsittely oikeudellisen velvoitteen täyttämiseksi. Samoin henkilötietoja voi käsitellä työntekijän tärkeän edun suojaamiseksi tai jos tietoja käytetään työtehtävän suorittamiseen viranomaisessa sekä muissa tapauksissa, joissa työnantajan tai muun henkilön, jolle henkilötiedot luovutetaan, intressi on suurempi kuin työntekijän yksityisyyden. Työnantajan oikeus valvontaan työpaikoilla on ratkaistu Ruotsin oikeuskäytännössä intressipunninnalla, jossa vertaillaan työnantajan direktio-oikeutta ja työntekijöiden yksityisyyden suojaa. Yksityisyyttä rajoittavien toimenpiteiden pitää olla oikeassa suhteessa tavoiteltuun päämäärään nähden.

Sähköisen viestinnän tietosuojadirektiivi on pantu Ruotsissa täytäntöön lailla sähköisestä viestinnästä (Lag om elektronisk kommunikation, 2000:389). Sähköisen viestinnän laki sääntelee myös viestintämarkkinakysymyksiä, sillä lailla on pantu täytäntöön koko EU:n viiden tietoliikennettä koskevan direktiivin lainsäädäntöpaketti. Ruotsissa ei siten ole erillistä sähköisen viestinnän tietosuojalakia. Ruotsin sähköisen viestinnän lain sääntely kohdistuu ainoastaan teleyrityksiin ja lisäarvopalvelun tarjoajiin eikä yhteisötilaajiin, jotka käsittelevät viestintäverkossaan käyttäjien luottamuksellisia viestejä tunnistamistietoja tai paikkatietoja.

Sähköisen viestinnän lain 2 §:n mukaan henkilötietolaki soveltuu myös tietoverkkojen ja sähköisten viestintäpalvelujen käyttöön, ellei laista muuta johdu.

Norja

Norjan perustuslaki on vuodelta 1814 (Kongerikets Norges Grundlov). Perustuslaki on muodoltaan hieman muista kansainvälisen vertailun kohdemaista poikkeava, sillä se ei sisällä nimenomaista yksityiselämän suojaa koskevaa määräystä. Yksityisyyden suoja on kehittynyt Norjassa oikeuskäytännön myötä. Vuonna 1952 Norjan korkein oikeus totesi, että henkilöllisyys nauttii Norjan oikeudessa suojaa ja henkilöllisyyden suoja käsittää yksityiselämän suojan. Norja ei ole Euroopan unionin jäsen, mutta on osa Euroopan talousaluetta, joten niin sanottu ensimmäisen pilarin lainsäädäntö, johon tietosuojaa ja sähköistä kaupankäyntiä koskevat direktiivit kuuluvat, on Norjaa sitovaa.

Norjassa ei ole erillistä lakia yritysalaisuuksien suojasta, vaan asiasta on säädetty vuonna 1972 säädetyssä markkinalaissa (Lov om kontroll med markedsføring og avtalevilkår, markedsføringsloven).

Norjan nykyinen tietosuojalaki (Lov om behandling av personopplysninger), on vuodelta 2000. Sitä täydentää tietosuoja-asetus (Forskrift om behandling av personopplysninger). Laki perustuu henkilötietodirektiiviin, joten sen määräykset ovat lähes kauttaaltaan samansisältöiset kuin direktiivin.

Norjassa sähköisen viestinnän tietosuojadirektiivi on pantu täytäntöön sähköistä viestintää koskevalla yleislailla eli Ekomlovenilla (Lov om elektronisk kommunikasjon).

Norjassa ei ole erillistä lakia yksityisyyden suojasta työelämässä, vaan asiaa on ohjeistettu Datatilsynetin ohjeilla. Pääsääntönä on, että

työnantajan halutessa lukea työntekijän sähköpostia ja muita tietokansioita, tämä tarvitsee työntekijän suostumuksen tai asia ratkaistaan Norjan tietosuojalain 8 § f -kohdan ja direktiivin tarkoittaman intressivertailun perusteella. Norjalainen työnantaja voi päättää direktio-oikeutensa perusteella, että työhön liittyviin tarkoituksiin on käytettävä työnantajan tietojärjestelmiä. Työnantajan on laadittava säännöt tietojärjestelmän käytölle, jolloin on täsmennettävä, missä laajuudessa järjestelmää voidaan käyttää yksityisiin tarkoituksiin. Näissä säännöissä, jotka on liitettävä yrityksen sisäisen tarkastuksen sääntöihin, on ilmaistava, missä olosuhteissa työnantaja voi lukea yksityistä sähköpostia. Lähtökohtana on, että jos tällaisia sääntöjä ei ole, ei työnantaja ole oikeutettu lukemaan työntekijän sähköpostia.

Mikäli työnantaja epäilee työntekijää epälojaaliudesta tai tämän toimivan sisäisten sääntöjen ja ohjeiden vastaisesti, voi työnantajalle syntyä oikeus tarkastaa työntekijän sähköposti- ja kirjeenvaihtoa. Jos työnantajalla on riittävät perustelut epäilyksille, voi asiallisten perustelujen vaatimus tarkastuksille täyttyä. Mikäli työnantajan tarkastusintressit konkreettisessa tapauksessa ovat suurempia kuin työntekijän oikeus yksityisyyteen, voidaan tarkastus suorittaa ilman työntekijän suostumusta.

Tanska

Tanskan vuodelta 1953 peräisin oleva perustuslaki sisältää kaksi yksityisyyden suojaa koskevaa määräystä. Perustuslain 71 § takaa kansalaisen henkilökohtaisen koskemattomuuden. Tanskan kansalaisen vapautta ei voi riistää poliittisen tai uskonnollisen vakaumuksen vuoksi tai syntyperän johdosta.

Perustuslain 72 § määrää kotirauhan loukkaamattomaksi. Kotietsintä, kirjeiden ja muun kirjallisen aineiston takavarikoiminen ja tutkiminen, samoin kuin postin, tietoliikenne- ja puhelinsalaisuuden murtaminen voi tapahtua ainoastaan oikeuden määräyksellä, ellei laissa ole toisin määrätty. Lainkohta soveltuu kaikkeen tietoliikenteeseen ja sähköiseen tietoon.

Tanskan markkinointilaki (Maerkedsfoeringsloven 1389, 21.12.2005) sääntelee yrityssalaisuuksien suojaa. Lain 19 §:n mukaan henkilö, joka on palvelussuhteessa yritykseen tai toimii yhteistyössä sen kanssa tai joka suorittaa tehtävää yrityksen lukuun ei saa hankkia tai yrittää hankkia tietoonsa tai haltuunsa kyseisen yrityksen yrityssalaisuuksia luvattomasti. Jos edellä mainittu henkilö on hankkinut tiedon yrityssalaisuudesta laillisesti, hän ei saa ilman asianmukaista lupaa luovuttaa tai käyttää yrityssalaisuutta. Kielto on voimassa kolme vuotta palvelusuhteen, yhteistyön tai tehtävän päättymisestä. Näitä sääntöjä sovelletaan samalla tavoin muuhun henkilöön, jolla on laillinen pääsy yritystietoon.

Tanskan tietosuojalaki (Lov om behandling af personoplysningar nr 429, 31.5.2000) on vuodelta 2000. Lailla on pantu täytäntöön henkilötietodirektiivi. Sähköisen viestinnän tietosuojamääräykset sisältyvät telelainsäädännön vuoden 2003 muutokseen (Lov om konkurrence- og forbrugerforhold på telemarkedet Lov nr. 418 af 31. maj 2000), jolla sähköisen viestinnän tietosuojadirektiivi pantiin täytäntöön.

Tanskassa ei ole erillistä työelämän tietosuojalakia, vaan työelämän yksityisyyden suojaa säännellään henkilötietolain pohjalta. Maan viranomaiset eivät ole ottaneet erityisen jyrkkää kantaa yksityisyyden suojaamiseen työelämässä. Tanskan tietosuojalaki tarjoaa työnantajalle mahdollisuuden kerätä ja jopa paljastaa henkilötietoja ilman työntekijän suostumusta, milloin tämä on välttämätöntä oikeudellisen velvoitteen täyttämiseksi, yhteiskunnan kannalta merkityksellinen tehtävän suorittamiseksi tai laillisen tarpeen täyttämiseksi, joka menee työntekijän edun edelle.

Saksa

Saksan liittotasavallan perustuslaki (Grundgesetz) on vuodelta 1949, ja sitä on viimeksi muutettu Saksojen jälleenyhdistymisen yhteydessä 1990. Perustuslain 10 artiklassa turvataan kirje- ja tietoliikennesalaisuus ja poikkeuksia tähän voidaan tehdä ainoastaan lain säännöksin. Silloin, kun rajoituksen tarkoituksena on demokraattisen yhteiskuntajärjestelmän tai liittovaltion turvallisuuden turvaaminen, voidaan lainsäädännössä määrätä, ettei kajoamisen kohteeksi joutunut henkilö saa tietää toimenpiteestä. Tuomioistuimien asemesta oikeusturvatienä toimivat tällöin liittopäivien nimeämät elimet.

Perustuslain turvaamasta viestintäsalaisuudesta säädetään tarkemmin telekommunikaatiolain eli Telekommunikationsgesetzin 85 §:ssä. Viestintäsalaisuus ulottuu myös yhteydenottoyrityksiin. Telekommunikaatiolain 86 §:ssä säädetään telekuuntelun kiellosta sekä vastaanottolaitteiden ylläpitäjän salassapitovelvollisuudesta. Vastaavasti lain 87 §:ssä säädetään ammattimaisessa tarkoituksessa tietoliikennelaitteita ylläpitävän henkilön velvollisuudesta ylläpitää teknisiä suojakeinoja muun muassa viestintäsalaisuuden ylläpitämiseksi.

Pakkokeinoista, myös tietoliikennettä koskevista, säädetään rikosprosessijärjestyksessä eli Strafprozessordnungissa (StPO).

Saksassa yrityssalaisuuksien suojasta säädetään vilpillistä kilpailua koskevan lain 17 §:ssä. Yrityssalaisuuden piiriin kuuluu kaupallisesti arvokas tieto, joka ei ole julkisesti saatavilla ja se, jolle tieto kuuluu, on ilmaissut objektiivisen aikomuksen tiedon salassa pitämiseksi. Lainkohdan 1 momentin mukaan rangaistaan sellaista työntekijää, oppisopimuskoulutuksessa olevaa tai muuta henkilöä, joka työsuhteen kuluessa ilmaisee ilman lupaa kolmannelle kauppa- tai teollisuussalaisuuden, joka on hänelle uskottu tai saatettu hänen tietoonsa työsuhteen puitteissa, jos hän tekee paljastuksen kilpailun tai henkilökohtaisen edun vuoksi, hyödyttääkseen kolmatta osapuolta tai vahingoittaakseen elinkeinonharjoittajaa. Vilpillistä kilpailua koskevan lain 17 §:n 2 momentin mukaan rangaistaan henkilöä, jotka yllä kuvatuista syistä hankkii luvatta kauppa- tai teollisuussalaisuuden käyttämällä teknisiä keinoja, luomalla salaisuuden sisältävän kopion tai irrottamalla esineen, johon salaisuus on sisällytetty. Sama koskee henkilöä, joka käyttää tai ilmaisee toiselle kaupallisen tai teollisen salaisuuden, jonka on hankkinut tai saanut ilman lupaa sen luvatta ilmaisseelta työntekijältä tai oman tai toisen henkilön toiminnan tuloksena.

Saksassa on Euroopan Unionin tiukimpia tietosuojalakeja. Maailman ensimmäinen tietosuojalaki säädettiin vuonna 1970 Hessenin osavaltiossa. Saksan nykyinen tietosuojalaki (Bundesdatenschutzgesetz) on vuodelta 1990, ja se on viimeksi uudistettu vuonna 2002. Laki antaa rekisteröidyille laajat mahdollisuudet vastustaa tiedon käsittelyä. Laki vaatii yritysien nimeävän tietosuojavastaavan, jos yritys kerää, käsittelee tai käyttää henkilötietoja. Henkilötietoja sisältävät tietokannat on rekisteröitävä tietosuojaviranomaisessa. Rekisteröitävän antaman suostumuksen merkitystä on korostettu.

Sähköisen viestinnän tietosuojaa koskevat määräykset sisältyvät vuonna 2004 muutettuun telekommunikaatiolakiin, johon yhdistettiin vuoden 2000 tietoliikennettä koskeva tietosuoja-asetus.

Kysymys työnantajan mahdollisuudesta seurata työntekijän sähköpostin tai internetin käyttöä on oikeuskäytännön varassa. Lähtökohtaisesti työnantajalla ei ole oikeutta saada tietoa työntekijän sähköposteista tai internetin käytöstä. Jos työnantaja on kieltänyt viestintäpalveluiden käytön yksityisiin tarkoituksiin, voi työnantaja seurata vain internetin käyttöön liittyviä tunnistamistietoja. Jos työnantajalla on konkreettinen epäily, että viestintäpalveluita on käytetty luvatta, saa työnantaja seurata niiden käyttöä siinä määrin kuin on välttämätöntä väärinkäytöksen selvittämiseksi.

Viro

Viron nykyinen perustuslaki on vuodelta 1992. Laki tunnustaa oikeuden yksityisyyteen, viestinnän luottamuksellisuuteen sekä, ainakin osittain, tietosuojaan.

Artiklan 43 jokaisella on oikeus luottamukselliseen viestintään kirjeen, sähkeen, puhelimen tai muun yleisesti käytetyn viestintävälineen avulla Poikkeuksia voidaan tehdä vain oikeuden suostumuksella, lain määräämissä tapauksissa ja lain mukaisia menettelytapoja noudattaen rikoksen ehkäisemiseksi tai rikostutkinta-aineiston hankkimiseksi. Viestinnän kuuntelu edellyttää tuomioistuimen myöntämää lupaa. Laittomasti hankittua todistusaineistoa ei voi esittää oikeudessa.

Yrityssalaisuuksien suojaa säännellään Virossa vuodelta 1993 peräisin olevassa kilpailulaissa.(RT I 1993, 47, 642, voimaan 1.1.1994.) Lain 7 § määrittelee yrityssalaisuuden väärinkäytön epärehelliseksi kilpailuksi, joka on kielletty. Kilpailulaki ei sisällä määräyksiä työntekijöiden velvollisuuksista yrityssalaisuuksien suhteen, vaan nämä velvollisuudet määräytyvät työlainsäädännön lojaliteettisäännösten perusteella.

Viroon säädettiin ensimmäinen tietosuojalaki vuonna 1996. Nykyinen lainsäädäntö, Viron henkilötietosuojalaki (RT I 2003, 26,158), jolla lainsäädäntö saatetaan henkilötietodirektiivin mukaiseksi, on tullut voimaan 1. lokakuuta 2003 ja sitä on jo muutettu kerran sen jälkeen.

Laki sähköisestä viestinnästä (RT2 I 2004, 87, 593, voimaan 1. tammikuuta 2005) sisältää luvussa 10 määräykset tietoturvasta ja tietosuojasta.

Iso-Britannia

Isossa-Britanniassa perusoikeussääntely perustuu oikeuskäytännön lisäksi Euroopan neuvoston ihmisoikeussopimukseen. Euroopan neuvoston yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi on saatettu Isossa-Britanniassa valtionsisäisesti voimaan vuoden 1998 Human Rights Actilla (Human Rights Act 1998). Yksityis- ja perhe-elämä on suojattu sopimuksen 8 artiklassa ja sananvapaus 10 artiklassa.

Yrityssalaisuuksien suoja Isossa-Britanniassa perustuu oikeuskäytäntöön ja salassapitosopimuksiin. Henkilötietojen suojasta säädetään vuonna 1998 annetussa Data Protection Actissa, jolla on pantu täytäntöön EU:n henkilötietodirektiivi. Sähköisen viestinnän tietosuojadirektiivi on saatettu voimaan vuonna 2003 Privacy and Electronic Communications (EC Directive) Regulations 2003 (2003 No. 2426) -säädöksellä, jossa on viestintäpalvelujen tarjoajia koskevat säädökset muun muassa tunnistamis- ja paikkatietojen luottamuksellisuudesta sekä sähköisestä suoramarkkinoinnista. Suomessa omaksuttua yhteisötilaajan käsitettä ei Isossa-Britanniassa ole käytössä. Säännöksen kohdan 29 mukaan viestintäpalvelun tarjoaja saa käsitellä tietoja, jos se on tarpeen laillisten oikeuksien perustamiseksi, käyttämiseksi tai puolustamiseksi, tai, jos käsittely muuten on tarpeen oikeusprosessiin liittyen. Lisäksi tietoja saa käsitellä jos se on tarpeen rikosten estämiseksi tai selvittämiseksi.

Sähköisen viestinnän luottamuksellisuus perustuu Isossa-Britanniassa vuonna 2000 annettuun Regulation of Investigatory Powers Actiin (RIPA). Vuonna 2000 RIPA:n nojalla on annettu säännös Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (2000 No. 2699). Säädös sallii luottamuksellisen viestinnän pääsäännöstä poiketen yritysten ja julkisten tahojen seurata verkossaan tapahtuvaa viestintää myös viestien sisällön osalta muun muassa jonkin seikan toteamiseksi, säädösten tai käyttösääntöjen noudattamisen varmistamiseksi, kansallisen turvallisuuden vuoksi, rikosten tutkimiseksi ja estämiseksi tai luvattoman käytön havaitsemiseksi.

Viestintäverkon ylläpitäjän tulee ilmoittaa verkon käyttäjille siitä, että verkon liikennettä voidaan seurata.

Venäjä

Venäjän perustuslaki on vuodelta 1993. Perustuslain 23 artiklan mukaan jokaisella on oikeus yksityiselämään, henkilökohtaisiin ja perheen salaisuuksiin sekä henkilökohtaisen kunnian ja maineen ylläpitämiseen. Lisäksi jokaisella on oikeus yksityisyyteen kirjesalaisuuden, puhelin- ja kaapeliliikenteen ja muiden kommunikaatiomuotojen osalta. Poikkeuksia voidaan sallia ainoastaan oikeuden määräyksellä.

Tiedon avoimuuteen ja suojaamiseen liittyvät kysymykset on Venäjällä käytännössä keskitetty liittovaltion tasolle. Keskeinen säännös on vuoden 1995 Venäjän federaation laki tiedosta, tiedon käsittelystä ja suojaamisesta. Lain viimeisin muutos on astunut voimaan 1.1.2004.

Laki tiedosta, tiedon käsittelystä ja suojaamisesta suojaa tiedonvälityksen vapautta. Sen mukaan puhelinkeskustelujen nauhoittamisen, sähköisen viestinnän tarkastamisen, kirjelähetysten viivyttämisen, tarkastamisen ja takavarikoimisen ja muun puuttumisen tiedonvälityksen salaisuuteen on tapahduttava oikeuden määräyksellä.

Liittovaltion laki yrityssalaisuuksien suojasta (Laki nro N98-FZ, 29.7.2004) sääntelee kaupallisten salaisuuksien käyttöä ja sitä, kuinka tiedon luottamuksellisuus voidaan turvata. Laki määrittelee liike- ja ammattisalaisuuden ainoastaan yleisin termein. Liikesalaisuuden haltijan tulee yksilöidä liikesalaisuutensa. Toisaalta laki luettelee tiedon, jota ei voida missään oloissa pitää yritysalaisuutena ja luetteloi tietoa, jota voidaan tilanteen mukaan pitää yrityssalaisuutena. Tällaista tietoa

on mm. työntekijöiden määrä, palkitsemisjärjestelmät, työolot mukaan luettuina turvallisuusjärjestelyt, työperäiset tapaturmat, ammatilliset kuolleisuusluvut, avoimena olevat työpaikat sekä lainrikkomukset.

Venäjän lainsäädännössä turvataan yrityssalaisuuksia myös siviilikoodin ja kilpailulainsäädännön määräyksillä. Venäjän federaation siviilikoodin artikla 139 määrää, että liike- ja ammattisalaisuudet on suojattu siviilioikeudellisin oikeussuojakeinoin, erityisesti vahingonkorvausvelvollisuuksin. Vahingonkorvausvelvolliseksi voivat joutua liikesalaisuuden haltijan työntekijät sekä kolmas henkilö, joka vastaanottaa luvattomasti tiedon yrityssalaisuudesta. Mainitun siviilikoodin artiklan mukaan tiedolla tulee olla todellinen tai mahdollinen kilpailullinen arvo. Toiseksi tiedon tulee olla tuntematon ulkopuolisille sekä yleisesti lain sallimien informaatiokanavien saavuttamattomissa. Kolmanneksi tiedon omistajan tulisi suorittaa toimenpiteitä suojatakseen tiedon luottamuksellisuutta. Muussa tapauksessa tiedon omistaja ei voi näyttää, että tieto on yrityssalaisuus.

Yrityksen on lainsäädännön mukaan tehtävä useita toimia saadakseen tiedolle yrityssalaisuuden aseman. Yrityksen on luetteloitava organisaation liikesalaisuuksien piiriin kuuluva aineisto, yrityksen on rajoitettava pääsyä liikesalaisuuteen luomalla menettelyt kyseisen tiedon käsittelyä ja menettelyn noudattamisen valvontaa varten. Yrityksen on myös lueteltava henkilöt, joilla on pääsy kyseiseen tietoon. Sen lisäksi yrityksen on säänneltävä suhdetta liikesalaisuustiedon käyttöön. Työntekijöiden osalta tämä tapahtuu työsopimusten ja liikekumppanien osalta liikesopimusten avulla. Liikesalaisuustieto on lisäksi varustettava tiedon omistajan osoittavalla leimalla.

Venäjän lain mukaan henkilöstön on noudatettava työnantajan asettamia luottamuksellisuusmääräyksiä. Henkilökunnan jäsen ei myöskään saa paljastaa työnantajan liikesalaisuutta aikana, joka on määritelty työnantajan kanssa sopimuksessa työsuhteen kestäessä, tai kolmena työsuhteen päättymisen jälkeisenä vuotena, milloin sopimusta ei ole solmittu. Työntekijän on myös korvattava työnantajalle vahinko, jonka tämä on kärsinyt työntekijän luovuttaessa tietoonsa tulleita yrityssalaisuuksia. Venäjän työsopimuslaki sisältää täsmälliset määräykset työntekijän korvausvelvollisuudesta ja rangaistusvastuusta. Työsuhteen päättyessä työntekijän on luovutettava työnantajalle kaikki liikesalaisuuksia sisältävä aineisto. Työnantajan on puolestaan tiedotettava työntekijöille yrityssalaisuuksista, työntekijän velvollisuuksista ja rikkomuksista seuraavista sanktioista.

Laki tiedosta, tiedon käsittelystä ja suojaamisesta sääntelee myös henkilötietoja yleisellä tasolla, vaikka Venäjä ei olekaan mukana Euroopan neuvoston tietosuojayleissopimuksessa. Henkilöön liittyvät tiedot katsotaan luottamukselliseksi tiedoksi. Henkilötiedot eli tieto kansalaisista tarkoittaa tietoja tosiseikoista, tapahtumista ja elämäntavoista, jotka yksilöivät yksittäisen kansalaisen. Kyseisen lain mukaan luonnollisen henkilön yksityiselämään liittyvän tiedon kerääminen, säilyttäminen, käyttö, levittäminen samoin kuin henkilökohtaiseen tai perhesalaisuuteen liittyvän tiedon käsittely ilman henkilön suostumusta on kielletty, ellei kyse ole tiedon käsittelystä oikeuden määräyksen perusteella tai asianomainen henkilö on antanut suostumuksensa toimenpiteeseen. Samoin viestintäsalaisuutta loukkaavan tiedon kerääminen, säilyttäminen, käyttö tai levittäminen on sallittu vain erityismääräysten nojalla tai asianosaisen suostumuksin.

Laki tiedosta, tiedon käsittelystä ja suojaamisesta viittaa yksityiskohtaisempaan federaation lainsäädäntöön. Seikkaperäinen tietosuojalaki on edelleen valmisteilla. Näitä koskevat ehdotukset tehtiin vuosina 1998 ja 2000 ja lakiesitys on ollut käsiteltävänä Venäjän duumassa vuoden 2006 aikana. Taustalla on Venäjän pyrkimys ratifioida Euroopan neuvoston tietosuojayleissopimus.

Venäjällä ei toistaiseksi ole sähköisen viestinnän tai työelämän tietosuojalainsäädäntöä.

1.4 Nykytilan arviointi

Sähköisen viestinnän tietosuojalain viestinnän luottamuksellisuuden tavoitteet ovat toteutuneet yrityksissä ja yhteisöissä melko hyvin.

Sähköisen viestinnän tietosuojalaki mahdollistaa yhteisötilaajille tunnistamistietojen käsittelyn niiden normaalin toiminnan edellyttämässä laajuudessa. Käytännössä eräiden voimassa olevien säännösten soveltaminen on osoittautunut ongelmalliseksi. Erityisesti lain

13 § on osoittautunut muotoilultaan niin suppeaksi, ettei se takaa yhteisötilaajille riittäviä toimintamahdollisuuksia.

Yhteisötilaajien mahdollisuuksissa selvittää ja saattaa esitutkintaan viestintäverkkoihinsa kohdistuneita sähköisen viestinnän avulla tapahtuneita väärinkäytöksiä on ilmennyt vaikeuksia. Lain 13 §:n väärinkäytössäädöksen soveltaminen yhteisötilaajien viestintäverkkojen väärinkäytöksiin on osoittautunut epäselväksi. Voimassaolevan lain ei ole katsottu sallivan yhteisötilaajien kerätä väärinkäytöksistä itse näyttöä, eikä televalvontakaan ole useimmissa tapauksissa ollut käytettävissä.

Elinkeinoelämän ja viranomaisten yhteisessä strategiassa yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi (Sisäasiainministeriön julkaisuja 15/2006) sähköisen viestinnän tietosuojalain on mainittu olevan jossakin määrin ongelmallinen rikosten uhriksi joutuneiden yritysten kannalta. Strategiassa pidettiin epäkohtana sitä, että yrityksillä on puutteelliset mahdollisuudet saattaa poliisin tutkittavaksi yrityssalaisuuksien luvattomia luovutuksia, jos luovutus on tehty sähköisessä muodossa.

Tiedustelutoimintaa kartoittavissa yritysturvallisuustutkimuksissa, joita muun muassa suojelupoliisi tekee säännöllisin välein, noin 10 % vastanneista yrityksistä ilmoittaa havainneensa ja 18 % epäilleensä laitonta tiedonhankintaa viimeisen kahden vuoden aikana.

Sähköisen viestinnän avulla toteutettujen väärinkäytösten selvittämisessä ja esitutkintaan saattamisessa on ilmennyt ongelmia, joita ei lakia säädettäessä osattu ennakoida. Myös teleyritykset ovat suhtautuneet varovaisesti säännösten tulkintaan. Tämän lisäksi ongelmia on saattanut syntyä siitä, että toimijoilla ovat menneet lain tarkoittamat viestinnän osapuolen, teleyrityksen ja yhteisötilaajan roolit sekaisin.

Viestintäpalvelujen tuottaminen ja käyttö vaatii runsaasti teknistä kehitystyötä. Käytännössä on tullut esille, että asianmukaiseen kehitystyöhön sisältyy piirteitä, jotka eivät ole luonteeltaan yksinomaan teknisiä, mutta ovat täysin välttämättömiä toiminnan kehittämisen kannalta. Tästä syystä sääntelyn tulisi mahdollistaa yhteisötilaajalle oikeuden käsitellä tunnistamistietoja kehittääkseen palvelujaan ja toimintaansa muutoinkin kuin yksinomaan teknisessä mielessä. Samoin on tullut esille, että teleyritykset eivät ole joko lain tai sen tulkintojen takia luovuttaneet yhteisötilaajille tunnistamistietoja, joiden perusteella yritys tai yhteisö olisi voinut optimoida käytössään olevien kiinteiden puhelinten ja kännyköiden välistä puhelinliikennettä mahdollisimman kustannustehokkaalla tavalla.

Voimassa olevan lain 20 §:n tietoturvasäännös ei vastaa täysin asianmukaisen tietoturvatyön vaatimuksia. Tietoturvauhat ovat lain säätämisen jälkeen olennaisesti muuttuneet ja laaja-alaistuneet. Kaikesta sähköpostiliikenteestä yli puolen arvioidaan olevan eitoivottuja suoramarkkinointiviestejä. Niin sanotun roskapostin suuri määrä saattaa vaarantaa yksittäisen käyttäjän viestintämahdollisuudet.

Elinkeinoelämän ja viranomaisten yhteisessä strategiassa yrityksiin kohdistuvien rikosten ja väärinkäytösten torjumiseksi on todettu sähköisen viestinnän tietosuojalain tietoturvasäännöksen saaneen sellaisen tulkinnan, mikä ei mahdollista tarkoituksenmukaista suojautumista ammattimaisesti toteutetulta hyökkäysliikenteeltä.

Tästä syystä tehokkaiden tietoturvatoimenpiteiden tulee olla käytettävissä aiempaa joustavammin.

2 Esityksen tavoitteet ja keskeiset ehdotukset

Esityksessä ehdotetaan muutoksia sähköisen viestinnän tietosuojalakiin ja eräisiin muihin lakeihin.

Käytännön tarpeista johtuen ehdotetaan teleyrityksille, lisäarvopalvelun tarjoajille ja yhteisötilaajille oikeutta käsitellä tunnistamistietoja automaattisen tietojenkäsittelyn avulla tilastollista analyysiä varten, jotta toimijat voisivat muun ohella kehittää palvelujaan ja toimintojaan muutoinkin kuin yksinomaan teknisessä mielessä.

Esityksessä ehdotetaan laajennettavaksi yhteisötilaajien oikeuksia käsitellä tunnistamistietoja väärinkäytöstilanteissa. Samalla teleyritysten ja lisäarvopalvelujen tarjoajien käsittelyoikeuksia väärinkäytöstilanteissa esitetään tarkistettavaksi.

Sääntelyä ehdotetaan täsmennettäväksi siten, että yhteisötilaajalla olisi tietyin edellytyksin oikeus käsitellä sähköisen viestinnän tunnistamistietoja viestintäverkkonsa ja maksullisten tietoyhteiskunnan palvelujen luvattoman käytön ja viestintäpalvelujen ohjeen vastaisen käytön selvittämiseksi.

Yhteisötilaajien tunnistamistietojen käsittelyoikeutta ehdotetaan laajennettavaksi siten, että yhteisötilaaja voisi käsitellä tietyin edellytyksin tunnistamistietoja, kun kyse olisi elinkeinotoiminnan kannalta keskeisten yrityssalaisuuksien oikeudettomasta paljastamisesta.

Sekä viestintäverkon tai viestintäpalvelun ohjeen vastaisen luvattoman käytön että yrityssalaisuuksien osalta edellytettäisiin, että viestintäverkon ja viestintäpalveluiden suunniteltu käyttö sekä yrityssalaisuuksien suoja on järjestetty asianmukaisin tietoturva- ja käyttäjähallintotoimenpitein. Ehdotetut tunnistamistietojen käsittelyoikeudet eivät oikeuttaisi yhteisötilaajia saamaan tietoa viestien sisällöistä.

Tunnistamistietojen käsittelyllä yhteisötilaaja ei saisi selville muiden kuin omien viestintäpalveluidensa kautta lähetettyjen ja vastaanotettujen viestien tunnistamistiedot. Kaupallisesti tarjolla olevien sähköposti-, verkkopankki- tai muiden teknisesti suojattujen palveluiden käytöstä tunnistamistiedot paljastaisivat vain käytetyn palvelun osoitteen, käytön ajankohdan ja keston.

Työnantaja-asemassa olevan yhteisötilaajan tulisi ottaa tunnistamistietojen käsittelyyn liittyvät asiat yhteistoimintamenettelyssä käsiteltäviksi ja tiedottaa niistä työntekijöille.

Ehdotettujen muutosten mahdollistamaa yhteisötilaajien tunnistamistietojen käsittelyä valvoisi tietosuojavaltuutettu.

Ehdotettu tietoturvasäännöksen muutos saattaisi säännöksen vastaamaan paremmin nykyisiä tarpeita viestintäverkkojen tai palvelujen tietoturvasta huolehtimiseksi. Yhteiskunnan elintärkeät toiminnot ovat kiinteästi riippuvaisia viestintäverkoista, viestintäpalveluista ja tietojärjestelmistä. Kriittisen infrastruktuurin suojaamisessa keskeisessä asemassa on sähköisten tieto- ja viestintäjärjestelmien toiminnan varmistaminen. Suomeen kohdistuvat tietoturvauhat ovat usein peräisin muista maista. Koska vaikutusmahdollisuudet ulkomaisiin toimijoihin tai järjestelmiin ovat rajatut, ongelmien haittavaikutukset on voitava minimoida kotimaisten teleyritysten, lisäarvopalvelujen tarjoajien ja yhteisötilaajien toimenpitein.

Viestintäviraston saamien tietojen luovuttamismahdollisuuksien muutosten tarkoituksena on tehostaa tietoturvauhkien torjumista ja selvittämistä.

2.1 Muutosten vaikutusten seuranta

Ehdotettujen muutosten vaikutusten arvioimiseksi liikenne- ja viestintäministeriöön on tarkoitus asettaa seurantaryhmä, jossa olisivat edustettuina ainakin yhteisötilaajien edustajat, Viestintävirasto, tietosuojavaltuutettu, teleyritykset ja työmarkkinakeskusjärjestöt.

Seurantaryhmän toimikausi alkaisi vuoden 2009 tammikuussa ja kestäisi vuoden 2010 kesäkuun loppuun. Seurantaryhmä teettäisi tutkimuksen ehdotettujen tunnistamistietojen käsittelyoikeuksien muutosten vaikutuksista yritysten tietohallintoon ja sähköisen viestinnän luottamuksellisuuteen. Lisäksi seurantaryhmä seuraisi tunnistamistietojen viranomaisvalvonnan toteutumista ja valvonnan voimavarojen riittävyyttä.

3 Esityksen vaikutukset

3.1 Taloudelliset vaikutukset

Esityksellä voidaan arvioida olevan positiivisia taloudellisia vaikutuksia teleyrityksille, yhteisötilaajille, viranomaisille ja kuluttajille. Selkeät ja yksiselitteiset käsittelysäännöt ja tiedonsaantia koskevat säännökset vähentävät tarpeettomia prosesseja ja säästävät kaikkien toimijoiden resursseja.

Ehdotus tarjoaa paremmat edellytykset sähköiselle asioinnille, jolla on kustannus- ja kilpailukykyvaikutusten vuoksi merkitystä taloudelliselle kehitykselle kotimaassa, yritysten kilpailukyvylle, sisämarkkinoiden ja siten koko eurooppalaisen hyvinvointiyhteiskunnan kehitykselle. Samalla sähköisiä palveluja käyttävien kuluttajien asema paranee ja lakia valvovien viranomaisten asema helpottuu.

Yritykset ja muut organisaatiot yhteisötilaajina soveltavat sähköisessä viestinnässään lain tunnistamistietojen käsittelysäännöksiä. Käsittelysäännökset ovat mahdollistaneet yhteisötilaajille viestinnän luottamuksellisuudesta huo-

limatta oikeuden käsitellä käyttäjien tunnistamistietoja ja samalla on turvattu käyttäjien yksityisyyden suoja uutta viestintäteknologiaa käytettäessä. Lain velvoitteiden selväpiirteisyys suomalaisten yritysten ja yhteisöjen aseman kannalta on olennaista.

3.2 Vaikutukset yritystoimintaan

Ehdotetut tunnistamistietojen käsittelysääntöjen muutokset parantavat sekä pienten että suurten yritysten toimintaedellytyksiä. Ehdotetut muutokset parantavat yhteisötilaajien mahdollisuuksia varmistaa viestintäverkkojensa ja palvelujensa käyttö suunnitellulla tavalla elinkeinotoiminnan tukena.

Tunnistamistietojen käsittelyoikeuksien selkeyttäminen poistaa tulkintaepäselvyyksiä. Uuden 13 a–13 j §:n mukainen tunnistamistietojen käsittelyoikeus väärinkäytöstapauksissa antaisi yhteisötilaajille aiempaa paremmat mahdollisuudet torjua viestintäverkkojensa ja -palvelujensa ohjeiden vastaisesti tapahtuvaa tai luvatonta käyttöä. Samoin kustannuksia aiheuttavien palvelujen luvatonta käyttöä voitaisiin tehokkaasti ehkäistä ja selvittää.

Esityksellä parannettaisiin yhteisötilaajien toimintamahdollisuuksia yritysalaisuuksien suojaamiseksi. Esitetty muutos on tarpeen teknologisen tai muun kehittämistyön sekä yrityksen liiketoiminnan kannalta keskeisten yrityssalaisuuksien tehokkaan suojan varmistamiseksi. Yhteisötilaaja saisi uusien 13 a–13 j §:n mukaan käsitellä tunnistamistietoja kun on perusteltua syytä epäillä jonkun lähettäneen tai antaneen oikeudetta pääsyn yrityssalaisuuksiin. Säännöksellä parannettaisiin tietopääoman omistajan yksinomaista oikeutta omaisuuteensa ja oikeutta hyödyntää omaisuuttaan taloudellisesti. Ehdotettu uudistus turvaisi myös aiempaa paremmin mahdollisuuden turvata esimerkiksi tuotekehitystyön jatkuminen tietovuodoista huolimatta, kun yhteisötilaaja voisi rajata olennaisesti tietovuodosta epäiltyjen piiriä.

Muutettaviksi esitetyt tietoturvaa koskevat säännökset mahdollistaisivat tietoturvatoimet myös lisäarvopalvelujen tai yhteisötilaajan viestintäverkkojen tai niihin liitettyjen palvelujen turvaamiseksi samalla, kun toimenpiteiden kattavuus tehtäisiin joustavammaksi ja saatettaisiin vastaamaan nykyisiä vaatimuksia.

Ehdotettu uusi sääntely, jonka mukaan teleyritykset voisivat luovuttaa tunnistamistietoja yhteisötilaajille tilastollista analyysiä varten, avaisi teleyrityksille uusia liiketoimintamahdollisuuksia. Esitys ei luo teleyrityksille tässä suhteessa suoria investointitarpeita, mutta sillä voidaan katsoa olevan epäsuoria kilpailuvaikutuksia. Teleyritykset kilpailevat keskenään raportointipalveluilla, joilla tuotetaan ja muokataan asiakkaille tietoja heidän puhelukäyttäytymisestään maksullisten palvelujen osalta. Kun ehdotus mahdollistaa tunnistamistietojen luovuttamisen täydellisenä asiakkaalle, saattaa se muuttaa kilpailutilannetta raportointipalveluiden osalta, mutta mahdollistaa myös uuden palvelun tarjoamisen.

Merkittävimmät esityksen taloudelliset vaikutukset kohdistuisivat yritysten toimintaedellytysten turvaamiseen. Teleyritysten, lisäarvopalveluja tarjoavien yritysten sekä yhteisötilaajien mahdollisuudet kehittää toimintaansa, torjua yritystietoon ja tietoverkkoihin kohdistuvaa rikollisuutta ja ylläpitää tietoturvaa paranevat.

Esitetyt yhteisötilaajien velvollisuudet tunnistamistietojen käsittelyoikeutta käytettäessä aiheuttaisivat niille yrityksille ja muille organisaatioille, jotka ryhtyvät käyttämään ehdotetun sääntelyn mukaisia oikeuksia, jonkin verran kustannuksia. Kustannukset aiheutuisivat henkilöstön koulutuksesta ja maksullisista valvontatoimenpiteistä sekä hallinnollisen työn lisääntymisestä huolehdittaessa ehdotettujen 13 a–13 j §:n mukaisista velvoitteista.

3.3 Vaikutukset viranomaisten toimintaan

Ehdotuksessa muutettaisiin Viestintäviraston ja tietosuojavaltuutetun tehtävänjakoa silloin, kun kyse on yhteisötilaajien tunnistamistietojen käsittelystä väärinkäytöstilanteissa, joita ovat viestintäverkon luvaton käyttö tai viestintäpalvelun ohjeen vastainen käyttö sekä yrityssalaisuuden oikeudeton paljastaminen.

Ehdotus ei lisäisi näiden valvontaelinten tehtäviä tavalla, jolla olisi välittömiä vaikutuksia valtiontalouteen. Kuitenkin tietosuojavaltuutetun toimistolle, jolla ei pienenä yksikkönä ole mahdollisuuksia sisäisin järjestelyin kohdentaa resursseja uuteen valvontatehtävään, ehdotuksen mukaisen valvonnan toteuttaminen

edellyttää kahden erityisasiantuntijan ja yhden toimistohenkilön ja näihin liittyvien lisämenojen, alustavasti arvioiden vuositasolla yhteensä 260 000 euron vuotuista määrärahalisäystä. Voimavarojen ja niistä aiheutuvien kustannusten täsmällistä arviota tehtäessä tulee kuulla asianomaisia ministeriöitä ja niitä, joita maksuvelvollisuus koskisi. Maksuvelvollisuuden tulee olla oikeassa suhteessa valvottavan kokoon ja toiminnan luonteeseen. Lisäresurssitarpeet voidaan ottaa huomioon asianomaisen ministeriön valmistelemalla, valtion maksuperustelain (150/1992) nojalla annettavalla asetuksella suoritteiden maksullisuudesta. Säännösten täsmentäminen antaisi Viestintäviraston ja tietosuojavaltuutetun työlle selkeämmät puitteet, mikä tehostaisi myös lain valvontaa ja sen tavoitteiden toteutumista.

Ehdotuksella edistettäisiin viranomaisten kansainvälistä yhteistyötä antamalla Viestintävirastolle oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja muissa valtioissa toimiville CERT-FI yksikköä vastaaville elimille, joiden tehtävänä on ennalta ehkäistä tai selvittää viestintäverkkoihin ja -palveluihin kohdistuvia tietoturvaloukkauksia. Koska tietoturvaan kohdistuvat uhat ovat tyypillisesti rajat ylittäviä, merkitsevät Viestintäviraston täsmennetyt toimintavaltuudet lisäedellytyksiä tietoturvan edistämiseksi muiden maiden organisaatioiden kanssa.

3.4 Yhteiskunnalliset vaikutukset

Täsmentämällä viestinnän eri osapuolten oikeuksia ja velvollisuuksia parannetaan erityisesti kuluttajien ja yritysten yleistä luottamusta sähköiseen viestintään ja tätä kautta sähköiseen liiketoiminta- ja asiointiympäristöön kokonaisuudessaan.

Nopea teknologinen kehitys ja verkottuneiden tietoteknisten välineiden laaja levinneisyys on samalla tuonut mukanaan myös uusia riskejä ja mahdollisuuksia lamauttaa yhteiskunnan keskeisiä toimintoja tietoverkkojen avulla. Näissä olosuhteissa tietoturvan merkitys ja sitä koskevan sääntelyn ajankohtaisuus vain korostuu.

Yritysten ja muiden yhteisötilaajien toimintamahdollisuudet paranisivat ehdotuksen myötä ja sääntely mahdollistaisi aiempaa paremmin yhteisötilaajien järjestelmien käytettävyydestä ja tietoturvasta huolehtimisen samalla, kun yksityisyyden suojaa koskevat lain alkuperäiset tavoitteet tulisivat täytetyiksi. Ehdotetut menettelylliset vaatimukset varmistaisivat viestintäverkkojen ja palvelujen käyttäjien yksityisyyden ja viestinnän luottamuksellisuuden. Yrityssalaisuuksien suojan parantaminen lisäisi yritysten toimintamahdollisuuksia ja edistää osaltaan taloudellista kehitystä ja hyvinvointia. Yritysten toimintamahdollisuuksien parantaminen kotimaassa edesauttaisi niiden toimintaa myös kansainvälisessä ympäristössä ja kilpailussa.

3.5 Tietoyhteiskuntavaikutukset

Ehdotettuihin yhteisötilaajan käsittelyoikeuksien edellytyksenä on velvollisuus huolehtia viestintäverkkojen tietoturvasta, yrityssalaisuuksien suojasta ja laatia viestintäverkkojen ja -palvelujen käytöstä sekä yrityssalaisuuksien käsittelystä ohjeet. Näiden velvollisuuksien voidaan arvioida parantavan pitkällä aikavälillä viestintäverkkojen käytön suunnittelua ja tietoturvariskeiltä suojautumista sekä yritysten toiminnan kannalta tärkeän tietoaineiston suojaamista sähköisessä toimintaympäristössä.

3.6 Vaikutukset yksilön asemaan

Ehdotetut yhteisötilaajien tunnistamistietojen käsittelyoikeuksien muutokset vaikuttavat kansalaisten luottamukselliseen viestintään siltä osin, kun yhteisötilaajien viestintäverkkojen ja palvelujen käyttäjät käyttävät yhteisötilaajan viestintämahdollisuuksia omaan viestintäänsä. Käsittelyoikeuksien rajaamisella vakaviin tapauksiin ja niihin liittyvillä menettelyillä on pyritty saamaan aikaan tasapaino viestintäverkkojen ja palvelujen käyttäjien ja yhteisötilaajien oikeutettujen intressien välillä.

Useat yhteisötilaajat ovat myös työnantajia, jolloin heidän tulee ottaa sähköiseen viestintään ja sen seurantaan liittyvät asiat yhteistoimintamenettelyssä käsiteltäviksi ja tiedottaa niistä työntekijöille.

Omaksutun ratkaisun voidaan arvioida mahdollistavan yksityisen viestinnän ja sähköisen

asioinnin ja yhteisötilaajien tarpeiden yhteensovittamisen siten että yhteisötilaajat voivat sallia viestintäverkkojensa käytön myös henkilökohtaisiin tarkoituksiin ilman että heidän tarvitsee tinkiä verkon turvallisuudesta.

Tietyissä tilanteissa käyttäjien viestinnän tunnistamistietoja voitaisiin tutkia, mutta missään tapauksessa viestien sisältö ei paljastu ulkopuolisille. Tunnistamistietojen käsittelyyn oikeuttavat tilanteet tulisivat työntekijöiden tietoon lain menettelysäännösten myötä.

Ehdotetuilla säännöksillä voidaan arvioida olevan myös myönteisiä vaikutuksia viestintäverkkojen ja palvelujen käyttäjien yksityisyyden kannalta, koska haittaa aiheuttavat toimenpiteet voivat usein vaarantaa verkkojen ja palveluiden toiminnan ohella myös käyttäjien yksityisyyden suojan toteutumisen.

4 Asian valmistelu

4.1 Valmisteluvaiheet ja -aineisto

Esitys on laadittu liikenne- ja viestintäministeriössä.

Sähköisen viestinnän tietosuojalain tultua voimaan vuonna 2004 sen vaikutusten arvioimiseksi perustettiin seurantaryhmä, jossa olivat edustettuina AKAVA ry, Elinkeinoelämän keskusliitto ry, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Fortum Oyj, Kuluttajavirasto, Keskuskauppakamari ry, liikenne- ja viestintäministeriö, sisäasiainministeriö, Suomen Ammattiliittojen Keskusjärjestö SAK ry, Suomen Suoramarkkinointiliitto ry SSML, Toimihenkilökeskusjärjestö STTK ry, Tekijänoikeuden tiedotus- ja valvontakeskus TTVK ry, Tietosuojavaltuutetun toimisto, työministeriö ja Viestintävirasto.

Seurantaryhmässä esiin tulleiden tarpeiden perusteella liikenne- ja viestintäministeriössä valmisteltiin keväällä 2006 luonnos hallituksen esitykseksi muun muassa yhteisötilaajien käsittelyoikeuksien laajentamiseksi. Luonnos hallituksen esitykseksi lähetettiin laajalle lausuntokierrokselle.

Lausunnoissa kiitettiin yleisesti lain täsmentämistä ja selkeyttämistä. Lausunnoissa kritisoitiin sitä, ettei lausuntokierroksella olevassa luonnoksessa ollut mukana vaikutusten arviointia eikä kansainvälistä vertailua. Vaikutusten arviointi valmistui lausuntokierroksen jälkeen. Lausunnot yksittäisiin pykälämuutoksiin olivat vaihtelevia. Niiden johdosta esitykseen tehtiin lausuntokierroksen jälkeen useita muutoksia.

Lausuntokierroksen jälkeen keskeisiltä ministeriöiltä saatiin tehtyihin muutoksiin näkemyksiä.

Liikenne- ja viestintäministeriö pyysi hallituksen esitysluonnoksesta myös oikeuskanslerin lausunnon sen selvittämiseksi, onko hallituksen esityksessä sellaisia ongelmia, jotka estäisivät esityksen antamisen eduskunnan ja sen perustuslakivaliokunnan arvioitavaksi. Oikeuskansleri esitti lausunnossa näkemyksenään, että esitysluonnoksessa tulisi arvioida kattavammin ja tarvittaessa täydentää luonnosta useiden perusoikeuskysymysten osalta. Oikeuskanslerin esittämien näkemysten pohjalta esitystä arvioitiin uudelleen.

Esityksen valmistelua jatkettiin liikenne- ja viestintäministeriön 3.10.2006 asettamassa työryhmässä, jonka tehtävänä oli laatia ehdotus sähköisen viestinnän tietosuojalain 13 §:n muuttamiseksi. Ehdotuksessa oli tarkasteltava yhteisötilaajan verkko- ja viestintäpalvelujen tunnistamistietojen käsittelyä 1) luvattoman käytön ja 2) yrityssalaisuuksien paljastamisen tilanteissa. Työryhmän puheenjohtajaksi määrättiin ylijohtaja liikenne- ja viestintäministeriöstä ja jäseniksi edustajat liikenne- ja viestintäministeriöstä, oikeusministeriöstä, sisäasiainministeriöstä, työministeriöstä, valtiovarainministeriöstä sekä työmarkkinakeskusjärjestöistä.

Esitysluonnoksen tunnistamistietojen käsittelyä koskeviin säännöksin on työryhmän työn tuloksena lisätty useita merkittäviä täsmennyksiä, jotka kaikki tarkentavat ja asettavat rajoja sekä 13 a–13 j §:ssä ehdotetulle tunnistamistietojen käsittelylle.

Ehdotuksen 13 a–13 j §, niiden yksityiskohtaiset perustelut ja soveltuvin osin yleisperustelut ja säätämisjärjestysperustelut on valmisteltu työryhmässä, jossa olivat edustettuina asian kannalta keskeiset ministeriöt ja työmarkkinakeskusjärjestöt.

Esitykseen laadittiin myös kokonaan uusi kansainvälinen vertailu.

4.2 Lausunnot ja jatkovalmistelu

Luonnos hallituksen esitykseksi lähetettiin lausuttavaksi kaikille ministeriöille ja usealle sadalle eri yhteisölle. Tämän lisäksi hallituksen esitysluonnos saatettiin avoimesti liikenne- ja viestintäministeriön kotisivuille, jotta kaikilla muillakin kuin edellä mainituilla tahoilla oli mahdollisuus lausua asiasta.

Lausunnoissa kiitettiin melko yleisesti lain täsmentämistä. Useimmat yhteisötilaajat pitivät yhteisötilaajien tunnistamistietojen käsittelyoikeuksia koskevaa sääntelyä tervetulleena. Tietoturvatoimenpiteitä koskevan 20 §:n uudistusta lausunnoissa pidettiin erittäin tarpeellisena.

Eräät lausujat pitivät ehdotettua yhteisötilaajien tunnistamistietojen käsittelyoikeutta ongelmallisena.

Esitysluonnoksen laskuerittelyä koskevaa 24 §:ää pidettiin pääosin tervetulleena, mutta etenkin teleyritykset katsoivat säännöksen vaativan lisäselvitystä.

Lausunnoissa esitetyn johdosta esitykseen tehtiin useita tarkennuksia ja laskuerittelysäännös erotettiin valmisteltavaksi erikseen.

YKSITYISKOHTAISET PERUSTELUT

1 Lakiehdotusten perustelut

1.1 Sähköisen viestinnän tietosuojalaki

9 §. *Tunnistamistietojen käsittely palvelujen toteuttamiseksi ja käyttämiseksi.* Ehdotuksella muutettaisiin 9 §:n 1 momenttia siten, että nykyistä selkeämmin kävisi ilmi, että viittauksella tietoturvasta huolehtimiseksi tarkoitetaan nimenomaan tässä laissa jäljempänä säädettyjä tietoturvaa koskevia säännöksiä.

On huomattava, että lain 8 §:ssä säädetään erikseen viestinnän osapuolen oikeuksista ja että sekä luonnollinen henkilö että oikeushenkilö voivat olla myös viestinnän osapuolena. Muilla kuin viestinnän osapuolilla on säännöksen mukaan oikeus käsitellä tunnistamistietoja palvelujen toteuttamiseksi ja käyttämiseksi sekä tietoturvasta huolehtimiseksi. Kyse on esimerkiksi puheluiden, sähköpostiviestien tai tekstiviestien siirtämisestä lähettäjältä vastaanottajalle taikka haittaohjelmien poistamisesta viesteistä lain 20 §:n edellytysten täyttyä. Tällöin tunnistamistietojen käsittelijä toimii viestinnässä sivullisen roolissa. Silloin, kun joku käsittelee viestejä ja tunnistamistietoja sivullisena, voi käsittely tapahtua vain lain 3 luvun mukaisten käsittelyoikeuksien perusteella.

Lain 9 §:n 1 momentin mukaisia tietoturvaa koskevia säännöksiä ovat lain 5 luvun säännökset. Lain 20 §:ssä on säädetty tyhjentävästi ne tilanteet, joissa tunnistamistietoja on oikeus käsitellä tietoturvasta huolehtimiseksi ja niistä toimenpiteistä, joita näissä tilanteissa on oikeus tehdä. Ehdotetun muutoksen on tarkoitus olla lähinnä informatiivinen.

Ehdotuksella lisättäisiin 9 §:n 2 momenttiin tunnistamistietojen käsittelyyn oikeutettujen joukkoon myös tilaajana olevan oikeushenkilön palveluksessa oleva sekä sen lukuun toimiva luonnollinen henkilö. Lisäys on tarpeen, jotta uuden 12 a §:n mukainen käsittelyoikeus tilastollista analyysiä varten voisi toteutua myös sellaisille tahoille, jotka käsittelevät esimerkiksi matkapuhelinliittymien tunnistamistietoja tilastollista analyysiä varten. Ehdotuksella muutettaisiin myös 2 momentin pykäläviittaukset kohdistumaan koko 3 luvun käsittelysäännöksiin. Muutoksen ei ole tarkoitus muuttaa vallitsevaa oikeustilaa.

12 §. *Käsittely teknistä kehittämistä varten.* Ehdotuksella muutetaan säännöksen 1 momenttia lähinnä kirjoitusteknisesti. Samalla ehdotetaan muutettavaksi 2 ja 3 momentin paikkaa. Ehdotetulla 2 momentilla pyrittäisiin selkeyttämään yhteisötilaajan oikeutta käsitellä tunnistamistietoja teknistä kehittämistä varten. Lisäksi ehdotetaan 3 momenttiin yhteisötilaajalle samankaltaista informointivelvollisuutta käsittelystä kuin teleyrityksillä ja lisäarvopalvelun tarjoajilla on jo voimassa olevan lain nojalla.

Lain 12 §:n 1 momentissa viitataan pelkästään palvelujen tekniseen kehittämiseen, kun luvun muissa säännöksissä eritellään palvelut verkkopalveluun, viestintäpalveluun ja lisäarvopalveluun. Ehdotuksella muutettaisiin 12

§:n 1 momentin säännös vastaamaan muita luvun säännöksiä.

Ehdotetulla 2 momentilla selkeytettäisiin yhteisötilaajan oikeutta käsitellä tunnistamistietoja teknistä kehittämistä varten. Yhteisötilaajalla olisi näin ollen samat oikeudet käsitellä omassa viestintäverkossaan olevia tunnistamistietoja teknistä kehittämistä varten kuin teleyrityksellä ja lisäarvopalvelun tarjoajallakin.

Tunnistamistietojen käsittely teknistä kehittämistä varten on tärkeää, jotta viestintäverkkoja ja -palveluja voitaisiin kehittää ja luoda uusia palveluja markkinoille. Teknisellä kehittämisellä tarkoitetaan esimerkiksi teknisen suorituskyvyn tai käytettävyyden parantamista. Viestintäverkkoon liitetyllä omalla palvelulla tarkoitetaan yhteisötilaajan palvelua, jonka se itse tuottaa omille käyttäjilleen omassa viestintäverkossaan. Kyse ei ole esimerkiksi sellaisesta tietoyhteiskunnan palvelusta, jonka jokin muu taho tuottaa yhteisötilaajalle, kuten esimerkiksi luettelopalvelun tarjoajan numerohakupalvelu, jonka yhteisötilaaja on luettelopalvelun tarjoajalta tilannut käyttäjiensä käytettäväksi.

Ehdotettua tunnistamistietojen käsittelyä palvelujen teknistä kehittämistä varten koskisivat edelleen myös 8 §:n 3 momentin ja 9 §:n yleiset edellytykset. Lain 8 §:n 3 momentin säännöksen mukaan muun muassa 12 §:ssä tarkoitettu käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa ja sillä ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Tunnistamistietoja on sallittua luovuttaa ainoastaan niille tahoille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa. Käsittelyn jälkeen viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä.

Ehdotetun 9 §:n 2 momentin mukaan tunnistamistietoja saa käsitellä vain teleyrityksen, lisäarvopalvelun tarjoajan, yhteisötilaajan ja tilaajana olevan oikeushenkilön palveluksessa oleva sekä näiden lukuun toimiva luonnollinen henkilö, jonka tehtävänä on käsitellä tietoja erikseen säädettyjen tarkoitusten toteuttamiseksi.

Voimassa olevan pykälän 2 momentin mukaan teleyritys ja lisäarvopalvelun tarjoaja ovat olleet velvollisia informoimaan 12 §:n mukaisesta tunnistamistietojen käsittelystä tekniseen kehittämiseen tilaajaa tai käyttäjää. Nyt säännöksen 3 momenttiin ehdotetaan lisättäväksi, että myös yhteisötilaaja olisi teleyrityksen ja lisäarvopalvelun tarjoajan tapaan velvollinen ennen käsittelyn aloittamista ilmoittamaan, millaisia tunnistamistietoja käsitellään ja kuinka kauan niiden käsittely kestää. Yhteisötilaajan olisi näin ollen ilmoitettava käyttäjälle, millaisia tunnistamistietoja käsitellään ja kuinka kauan niiden käsittely kestää. Kuten voimassa olevan lain 12 §:n hallituksen esityksen yksityiskohtaisissa perusteluissa on kuvattu, teleyritysten ja lisäarvopalvelujen tarjoajien antama ilmoitus voidaan antaa esimerkiksi liittymäsopimuksessa tai teleyrityksen tai lisäarvopalvelun tarjoajan kotisivuilla. Samalla tavoin yhteisötilaajan ilmoitus voisi olla kertaluontoinen ja se voisi koskea ajallisesti pitkääkin ajanjaksoa. Poikkeuksellisista ja merkityksellisistä toimista voitaisiin antaa erillinen ilmoitus.

12 a §. *Käsittely tilastollista analyysiä varten.* Ehdotettu uusi säännös antaisi teleyritykselle, lisäarvopalvelun tarjoajalle ja yhteisötilaajalle tunnistamistietojen käsittelyoikeuden automaattisen tietojenkäsittelyn avulla toteutettavaa tilastollista analyysiä varten. Samoin tilaajana oleva oikeushenkilö saisi käsitellä liittymänsä ja päätelaitteensa tunnistamistietoja tilastollista analyysiä varten.

Voimassa olevan lain mukaan tilastoja on voinut kerätä niin sanotuista anonyymeistä tiedoista, joista ei ole voinut tunnistaa tilaajaa tai käyttäjää. Ehdotetun muutoksen jälkeenkin tämä olisi mahdollista. Kuka tahansa voi tehdä anonyymeistä tiedoista tilaston tai muutoin käsitellä anonyymejä tietoja vapaasti. Ehdotettu säännös antaisi sen sijaan oikeuden käsitellä tilastollista analyysiä varten myös sellaisia tietoja, joista tilaaja tai käyttäjä voidaan tunnistaa. Tosin lopputuloksesta eli tilastollisesta analyysistä ei enää luonnollista henkilöä saisi tunnistaa. Tilastollinen analyysi olisi säännöksen mukaan tuotettava automaattisen tietojenkäsittelyn avulla.

Tilastollisen analyysin tarkoituksena ei ole itse tilaston tuottaminen, vaan jonkin muun asian selvittäminen, kuten esimerkiksi hinnoittelumuutoksen vaikutusta liikevaihtoon.

Viestintäpalvelujen tuottaminen ja käyttö vaatii runsaasti teknistä kehitystyötä, johon

lain 12 § antaa mahdollisuuden. Käytännössä on tullut esille, että asianmukaiseen kehitystyöhön sisältyy piirteitä, jotka eivät ole luonteeltaan yksinomaan teknisiä, mutta täysin välttämättömiä toiminnan kehittämisen kannalta. Kyse voi olla taloudellisesta kehittämisestä, kuten esimerkiksi puhelukulujen taloudellisesta optimoimisesta.

Teleyritykset eivät ole joko lain tai sen tulkintojen takia luovuttaneet tilaajille tunnistamistietoja, joiden perusteella yritys tai yhteisö olisi voinut esimerkiksi optimoida käytössään olevien kiinteiden puhelinten ja kännyköiden välistä puhelinliikennettä mahdollisimman kustannustehokkaalla tavalla. Erityisesti asia on ollut ongelmallinen tilanteessa, jossa yritys tai yhteisö on kokonsa tai kansainvälisen toimintansa takia tilannut viestintäpalvelut usealta eri teleyritykseltä. Esimerkiksi suurella yhtiöllä, joka tilaajan ominaisuudessa maksaa käyttäjiensä puhelinlaskut, on huomattava taloudellinen intressi pyrkiä minimoimaan syntyvät kustannukset. Pelkkien lain 24 §:n mukaisten laskuerittelyjen läpikäyminen tilaston muodostamiseksi on jo muutamien kymmenienkin henkilöiden organisaatioissa haastava tehtävä. Toisaalta teleyritysten tuottamat raportit saattavat vaihdella teleyrityskohtaisesti huomattavasti, jolloin eri raporteista muodostettavan yhteenvedon tuottaminen voi käytännössä olla mahdotonta. Tilaajalla on erityinen tarve saada esimerkiksi tarjouspyyntötilanteessa kilpailuttaessaan teleyrityksiä tunnistamistiedot itselleen, jotta se voi huomioida, kuinka paljon puhelinliikenteestä on esimerkiksi yhtiön sisäistä matkapuhelinliikennettä.

Yrityksen tai muun yhteisön puheviestintäverkko voi myös muodostua yhdeltä tai useammalta teleyritykseltä ostetuista palveluista, usein eri teleyrityksiltä ostetuista kiinteän verkon puhelinpalveluista sekä itse omassa vaihdeverkossa toteutetuista sisäpuheluista. Yrityksellä tai muulla yhteisöllä saattaa olla usein tarve kehittää tätä kokonaisuutena myös yli maarajojen, jolloin osapuolien lukumäärä moninkertaistuu. Kehittämistä varten mikään edellä mainittu taho ei yksinään pysty tuottamaan kaikkia tarvittavia raportteja, eivätkä raporttien tiedot olisi järkevästi yhdisteltävissä. Tilastollisella analyysillä toimijoille annettaisiin mahdollisuus kehittää asianmukaisesti palveluitaan ja omaa toimintaansa muutoinkin kuin yksinomaan teknisesti.

On oletettavaa, että tulevaisuudessa yritys tai yhteisö voi hankkia teleyritysten kilpailuttamisen kannalta välttämättömät puheluiden suuntautumistiedot kootusti myös omista päätelaitteistaan. Ehdotuksella pyritään siihen, että palvelun tarjoajat, tilaajat ja yhteisötilaajat voisivat luottamuksellisen viestin suojaa vaarantamatta saattaa palvelut ja toiminnot vastaamaan yhä paremmin muuttuvan todellisuuden vaatimuksia.

Ehdotetun 12 a §:n 1 momentin mukaan teleyritykselle ja lisäarvopalvelun tarjoajalle annettaisiin oikeus käsitellä verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun tunnistamistietoja ja yhteisötilaajalle annettaisiin oikeus käsitellä sen omassa viestintäverkossa tai siihen liitetyssä omassa palvelussa olevia tunnistamistietoja automaattisen tietojenkäsittelyn avulla tilastollista analyysiä varten. Koska esimerkiksi matkapuhelinliittymien tunnistamistiedot eivät ole yhteisötilaajien käytettävissä niiden omissa viestintäverkoissa, ehdotetaan 12 a §:n 2 momentissa myös tilaajana olevalle oikeushenkilölle liittymänsä tai päätelaitteensa tunnistamistietojen käsittelyoikeutta tilastollista analyysiä varten 1 momentissa säädetyin edellytyksin. Kyse on niistä liittymistä ja päätelaitteista, joita tilaajana oleva oikeushenkilö tarjoaa käyttäjilleen käytettäväksi.

Teleyritys voi ehdotetun säännöksen myötä luovuttaa matkapuhelinliittymien tunnistamistietoja tilaajana olevalle oikeushenkilölle tilastollista analyysiä varten. Yritys tai muu yhteisö voisi saada teleyrityksiltä tarvittavat puhelinsoittojen suuntautumisvertailut ja siten se voisi kilpailuttaa teleyritysten viestintäpalvelut keskenään.

Oli kyse yrityksen tai muun yhteisön toimintojen taloudellisesta tai muusta kehittämisestä taikka teleyrityksen asiakassegmentoinnista, kaikissa tapauksissa tunnistamistietojen käsittely tapahtuisi teknisesti tilastollisen analyysin muodostamista varten, minkä jälkeen tunnistamistiedoista ei voitaisi luonnollista henkilöä tunnistaa.

Ehdotetun säännöksen mukaan tunnistamistietoja saisi käsitellä ainoastaan tilastojen muodostamiseksi eikä lainkaan yksittäisen käyttäjän yksittäisten puhelujen tarkistamiseksi. Säännöksen mukaisessa tunnistamistietojen

käsittelyssä on otettava myös huomioon lain 8 §:n 3 momentissa asetetut rajoitukset, joiden mukaan tunnistamistietojen käsittelyllä ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Tunnistamistietojen käsittelyn tilastointia varten tulee olla asiallisesti perusteltua.

On myös huomattava, että joissakin tilanteissa yritys, joka toimii myös teleyrityksenä, voi toimia myös yhteisötilaajan lukuun, jolloin kyse on alihankkijan yhteisötilaajalle tuottamasta tiedosta. Näin on esimerkiksi silloin, kun yritys ylläpitää yhteisötilaajan omia järjestelmiä.

Tunnistamistietojen käsittelyä tilastotarkoitusta varten rajaavat myös säännöksessä luetellut edellytykset. Ehdotetun 12 a §:n 1 momentin mukaan käsittely on mahdollista, jos tilastollista analyysiä ei voida muuten tuottaa ilman kohtuutonta vaivaa ja analyysistä ei voida luonnollista henkilöä eli yksittäistä tilaajaa tai käyttäjää tunnistaa. Kulloisessakin tilanteessa olisi aina harkittava tarkoin, voidaanko tilastotarve saavuttaa muilla käytettävissä olevilla keinoilla, esimerkiksi jo anonymisoituja tietoja käyttämällä. Tilastollisesta analyysistä ei myöskään saa tunnistaa yksittäistä tilaajaa tai käyttäjää. Tilastollista analyysiä ei voida siten tuottaa, jos kyse on esimerkiksi yhdestä käyttäjästä ja hänen tunnistamistiedoistaan tai niin pienestä joukosta käyttäjiä, ettei analyysia voida tehdä siten, ettei siitä voida tunnistaa luonnollista henkilöä.

13 §. *Teleyrityksen ja lisäarvopalvelun tarjoajan käsittelyoikeus väärinkäytöstapauksissa*. Ehdotetussa 13 §:ssä esitetään säädettäväksi teleyrityksen ja lisäarvopalvelun tarjoajan tunnistamistietojen käsittelyoikeuksista.

Ehdotetun 13 §:n 1 momenttiin ei enää sisältyisi rajausta yksittäiseen väärinkäytökseen. Säännöksessä annettavaksi ehdotetun käsittelyoikeuden käyttäminen ei edellyttäisi epäilyä tietystä yksittäisestä väärinkäytöksestä. Käsittely voitaisiin kohdistaa laajempana kuin aiemmin kaikissa säännöksessä mainituissa tapauksissa. Kyse ei kuitenkaan olisi viestiliikenteen seurannasta siinä mielessä, että yksittäisten viestinnän osapuolten viestintää saisi seurata, vaan väärinkäytöksiin viittaavien poikkeamien havaitsemisesta.

Ehdotetussa 2 momentissa lain noudattamista valvovalle Viestintävirastolle ehdotetaan oikeutta antaa teknisiä määräyksiä. Viestintävirasto antaisi määräyksiä teleyrityksille ja lisäarvopalvelun tarjoajille. Määräysten antaminen on välttämätöntä nopeasti muuttuvan teknisen ympäristön vaatiman tarvittavan jouston mahdollistamiseksi ja tarvittavista teknisistä yksityiskohdista säätämiseksi. Viestintäviraston määräyksenantovaltuus ei koskisi valtionhallinnon tarjoamia tietoyhteiskunnan palveluita.

13 a §. *Yhteisötilaajan käsittelyoikeus väärinkäytöstapauksissa.* Ehdotetun 13 a §:n 1 momentin mukaan yhteisötilaajalla on oikeus käsitellä tunnistamistietoja maksullisen tietoyhteiskunnan palvelun tai viestintäverkon luvattoman käytön, viestintäpalvelun ohjeen vastaisen käytön taikka yrityssalaisuuksien paljastamisen selvittämiseksi siten kuin 13 b–13 j §:ssä säädetään.

Ehdotettu tunnistamistietojen käsittelyoikeus liittyy yhteisötilaajien viestintäverkkojen ja viestintäpalvelujen käytön turvaamiseen sekä yrityssalaisuuksien oikeudettoman paljastamisen selvittämiseen. Yhteisötilaajat voisivat ehdotetun säännöksen nojalla käsitellä tunnistamistietoja, kun kyse on maksullisen tietoyhteiskunnan palvelun tai viestintäverkon luvattomasta käytöstä taikka viestintäpalvelun ohjeen vastaisesta luvattomasta käytöstä sekä epäiltäessä yrityssalaisuuksien oikeudetonta paljastamista.

Sähköisen viestinnän tietosuojalain 8 §:n 3 momentin mukaan tunnistamistietojen käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa ja se on toteutettava luottamuksellisen viestin ja yksityisyyden suojaa tarpeettomasti vaarantamatta. Käsittelyn jälkeen viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä.

Lain 8 §:n 3 momentista johtuu, että väärinkäytökset on ensisijaisesti pyrittävä selvittämään muiden kuin luottamuksellista viestintää koskevien tunnistamistietojen avulla. Jos tunnistamistietojen käsittely on välttämätöntä väärinkäytöksen selvittämiseksi, on käsiteltäväksi tulevien tunnistamistietojen piiri rajattava aina tapauskohtaisesti käytettävissä olevien muiden tietojen perusteella. Käsiteltäväksi voitaisiin välttämättömyysvaatimuksen vuoksi tällöinkin ottaa vain lähinnä käyttäjän lähet-

tämien eikä tämän vastaanottamien viestien tunnistamistietoja.

Pykälässä ehdotetun tunnistamistietojen käsittelyoikeuden yleisten ja erityisten edellytysten ja lain 8 § 3 momentin välttämättömyysedellytyksen vuoksi yhteisötilaaja ei voisi seurata tavanomaisiin viesteihin liittyviä tunnistamistietoja. Esimerkiksi työnantajaasemassa oleva yhteisötilaaja ei voisi seurata viestintäverkon tai viestintäpalvelujen käyttöä työajan seuraamiseksi eikä sen selvittämiseksi, onko käyttäjä ollut yhteydessä henkilöstön edustajaan, työsuojeluviranomaisiin tai työterveyshuoltoon. Ajallisesti käsiteltäväksi voitaisiin ottaa vain kulloinkin käsillä olevan tapauksen selvittämisen kannalta välttämättömät tunnistamistiedot eikä säännös oikeuttaisi käsittelemään tunnistamistietoja tätä laajemmin.

Ehdotetun säännöksen mukaisia yhteisötilaajan viestintäpalveluja ja tietoyhteiskunnan palveluja olisivat sen omaan viestintäverkkoon liitetyt palvelut sekä sellaiset palvelut, joita käytetään yhteisötilaajan viestintäverkon kautta, mutta jotka ovat luonteeltaan tietoyhteiskunnan palveluja ja joiden käytön yhteisötilaaja maksaa.

Tietoyhteiskunnan palvelujen tarjoamisesta annetun lain (458/2002) 2 §:n mukaan tietoyhteiskunnan palvelulla tarkoitetaan palvelua, joka toimitetaan ilman, että osapuolet ovat yhtä aikaa läsnä, sähköisesti, palvelun vastaanottajan henkilökohtaisesta pyynnöstä tapahtuvana tiedonsiirtona ja tavallisesti vastiketta vastaan.

Esimerkkinä maksullisen tietoyhteiskunnan palvelun luvattomasta käytöstä voisi olla se, että yrityksen henkilökunnan koon mukaan hinnoiteltua palvelua jaettaisiin luvatta ulkopuolisten käyttöön. Tällöin yritys joutuisi vastaamaan hankkimansa käyttöoikeuden ylittävästä käytöstä.

Viestintäverkon luvatonta käyttöä tai viestintäpalvelun ohjeen vastaista käyttöä olisi sellainen toiminta, jonka yhteisötilaaja on määritellyt luvattomaksi 13 b §:n 3 momentissa tarkoitetussa ohjeessa.

Yrityssalaisuuksien oikeudettoman paljastamisen selvittämisessä ovat käytettävissä tietohallinnolliset keinot, kuten käyttäjätietolokien tarkastaminen, pääsyä rajoittaviin järjestelmiin kirjautuvien tietojen tarkastaminen sekä järjestelmien teknisessä ylläpidossa kerätyt tiedot. Näistä tiedoista käy ilmi, kuka on tallentanut mitäkin tietoja, missä muodossa, koska ja mille tallenteelle, kuten kovalevylle tai siirrettävälle tallenteelle. Siirrettäviä tallenteita ovat esimerkiksi muistitikut ja cd-levyt. Myös aineiston muuta käsittelyä, kuten tulostamista koskevat tiedot, voidaan tallentaa. Näiden tietojen käsittelylle sähköisen viestinnän tietosuojalaissa ei aseteta rajoituksia. Toisaalta näiden tietojen avulla pystytään vain poikkeuksellisesti selvittämään yrityssalaisuuden paljastaminen kokonaisuudessaan.

Työnantaja voi suojata yrityssalaisuuksia myös muilla tietoturvallisuustoimenpiteillä. Esimerkkinä voidaan mainita, että työnantajat käyttävät myös työntekijän kanssa tehtäviä salassapitosopimuksia keinoina yrityssalaisuuksien suojaamisessa. Työnantaja voi myös turvallisuusselvityksistä annetun lain (177/2002) mukaan hankkia selvityksen työntekijän luotettavuudesta, milloin suojattavana on huomattavan arvokas liike- tai ammattisalaisuus tai muu tähän rinnastettava erittäin merkittävä yksityinen etu.

Pykälässä tarkoitettu yrityssalaisuuden käsite vastaisi rikoslain 30 luvun 11 §:n yrityssalaisuuden määritelmää. Rikoslain 30 luvun 11 §:n yrityssalaisuuden määritelmän mukaan yrityssalaisuudella tarkoitetaan liike- tai ammattisalaisuutta, taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle.

Rikoslaissa määritelty yrityssalaisuus on siten jossain määrin laajempi kuin viranomaisten toiminnan julkisuudesta annetun lain (621/1999) elinkeinotoiminnan intressien suojaamiseksi säädetyn salassapitosäännöksen (24 §:n 1 momentin 20 kohta) soveltamisala, jonka piiriin eivät esimerkiksi kuulu elinkeinonharjoittajan velvollisuuksia ja niiden hoitamista koskevat tiedot. Käsite kattaa sellaisetkin teknologista ja muuta kehittämistyötä koskevat tiedot, joissa ei vielä ole kysymys esimerkiksi patentoitavista tuotteista. Yrityssalaisuuden käsitteen piiriin kuuluvat siten myös sellaiset tiedot, jotka viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 21 kohdan mukaan ovat salassa pidettäviä.

Yrityssalaisuuden käsite on katsottu esitystä valmisteltaessa asianmukaisimmaksi käsitteeksi, koska tähän käsitteeseen liittyy kiinteästi elinkeinonharjoittajan oma salassapitotahto ja koska säännökset vaikuttavat yksityisten osapuolten välillä.

Tunnistamistietojen käsittely 13 a–13 j §:n ja 8 §:n käsittelysääntöjen vastaisesti saattaa täyttää rikoslain 38 luvun 3 §:ssä ja 4 §:ssä säädetyn viestintäsalaisuuden loukkaamisen tai törkeän viestintäsalaisuuden loukkaamisen tunnusmerkistön. Tunnistamistietojen käsittelyn asianmukaisuuden takaavien 13 b–13 c §:ssä tarkoitettujen ennakollisten velvoitteiden laiminlyönti täyttäisi lain 42 §:n 2 momentin 5 kohdassa tarkoitetun sähköisen viestinnän tietosuojarikkomuksen tunnusmerkistön. Ehdotetulla 42 §:n 2 momentin uudella 9 kohdalla säädettäisiin rangaistavaksi sähköisen viestinnän tietosuojarikkomuksena tunnistamistietojen käsittelyn lainmukaisuuden takaavien jälkikäteisten velvoitteiden laiminlyönti.

Ehdotetun 2 momentin mukaan säännöksessä tarkoitetusta viestintäverkon luvattomasta käytöstä tai viestintäpalvelun ohjeen vastaisesta käytöstä olisi kyse, jos joku asentaa yhteisötilaajan viestintäverkkoon sen käytöstä annettujen ohjeiden vastaisesti laitteita, ohjelmia tai palveluita tai käyttää muuten näihin rinnastuvalla tavalla viestintäverkkoa tai viestintäpalveluita käytöstä laadittujen 13 b §:ssä tarkoitettujen ohjeiden vastaisesti.

Ehdotetussa 3 momentissa rajataan kiinteän ja matkapuhelinverkon puhelinpalvelujen tunnistamistiedot väärinkäytössäännöksien ulkopuolelle. Tällöin yhteisötilaaja ei saisi käsitellä puheluihin, tekstiviesteihin tai muihin vastaaviin viesteihin liittyviä tietoja. Lain määritelmän mukaan viestillä tarkoitetaan joko osapuolten välillä tai vapaasti valikoituville vastaanottajille välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, puheviestiä ja muuta vastaavaa sanomaa (HE 125/2003 vp, s. 45–46). Tilaajan oikeudesta saada puhelupalvelulaskun erittely on säädetty erikseen.

13 b §. *Yhteisötilaajan huolehtimisvelvollisuus väärinkäytöstapauksissa.* Ehdotettuun 13 b §:n 1 momenttiin otettaisiin säännökset niistä ennakollisista edellytyksistä, joiden rajoissa yhteisötilaaja voisi selvittää maksullisen tietoyhteiskunnan palvelun tai viestintäverkon luvatonta käyttöä ja viestintäpalvelun ohjeen vastaista käyttöä.

Ehdotetun sääntelyn mukaan ensisijaisena keinona viestintäverkon ja viestintäpalvelun käytön asianmukaisuuden turvaamisessa olisivat tietoturvasta huolehtiminen sekä verkkojen ja palvelujen käyttäjille annetut ohjeet ja niiden noudattamisen automaattisesti tapahtuva seuranta.

Ehdotetussa 1 momentissa säädettäisiin yhteisötilaajan huolehtimisvelvollisuudesta ennen tunnistamistietojen käsittelyn aloittamista tietoyhteiskunnan palvelun tai viestintäverkon luvattoman käytön taikka viestintäpalvelun ohjeen vastaisen käytön ehkäisemiseksi. Momentin 1 kohdan mukaisena tunnistamistietojen käsittelyn edellytyksenä olisi, että yhteisötilaaja on rajoittanut pääsyä viestintäverkkoonsa ja viestintäpalveluunsa ja niiden käyttöön sekä ryhtynyt muihin toimenpiteisiin viestintäverkkonsa ja viestintäpalvelunsa käytön suojaamiseksi asianmukaisin tietoturvallisuustoimenpitein.

Yhteisötilaajan on tullut ennalta käsin asianmukaisesti ryhtyä käytettävissä olevin keinoin toimenpiteisiin sen estämiseksi, että viestintäverkkoa tai siihen liitettyjä palveluja käyttäisivät ulkopuoliset tahot tai sellaiset yhteisötilaajan palveluksessa olevat, joiden käyttöön niitä ei ole osoitettu taikka viestintäpalveluja käytettäisiin käytöstä annettujen ohjeiden vastaisesti. Samoin yhteisötilaajan tulee huolehtia, että tietoturvallisuuden taso on riittävä. Jos verkkoa tai palveluita asianmukaisesta käyttäjähallinnosta ja muista tietoturvatoimista huolimatta käytetään luvatta, olisi yhteisötilaajalla oikeus ryhtyä tunnistamistietojen käsittelyyn asian selvittämiseksi.

Ehdotetun 1 momentin 2 kohdan mukaan yhteisötilaajan on määriteltävä, minkälaisia viestejä sen viestintäverkon kautta saa välittää ja hakea, sekä miten sen viestintäverkkoa ja viestintäpalvelua saa muutoin käyttää ja minkälaisiin kohdeosoitteisiin viestintää ei saa harjoittaa. Tunnistamistietojen käsittelyn salliminen ehdotetulla tavalla edellyttää, että viestintäverkon tai viestintäpalvelun käyttäjällä on tieto siitä, miten yhteisötilaajan verkkoa saa käyttää. Noudattamalla näitä vaatimuksia verkon käyttäjä voi välttyä siltä, että hänen viestintäänsä koskevat tunnistamistiedot tulisivat yhteisötilaajan tietoon.

Ehdotettuun 13 b §:n 2 momenttiin otettaisiin säännökset niistä ennakollisista toimista, joihin yhteisötilaajan on ryhdyttävä ennen kuin se ryhtyy käsittelemään tunnistamistietoja yrityssalaisuuksien paljastamisen ehkäisemiseksi.

Ehdotetun sääntelyn mukaan ensisijaisina keinoina yrityssalaisuuksien luottamuksellisuuden turvaamisessa olisivat tietoturvasta huolehtiminen sekä verkkojen käyttäjille annetut ohjeet ja niiden noudattamisen automaattisesti tapahtuva seuranta.

Ehdotetun 2 momentin 1 kohdassa edellytetään, että yrityssalaisuudet olisi tosiasiallisesti suojattava yrityssalaisuuden käsittelyn kannalta ulkopuolisilta tahoilta. Yhteisötilaajan on ennen tunnistamistietojen käsittelyn aloittamista tullut rajoittaa pääsyä keskeisiin yrityssalaisuuksiin ja ryhtyä muihin toimenpiteisiin tietojen suojaamiseksi asianmukaisin tietoturvallisuustoimenpitein. Käytännössä tämä tarkoittaa sitä, että organisaatiossa vain tiettyjä tehtäviä hoitavat käyttäjät pääsevät yrityssalaisuuksiin käsiksi. Pääsyä voidaan käytännössä rajoittaa muun muassa tietohallinnollisin toimenpitein, kuten käyttäjätunnuksin ja salasanoin tai muuten käyttäjäoikeuksia hallinnoimalla.

Ehdotetun 2 momentin 2 kohdan mukaan yhteisötilaajan on määriteltävä, miten yrityssalaisuuksia saa siirtää, luovuttaa tai muutoin käsitellä ja minkälaisiin kohdeosoitteisiin yrityssalaisuuksia käsittelemään oikeutetut henkilöt eivät ole oikeutettuja lähettämään viestejä. Yrityssalaisuutena suojattavan tiedon kanssa tekemisiin joutuvien olisi miellettävä tieto salaiseksi, mikä ilmenisi rajoitetusta pääsystä ja erityisistä tietojen suojaamistoimista sekä käsittelysäännöistä. Jos yhteisötilaaja haluaa kieltää liikennöinnin kokonaan tietyn tyyppisiin kohdeosoitteisiin, myös se on määriteltävä ohjeessa.

Ehdotetun 3 momentin mukaisena edellytyksenä on, että yhteisötilaaja on laatinut kirjallisen ohjeen, jossa se on määritellyt, miten sen viestintäverkkoa ja -palveluita saa käyttää. On selvää, että käyttäjälle annetuissa ohjeissa on oltava riittävän tarkka informaatio viestintäverkon käytölle asetetuista rajoituksista. Jos yhteisötilaaja haluaa rajoittaa liikennöintiä tai estää liikennöinnin kokonaan tietyn tyyppisiin kohdeosoitteisiin, myös se on määriteltävä ohjeessa. Kohdeosoitteet voitaisiin määritellä kohtuullisen yleisellä tasolla. Määrittelystä tulisi kuitenkin olla selkeästi ymmärrettävissä, mikä on väärinkäyttöä.

13 c §. *Yhteisötilaajan suunnittelu- ja yhteistoimintavelvoite väärinkäytöstapauksissa.* Ehdotetun 13 c §:n 1 momentin mukaan 13 a §:n 1 momentissa tarkoitetun tunnistamistietojen käsittelyn edellytyksenä on se, että yhteisötilaaja on nimennyt ne henkilöt, joiden tehtäviin tunnistamistietojen käsittely kuuluu tai määritellyt mainitut tehtävät. Tunnistamistietoja voivat käsitellä vain yhteisötilaajan viestintäverkon ja viestintäpalvelun ylläpidosta ja tietoturvasta sekä turvallisuudesta huolehtivat henkilöt. Käyttäjien oikeusturvan kannalta on tärkeää, että he tietävät, ketkä yhteisötilaajan puolesta tunnistamistietoja voivat käsitellä. Yhteisötilaajan tulisi ainakin määritellä ne tehtävät tai esimerkiksi toimintayksiköt, joissa tunnistamistietoja voidaan 13 a–13 j §:ssä tarkoitetuissa tilanteissa käsitellä. Jos yhteisötilaaja hankkii kyseisen palvelun ulkopuoliselta taholta, on riittävää, että on määritelty palveluntarjoajan kyseiset tehtävät tai toiminnot.

Jos tunnistamistietojen käsittelyyn osallistuu ulkopuolisen yrityksen palveluksessa oleva henkilö, tulisi yhteisötilaajan varmistua ennen toimenpiteisiin ryhtymistä siitä, että käsittelyn 13 a–13 d §:ssä säädetyt edellytykset täyttyvät.

Ehdotetussa 2 momentissa säädettäisiin työnantaja-asemassa olevan yhteisötilaajan velvoitteista, joita on noudatettava 1 momentissa tarkoitettujen velvoitteiden lisäksi.

Yksityisyyden suojasta työelämässä annetun lain (759/2004) 4 §:ssä säädetään, että henkilötietojen kerääminen työhönotossa ja työsuhteen aikana kuuluu yhteistoimintalainsäädännössä tarkoitettujen yhteistoimintamenettelyjen piiriin ja asioiden käsittelystä on säädetty muun muassa yhteistoiminnasta yrityksissä annetussa laissa (334/2007) ja yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa (651/1988) sekä yhteistoimintamenettelystä kunnissa annetussa laissa (449/2007).

Työnantajan on myös noudatettava, mitä yksityisyyden suojasta työelämässä annetun lain 21 §:ssä säädetään. Säännöksen mukaan työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin

ja muun tietoverkon käyttö kuuluvat edellä mainitussa yhteistoimintalainsäädännössä tarkoitettujen yhteistoimintamenettelyjen piiriin.

Yhteistoiminta- tai kuulemismenettelyn jälkeen työnantajan on määriteltävä työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan käyttötarkoitus ja siinä käytettävät menetelmät sekä tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä sekä sähköpostin ja tietoverkon käytöstä. Lisäksi on otettava huomioon, että työnantaja-asemassa oleviin yhteisötilaajiin sovelletaan edellä mainitun erityislain muitakin säännöksiä, kuten 6 luvussa tarkoitettuja säännöksiä työnantajalle kuuluvien sähköpostiviestien hakemisesta ja avaamisesta.

Säädösten keskinäisestä suhteesta joutuen asiasta on tarpeen säätää myös sähköisen viestinnän tietosuojalaissa. Sääntelyn tarvetta korostaa lisäksi se, että 13 a–13 j §: §:ssä tarkoitettu tunnistamistietojen käsittely ei kaikissa tapauksissa ole henkilötietolaissa (523/1999) tarkoitettua henkilötietojen käsittelyä.

Pykälän 2 momentin 1 kohdan mukaan työnantajan olisi ensinnä käsiteltävä 13 a–13 j §:ssä tarkoitetussa tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt yhteistoiminnasta yrityksissä annetun lain 4 luvussa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa ja työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa tarkoitetussa yhteistoimintamenettelyssä. Tämä tarkoittaa, että ennen kuin työnantaja ottaa käytäntöön 13 a–13 j §:ssä tarkoitettuja menettelyjä tai niiden muutoksia, olisi niiden perusteista, tavoitteista, tarkoituksesta ja vaikutuksista neuvoteltava niiden työntekijöiden edustajien kanssa, joita asia koskee.

Yhteistoimintamenettelyn piiriin kuuluisivat viestintäverkon luvattomaan käyttöön tai viestintäpalvelun ohjeen vastaiseen käyttöön liittyvät keskeiset kysymykset, kuten viestintäverkon käytöstä laaditut ohjeet, automaattisen haun toimintaperiaatteet ja millä perusteella viestintäverkon luvattoman käytön tai viestintäpalvelun ohjeen vastaisen käytön katsotaan aiheuttavan työnantajalle merkittävää haittaa ja vahinkoa. Yhteisötilaajan tulisi vastaavasti selvittää myös ne seikat ja perusteet, joiden perusteella automaattinen tai manuaalinen käsittely olisi mahdollista yrityssalaisuuksien paljastamisen selvittämiseksi.

Toiseksi yhteistoimintamenettelyssä olisi käsiteltävä ne ehdotetussa 1 momentissa tarkoitetut tehtävät, joissa tunnistamistietoja voidaan käsitellä.

Tämän lisäksi työnantajan olisi tiedotettava käsitellyistä asioista tekemänsä päätökset työntekijöille tai heidän edustajilleen siten kuin yksityisyyden suojasta työelämässä annetun lain 21 §:ssä säädetään.

Ehdotetun 3 momentin mukaan muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi edellä mainituista asioista.

Ehdotetussa 4 momentissa ehdotetaan säädettäväksi muiden kuin työnantaja-asemassa olevien yhteisötilaajien tiedottamisvelvollisuudesta käsittelyoikeutta käytettäessä, mitä olisi noudatettava 13 b ja 13 c §:n 1 momentissa tarkoitettujen velvoitteiden lisäksi. Säännös koskisi tällöin lähinnä oppilaitoksia, kirjastoja ja muita organisaatioita, jotka tarjoavat käyttäjiensä käytettäväksi viestintäpalveluita.

Ehdotetun säännöksen mukaan yhteisötilaajan tulisi tiedottaa käyttäjille 13 a–13 j §:ssä tarkoitetussa tunnistamistietojen käsittelyssä noudattamastaan menettelystä ja 13 c § 1 momentissa tarkoitetuista tehtävistä, joita hoitavat henkilöt voivat tunnistamistietoja käsitellä. Ilmoitus olisi kertaluontoinen ja se voitaisiin tehdä joko silloin, kun käyttöoikeus viestintäverkon tai viestintäpalvelun käyttöön annetaan käyttäjälle tai jos se ei ole mahdollista, muulla sopivalla tavalla.

13 d §. *Yhteisötilaajan käsittelyoikeuden edellytykset väärinkäytöstapauksissa.* Ehdotetussa 13 d §:ssä säädettäisiin tunnistamistietojen käsittelyn menettelytavoista ja menettelyyn liittyvistä edellytyksistä.

Ehdotetun 1 momentin mukaan yhteisötilaaja saa käsitellä tunnistamistietoja automaattisen hakutoiminnon avulla, joka voi perustua viestien kokoon, yhteenlaskettuun kokoon, tyyppiin, määrään, yhteystapaan tai kohdeosoitteisiin.

Ennen tunnistamistietojen käsittelyyn ryhtymistä yhteisötilaajan olisi tullut huolehtia, että kaikki ehdotetussa 13 a–13 j §:ssä tarkoitetut käsittelyn edellytykset täyttyvät.

Automaattisella hakutoiminnolla tarkoitetaan toimintoa, jossa hakua ei tapauskohtaisesti kohdisteta ihmistyövoimin, vaan jossa hakukone hakee viestintäverkosta automaattisesti poikkeamia tietyin ennalta määritellyin kriteerein. Automaattinen haku olisi kyseessä, kun viestintäliikennettä analysoidaan massamuotoisesti esimerkiksi liikenteen määrän, tyypin tai liikenteen kohdeosoitteen tyypin, mutta ei viestintäverkon tai -palvelun käyttäjän yhteysosoitteen perusteella. Automaattisessa haussa yksittäisen käyttäjän viestien tunnistamistiedot eivät tulisi luonnollisen henkilön tietoon.

Viestintäverkkojen luvatonta käyttöä ja viestintäpalvelujen ohjeen vastaista käyttöä voidaan käytännössä selvittää muun muassa automaattisin kapasiteetin käyttömittarein tai tunkeutumisenestosovelluksin, kuten palomuurein. Samoja teknisiä sovelluksia käytetään myös automaattiseen kapasiteetin seurantaan sekä vika- ja häiriötilanteiden havaitsemiseen. Samoilla sovelluksilla yhteisötilaajat voivat myös määritellä viestintäverkkonsa ja -palvelunsa käytölle rajat: he voivat esimerkiksi estää liikennöinnin omasta verkostaan tiettyihin yhteysosoitteisiin tai estää tietyntyyppisen liikenteen kokonaan.

Automaattisessa haussa viestintäverkon luvaton käyttö tai viestintäpalvelun ohjeen vastainen käyttö tai yrityssalaisuuden paljastaminen tunnistettaisiin viestien koon, tyypin, määrän, yhteystavan tai viestien kohdeosoitteen perusteella. Viestin tyypillä tarkoitetaan esimerkiksi viestin, sen osan tai liitteen tallennusmuotoa, kuten esimerkiksi .doc tai .mp3. Viestin yhteystavalla tarkoitetaan esimerkiksi protokollaa, minkä mukaisena se viestintäverkossa välitetään, kuten http tai tcp. Viestin kohdeosoitteella tarkoitetaan sellaisia palveluja tai muita osoitteita, joihin suuntautuvaa liikennettä yhteisötilaaja on kieltänyt, rajoittanut tai estänyt sen kokonaan.

Edellä mainittujen automaattisen haun määrittelyjen tarkoituksena on, että tunnistamistietojen seuranta ei kohdistuisi tavanomaisiin sähköpostiviesteihin ja että rajoitukset olisivat muutoinkin asiallisia ja perusteltuja verkon käytön asiamukaisuuden varmistamisen kannalta.

Ehdotetun 13 d §:n 2 momentin mukaan yhteisötilaaja saa käsitellä tunnistamistietoja tietyin edellytyksin myös manuaalisesti.

Manuaalisella käsittelyllä tarkoitetaan sähköisessä muodossa olevien tietojen käsittelyä silloin, kun käsittely kohdistetaan ihmistyövoimin tapauskohtaisesti tietyn käyttäjän yhteysosoitteen tai tietyn käyttäjäjoukon yhteysosoitteiden tunnistamistietoihin.

On huomattava, että ehdotetut 13 d §:n 3 ja 4 momentit rajaavat manuaalista käsittelyoikeutta.

Ehdotetun 2 momentin 1 kohdan mukaan manuaaliseen käsittelyyn tiedot voisi ottaa automaattisen hakutoiminnon havaittua viestinnässä 1 momentissa tarkoitetuissa tekijöissä poikkeaman. Poikkeamalla tarkoitetaan sellaisia viestejä, joista on niiden koon, tyypin, määrän, yhteystavan tai kohdeosoitteen perusteella, tallentunut automaattiseen hakuun havainto.

Ehdotetun 2 momentin 2 kohdan mukaan tunnistamistiedot voisi ottaa manuaalisesti käsiteltäviksi, jos maksullisen tietoyhteiskunnan palvelun käytön kustannukset ovat nousseet epätavallisen korkeiksi.

Ehdotetun 2 momentin 3 kohdan mukaan manuaalinen käsittely olisi sallittua, jos viestintäverkossa havaitaan sinne oikeudetta asennettu laite, ohjelma tai palvelu.

Ehdotetun 4 kohdan mukaan tunnistamistietoja saisi käsitellä manuaalisesti, jos yrityssalaisuus julkaistaan tai sitä käytetään luvatta.

Ehdotetun 5 kohdan mukaan manuaalinen käsittely olisi yksittäistapauksessa sallittua, jos yhteisötilaajalla on muun 1–4 kohtaan rinnastuvan, yleisesti havaittavissa olevan seikan perusteella syy epäillä, että maksullista tietoyhteiskunnan palvelua tai viestintäverkkoa käytetään luvatta tai että viestintäpalvelua käytetään annetun ohjeen vastaisesti taikka että yrityssalaisuus on luvattomasti annettu ulkopuoliselle.

Yrityssalaisuuden luvattomalla antamisella ulkopuoliselle tarkoitetaan sitä, että viestintäverkon tai -palvelun käyttäjä lähettää tai antaa luvatta sivulliselle pääsyn yrityssalaisuuksiin yhteisötilaajan viestintäverkon kautta tai viestintäpalvelua hyväksikäyttämällä.

Luvatonta käyttöä olisi perusteltua syytä epäillä muun muassa silloin, jos tietohallinnollisen ylläpidon yhteydessä havaitaan viestintä-

verkossa ilmeisesti oikeudetta asennettu laite tai palvelu. Laitteen tai palvelun oikeudettomuus voisi käydä ilmi esimerkiksi poikkeavasta nimeämisestä tai toiminnallisuudesta. Tällöin voitaisiin selvittää minkälaista liikennettä kyseisestä laitteesta tai palvelusta on tapahtunut.

Lisäksi ohjeen vastaista tai luvatonta käyttöä voisi olla perusteltu syy epäillä, jos yhteisötilaajan yhteysosoitteesta havaitaan tulevan viestintäpalvelujen määrityksiin nähden vieraan tyyppistä liikennettä tai muun vastaavan seikan perusteella. Esimerkkinä tällaisesta tilanteesta voisi olla se, että yhteisötilaajan verkossa havaitaan sinne luvatta perustettu julkinen verkossa toimiva asunnonvälityspalvelu tai muu yhteisötilaajan toimintaan kuulumaton palvelu.

Perusteltu syy epäillä yrityssalaisuuksien oikeudetonta paljastamista voisi olla esimerkiksi silloin, jos yrityssalaisuus on julkaistu tai salaisen kehitystyön tietojen perusteella joku muu on kehittänyt kehitystyötä harjoittavan tahon kanssa samanlaisen laitteen tai palvelun.

Ehdotetussa 3 momentissa säädettäisiin tunnistamistietojen sekä automaattisen että manuaalisen käsittelyn edellytyksistä. Momentin mukaan yhteisötilaajan tunnistamistietojen sekä automaattisen hakutoiminnon avulla että manuaalisesti tapahtuva käsittelyoikeus edellyttäisivät, että tapahtuma tai teko todennäköisesti aiheuttaa yhteisötilaajalle merkittävää haittaa tai vahinkoa taikka epäilty yrityssalaisuuden paljastaminen kohdistuu yhteisötilaajan tai sen yhteistyökumppanin elinkeinotoiminnan kannalta keskeisiin yrityssalaisuuksiin taikka teknologisen tai muun kehittämistyön tuloksiin, jotka todennäköisesti ovat merkittäviä elinkeinotoiminnan käynnistämisen tai sen harjoittamisen kannalta.

Säännöksessä tarkoitettua merkittävää haittaa voisi muun muassa olla lisääntyneet kustannukset tai sellainen lisääntynyt tiedonsiirtokapasiteetin käyttö, tietoturvauhka, tai muu vastaava syy, joka vaarantaa, vaikeuttaa tai hidastaa viestintäverkon tai palvelujen käyttöä niille suunniteltuun käyttötarkoitukseen.

Tunnistamistietojen käsittely olisi mahdollista silloin, kun kyseessä olisivat elinkeinotoiminnan kannalta keskeiset yrityssalaisuudet taikka teknologisen tai muun kehittämistyön tulokset. Säännöksessä tarkoitetulla tavalla keskeisiä yrityssalaisuuksia olisivat muun muassa tiedot, jotka antavat yritykselle kilpailuedun ja joita ei julkisista lähteistä ole selvitettävissä. Keskeisinä voitaisiin pitää niitä tietoja, joiden käsittelystä ja suojaamisesta elinkeinonharjoittaja on laatinut erityiset ohjeet ja suojaamiskäytännöt, kuten 13 b §:ssä edellytetään.

Kehittämistyön tulokset on mainittu säännöksessä erikseen, koska kaikissa tapauksissa ei ole selvää, missä vaiheessa niitä olisi pidettävä liiketoiminnan kannalta keskeisinä. Kehittämistyön tuloksina voidaan pitää myös tutkimus- tai kehittämishankkeiden sellaisenaan merkityksellisiä välivaiheen tuloksia sekä tuloksia, jotka osoittavat kehittämistyön jatkamisen kannattamattomuuden. Tunnistamistietojen käsittelyoikeus esitetään ulotettavaksi tilanteisiin, joissa epäillään kehittämistyön tulosten oikeudetonta paljastamista. Tietojen tulisi olla tai niiden olisi voitava olla merkittäviä elinkeinotoiminnan harjoittamisen tai käynnistämisen kannalta.

Kehittämistyön tulosten oikeudeton paljastaminen voi olla niiden omistajan kannalta erittäin haitallista ja estää muun muassa immateriaalioikeudellisen suojan saamisen.

Ehdotetussa 4 momentissa on lisäedellytys manuaaliselle käsittelyoikeudelle. Manuaalisen käsittelyn edellytyksenä on lisäksi, että tiedot ovat välttämättömiä väärinkäytöksen ja siitä vastuussa olevien selvittämiseksi sekä luvattoman tai ohjeen vastaisen käytön lopettamiseksi.

Sähköisen viestinnän tietosuojalain 8 §:n 3 momentin välttämättömyysedellytys asettaa ehdotetulle tunnistamistietojen käsittelylle sekä asialliset että ajalliset rajat.

Pykälässä ehdotetun tunnistamistietojen käsittelyoikeuden yleisten ja erityisten edellytysten ja lain 8 § 3 momentin välttämättömyysedellytyksen vuoksi yhteisötilaaja ei voisi seurata tavanomaisiin viesteihin liittyviä tunnistamistietoja. Esimerkiksi työnantajaasemassa oleva yhteisötilaaja ei voisi seurata viestintäverkon tai viestintäpalvelujen käyttöä työajan seuraamiseksi eikä sen selvittämiseksi onko käyttäjä ollut yhteydessä henkilöstön edustajaan, työsuojeluviranomaisiin tai työterveyshuoltoon. Ajallisesti käsiteltäväksi voitaisiin ottaa vain kulloinkin käsillä olevan tapauksen selvittämisen kannalta välttämättömät

tunnistamistiedot eikä säännös oikeuttaisi käsittelemään tunnistamistietoja tätä laajemmin.

Sähköisen viestinnän tietosuojalain 8 §:n 3 momentin mukaan tunnistamistietojen käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa ja se on toteutettava luottamuksellisen viestin ja yksityisyyden suojaa tarpeettomasti vaarantamatta. Käsittelyn jälkeen viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä.

13 e §. *Käsittelyoikeuden erityiset rajoitukset väärinkäytöstapauksissa.* Ehdotettuun 13 e §:n 1 momenttiin esitetään otettavaksi säännös, jonka mukaan automaattista hakua ei saisi kohdistaa siten, että sillä pyrittäisiin saamaan selville lähdesuojan piiriin kuuluvia tietoja. Tunnistamistietoja ei myöskään saisi ottaa manuaalisesti käsiteltäviksi tällaisten seikkojen selville saamiseksi.

Lain yleisistä käsittelysäännöistä ja käsittelyoikeuden rajauksista huolimatta lainvalmistelussa on katsottu tarpeelliseksi täsmentää nimenomaisella säännöksellä sitä seikkaa, että ehdotettua käsittelyoikeutta ei ole sallittua käyttää lähdesuojan alaisten tietojen selville saamiseksi.

Ehdotetun 2 momentin mukaan käsittelyoikeus yrityssalaisuuksien paljastamisen selvittämiseksi rajattaisiin koskemaan vain työnantaja-asemassa olevia yhteisötilaajia. Käsiteltäväksi voivat tulla vain sellaisten henkilöiden tunnistamistiedot, joille yhteisötilaaja on antanut pääsyn tai joilla muutoin on yhteisötilaajan hyväksymällä tavalla pääsy yrityssalaisuuksiin. Pääsyn antaminen voi tapahtua esimerkiksi käyttäjäoikeuksia hallinnoimalla. Henkilötahoja, joilla on pääsy yrityssalaisuuksiin, ovat ensisijaisesti asiantuntija- ja kehitystehtävissä työskentelevät henkilöt, joiden tehtäviin yrityssalaisuuksien käsittely kuuluu. Lisäksi yrityssalaisuudet voivat tulla erilaisissa avustavissa tehtävissä työskentelevien sekä tietojärjestelmien ylläpidosta ja huollosta vastaavien henkilöiden tietoon työtehtävien tai laajojen käyttäjäoikeuksien kautta.

13 f §. *Yhteisötilaajan tiedonantovelvollisuus käyttäjälle väärinkäytöstapauksissa.* Ehdotetun 1 momentin mukaan yhteisötilaajan olisi laadittava 13 d §:n 1 ja 2 momentissa tarkoitetusta manuaalisesta tunnistamistietojen käsittelystä selvitys.

Selvityksen tulisi sisältää tieto siitä, mikä 13 d §:n 2 momentissa tarkoitettu teko tai tapahtuma on ollut käsittelyn perusteena ja millä perusteella tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty. Ehdotetun 13 d §:n 2 momentin perusteella manuaaliseen käsittelyyn oikeuttaa joko automaattisessa haussa havaittu poikkeama viestinnässä tai yleisesti havaittavissa oleva seikka. Jos käsittelyyn on ryhdytty automaattisen haun perusteella, olisi selvitettävä, minkä automaattisen hakutoimintoon asetetun hakukriteerin perusteella tunnistamistiedot ovat päätyneet manuaaliseen käsittelyyn. Jos käsittelyyn on ryhdytty yleisesti havaittavissa olevan seikan perusteella, olisi kyseinen seikka ilmoitettava. Selvityksestä tulisi myös käydä ilmi ajankohta, käsittelijät ja käsittelystä päättänyt henkilö.

Ehdotetun 2 momentin mukaan käsittelyyn osallistuneiden on allekirjoitettava selvitys. Selvitys on tarpeen viestintäverkkojen ja palvelujen käyttäjien, tietojen käsittelyyn osallistuneiden ja siitä päättäneen henkilön oikeusturvan kannalta. Jälkikäteen on voitava selvittää, kuka tietoja on käsitellyt, mihin ajankohtaan ja kenen aloitteesta. Tiedoilla voidaan jälkikäteen selvittää mahdollisia väärinkäytöksiä. Selvityksen säilyttämisajaksi ehdotetaan säädettäväksi kaksi vuotta.

Tietosuojavaltuutetun toimisto on 10. päivänä helmikuuta 2003 antanut ohjeen käyttäjälokien tietojen käsittelystä henkilötietolain mukaan. Ohjeen mukaan lokiin tallentuvia tietoja voidaan säilyttää niin kauan kuin rekisteröity voi esittää rikosperusteisia vaatimuksia henkilötietojen käsittelijää tai sivullisia vastaan. Ohjeessa todetaan, että koska henkilötietojen lainvastainen käsittely ja rekisteriin tunkeutuminen ovat kriminalisoituja tekoja, joiden syyteoikeus vanhentuu kahdessa vuodessa, on lokia säilytettävä kahden vuoden ajan, jollei aiemmin ole voitu todeta säilyttämisen perusteen menettäneen merkityksensä. Selvityksistä tai tallennetuista tiedoista muodostuu henkilötietolain tarkoittama henkilörekisteri, jota koskee kaikki henkilötietojen käsittelyä koskevat säännökset, kuten esimerkiksi tarkastusoikeutta (26 §), mutta myös tarkastusoikeuden rajoituksia (27 §) koskevat säännökset.

Ehdotetun 3 momentin mukaan 1 momentissa tarkoitettu selvitys on annettava tiedoksi käyttäjälle heti, kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta. Saatuaan tiedon tunnistamistietojensa käsittelystä, käyttäjällä on mahdollisuus varmistua toimien lain mukaisuudesta ja kääntyä tarvittaessa tietosuojavaltuutetun tai poliisin puoleen. Jos käyttäjä on työntekijä, voi hän kääntyä myös ammattijärjestönsä puoleen.

Momenttiin ehdotetaan otettavaksi säännös siitä, että viestintäverkon tai viestintäpalvelun käyttäjällä on oikeus lakiin tai sopimukseen perustuvan salassapitovelvollisuuden estämättä luovuttaa selvitys ja sen yhteydessä saamansa tiedot etujaan tai oikeuksiaan koskevan asian käsittelyä varten. Säännös olisi pakottava, eikä siitä voisi poiketa sopimuksella.

Selvitystä ei kuitenkaan olisi tarpeen antaa sellaisille käyttäjille, joiden tunnistamistietoja on käsitelty manuaalisesti siten, että käsittely on ollut massamuotoista, eikä se ole kohdistunut tietyn käyttäjän tunnistamistietoihin.

Ehdotuksessa ei ole säädetty selvityksen tiedoksi antamiselle takarajaa. Selvitys tai tiedot olisi annettava mahdollisimman pian käsittelyn päätyttyä. Käynnissä olevasta esitutkinnasta johtuvat tutkinnalliset seikat tai tähän verrattavissa olevat syyt voisivat oikeuttaa selvityksen tiedoksi antamisen lykkäämistä, kunnes tiedoksianto voidaan tutkintaa vaarantamatta tehdä.

Lain 8 §:n 3 momentin välttämättömyysedellytys rajoittaa osaltaan myös tutkinnallisista syistä johtuvaa selvityksen antamisen lykkäämistä. Käsittelyllä ei saa rajoittaa luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä tavoiteltavan tarkoituksen kannalta. Heti kun epäiltyä väärinkäytöstä on selvitetty riittävästi, on käsittely lopetettava ja siitä on laadittava ja annettava käyttäjälle selvitys.

13 g §. *Yhteisötilaajan tiedonantovelvollisuus työntekijöiden edustajalle väärinkäytöstapauksissa.* Ehdotetussa 13 g §:n 1 momentissa säädettäisiin työnantajan velvollisuudesta antaa vuosittainen selvitys 13 d §:n 2 momentissa tarkoitetusta tunnistamistietojen manuaalisesta käsittelystä työntekijöiden edustajalle yksityisyyden suojan tehokkaan valvonnan toteuttamiseksi. Selvityksen sisältö vastaisi 13 h §:n 2 momentissa tarkoitettua selvitystä; siitä tulisi käydä ilmi tunnistamistietojen manuaalisten käsittelykertojen määrä vuoden aikana ja niiden perusteet.

Pykälän 2 momentin mukaan työntekijöiden edustajalla, jolle 1 momentissa tarkoitettu selvitys olisi annettava, tarkoitetaan lähtökohtaisesti joko työehtosopimuksen mukaista luottamusmiestä tai työsopimuslain 13 luvun 3 §:ssä tarkoitettua luottamusvaltuutettua. Jos jollakin henkilöstöryhmällä ei ole tällaista edustajaa, edustaisi heitä yhteistoimintalainsäädännössä tarkoitettu yhteistoimintaedustaja tai edustaja. Jos tällaistakaan ei olisi valittu, olisi mainittu selvitys annettava tiedoksi kaikille kyseisen henkilöstöryhmän työntekijöille.

Osa yhteistoimintamenettelyn tai tiedottamisen piiriin kuuluvista tiedoista ei ole julkisia. Elinkeinotoiminnan jatkumisen ja menettelyjen tarkoituksen kannalta on tärkeää, etteivät tiedot leviä pykälän tarkoitusta laajemmin. Tämän vuoksi pykälän 3 momentissa ehdotetaan, että pykälässä tarkoitettu työntekijöiden edustajan tai työntekijän olisi pidettävä salassa tietoonsa saamat yrityssalaisuuden loukkaukset ja epäilyt yrityssalaisuuden loukkaamisesta.

Salassapitovelvollisuuden piiriin kuuluvaa tietoa ei saisi paljastaa sivulliselle senkään jälkeen, kun henkilö ei enää hoida sitä tehtävää, jossa hän on tiedon saanut. Salassapitovelvollisuus jatkuisi sekä työntekijöiden että heidän edustajiensa osalta koko työsuhteen voimassaoloajan. Rangaistuksesta vaitiolovelvollisuuden rikkomisesta säädettäisiin lain 42 §:ssä.

Viranomaisten toiminnan julkisuudesta annetun lain 24 §:ssä säädetään salassapitovelvoitteista. Ehdotettu säännös olisi osittain päällekkäinen siitä, mitkä tiedot säädettäisiin tässä laissa salassa pidettäviksi. Tämä ei ole tarkoituksenmukaista. Siksi ehdotetaan, että virkamiehen ja muun viranomaisessa toimivan vaitiolovelvollisuudesta olisi voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa ja muualla laissa säädetään.

Ehdotettu salassapitovelvollisuus ei estäisi tietojen antamista lakia valvovalle viranomaiselle.

Ehdotuksessa ei oteta kantaa työsuhteen päättymiseen liittyviin kysymyksiin. Kysymys siitä, milloin tietoyhteiskunnan palvelujen tai viestintäverkkojen luvaton käyttö taikka viestintäpalvelujen tai ohjeen vastainen käyttö tai

rikollinen toiminta oikeuttaa työsuhteen päättämiseen, ratkeaa työsopimuslain ja muun työoikeudellisen lainsäädännön perusteella. Työsuhteen päättämistä koskevissa oikeudenkäynneissä työnantaja on velvollinen näyttämään työsuhteen päättämisperusteen olemassaolon. Ehdotukset eivät aiheuttaisi muutoksia näihin periaatteisiin.

13 h §. *Ennakkoilmoitus ja vuosittainen selvitys tietosuojavaltuutetulle väärinkäytöstapauksissa.* Ehdotetussa 13 h §:ssä säädettäisiin yhteisötilaajan velvollisuudesta antaa tunnistamistietojen käsittelystä selvitys tietosuojavaltuutetulle.

Ehdotetun 1 kohdan mukaan yhteisötilaajan olisi ennen tunnistamistietojen käsittelyn aloittamista annettava tietosuojavaltuutetulle kertaluonteinen selvitys, josta kävisi ilmi 13 d §:ssä tarkoitetuissa tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt. Momentin 2 kohdan mukaan ennakkoilmoituksessa on käytävä ilmi 13 c §:n 1 momentissa tarkoitetut tehtävät, joissa tietoja käsitellään. Näiltä osin selvityksestä tulisi käydä ilmi samat seikat, mitkä 13 c §:n 2 momentin mukaan on käsiteltävä yhteistoimintamenettelyssä. Selvityksestä tulisi 3 kohdan mukaan käydä selville myös se, miten yhteisötilaaja on tiedottanut tai tiedottaa näistä seikoista viestintäverkkojen ja palvelujen käyttäjille. Jos selvityksen kohteena olevissa seikoissa tapahtuu olennaisia muutoksia, tulisi muutoksista toimittaa uusi selvitys.

Voimassa olevan lain 13 §:n tunnistamistietojen käsittely väärinkäytöstapauksissa ei edellytä minkäänlaista ennakollista toimenpidettä ennen käsittelyyn ryhtymistä. Myöskään laissa yksityisyyden suojasta työelämässä, sen 6 luvussa, joka koskee työnantajalle kuuluvien sähköpostiviestien hakemista ja avaamista, ei ole erityistä ennakollista ilmoitus- tai lupamenettelyä toiminnalle.

Ehdotetulla ilmoitusvelvollisuudella parannetaan käyttäjien oikeusturvaa. Esimerkiksi lupamenettelyyn nähden, ehdotetun ennakkoilmoituksen antamisen voidaan katsoa olevan oikeassa suhteessa suojeltavaan etuun nähden. Tietosuojavaltuutettu saa etukäteen tiedon niistä tahoista, jotka ryhtyvät käyttämään käsittelyoikeuttaan ja voi toimintansa tarkoituksenmukaisella järjestämisellä ryhtyä toteuttamaan ehdotetun 32 §:n 1 momentin 1 kohdan mukaista valvontaa.

Ehdotetun 2 momentin mukaan yhteisötilaajan tulisi antaa tietosuojavaltuutetulle vuosittain selvitys, jossa hänen olisi selvitettävä kuluneen vuoden osalta kunkin manuaalisen tunnistamistietojen käsittelykerran osalta, onko käsittelyn perusteena ollut maksullisen tietoyhteiskunnan palvelun tai viestintäverkon luvaton käyttö tai viestintäpalvelun ohjeen vastainen käyttö vai yrityssalaisuuden paljastaminen.

13 i §. *Yhteisötilaajan oikeus säilyttää tunnistamistietoja väärinkäytöstapauksissa.* Ehdotettuun 13 i §:ään ehdotetaan selventävää säännöstä siitä, että 13 a–13 h § ei oikeuta yhteisötilaajaa säilyttämään tunnistamistietoja kauempaa kuin lain mukaan on sallittua.

Lain 8 §:n 3 momentin mukaan tunnistamistiedot on käsittelyn jälkeen hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään.

Sellaiset tunnistamistiedot, joista on tunnistettavissa luonnollinen henkilö, ovat myös henkilötietolaissa (523/1999) tarkoitettuja henkilötietoja. Henkilötietolaissa omaksutun henkilörekisterin käsitteen vuoksi sellaiset tunnistamistiedot muodostavat henkilötietolaissa tarkoitetun henkilörekisterin, vaikka näitä tietoja ei talletettaisikaan erilliseen tekniseen rekisteriin (henkilötietolaki, 3 §:n 3 kohta).

13 j §. *Yhteisötilaajan oikeus tietojen luovuttamiseen väärinkäytöstapauksissa.* Pykälään ehdotetaan otettavaksi säännös, joka oikeuttaisi yhteisötilaajan luovuttamaan ehdotetun 13 a–13 i §:n mukaisessa menettelyssä saamansa yhteisötilaajan viestintäverkon käyttäjää koskevat tunnistamistiedot poliisille asianomistajana tekemänsä rikosilmoituksen tai tutkintapyynnön yhteydessä.

Säännösehdotuksen muotoilussa on otettu huomioon se, että se oikeuttaisi myös poliisin käsittelemään näin saamiaan tietoja. Säännös on tarpeen sen mahdollistamiseksi, että yhteisötilaaja voi saattaa rikoksena selvitettäväksi sellaiset tapaukset, joissa voi olla kysymys rangaistavaksi säädetystä teosta, kuten luvattomasta käytöstä tai yrityssalaisuuteen kohdistuvasta rikoksesta.

14 §. *Käsittely teknisen vian tai virheen havaitsemiseksi.* Koska vika- ja virhetilanteet on

pystyttävä havaitsemisen ohella estämään ja selvittämään, säännöstä ehdotetaan täsmennettäväksi. Myös voimassa olevan lain hallituksen esityksen 14 §:n yksityiskohtaisten perustelujen valossa on selvää, että säännöksellä on tarkoitettu vika- ja virhetilanteiden havaitsemisen lisäksi estämistä ja selvittämistä.

20 §. *Toimenpiteet tietoturvan toteuttamiseksi*. Ehdotetussa 20 §:ssä esitetään säädettäväksi teleyritysten, lisäarvopalvelun tarjoajien ja yhteisötilaajien oikeuksista toimenpiteisiin tietoturvasta huolehtimiseksi. Säännös mahdollistaisi viestintäverkkojen sekä niihin liitettyjen palvelujen tietoturvalle haittaa aiheuttavien häiriöiden havaitsemisen, estämisen, selvittämisen ja esitutkintaan saattamisen.

Tietoturvauhat ovat tyypillisesti ulkopuolelta viestintäverkkoon tai -palveluihin kohdistuvia uhkia, joilla pyritään esimerkiksi saamaan selville käyttäjien tietoja tai ottamaan haltuun tietokoneita palvelunestohyökkäysten toteuttamiseksi taikka ei toivotun suoramarkkinointiviestien lähettämiseksi. Tietoturvatoimenpiteet kohdistuvat useimmiten viestintäverkkoon tai palveluun saapuvaan liikenteeseen, joskin tietyissä tilanteissa on tarve kohdistaa toimenpiteitä myös lähtevään liikenteeseen tietoturvauhan selvittämiseksi.

Pykälän 1 momentissa yksilöitäisiin tietoturvatoimiin oikeutetut tahot sekä tilanteet, joissa tietoturvatoimiin voidaan ryhtyä. Pykälässä ehdotettujen viestintään liittyvien toimien lisäksi tietoturvasta voidaan huolehtia myös tietohallinnollisin keinoin ja asettamalla viestintäverkon tai palvelun käytölle teknisiä rajoituksia, joiden käyttämiselle sähköisen viestinnän tietosuojalaki ei aseta rajoituksia.

Ehdotetun 1 momentin 1 kohdassa tarkoitettuja tietoturvalle haittaa aiheuttavia häiriöitä olisivat esimerkiksi tahallisten haittaohjelmien laaja levittäminen ja käyttö. Tällaisia häiriöitä olisivat myös viestintäverkon käyttö eitoivottujen suoramarkkinointiviestien lähettämiseen tai tällaisten viestien laajamittainen saapuminen viestintäverkkoon taikka muiden viestien käyttö tietoliikenteen tai tietojärjestelmien lamauttamiseen taikka muut viestintäverkon tai siihen liitetyn palvelun toimintakyvyn kannalta hyvin vakavat häiriöt. Myös tilanteet, joissa viestintäverkon normaali toiminta häiriintyy muilla tavoin, taikka joissa luvatta tuhotaan tai muutetaan koneisiin tallennettuja tietoja, voisivat olla tällaisia haittaa aiheuttavia häiriöitä.

Ehdotetun säännöksen viestintäverkkoon liitetyillä palveluilla tarkoitetaan voimassa olevan lain 2 §:n 1 momentin määritelmien 6 kohdassa tarkoitettujen viestintäpalvelujen ja 7 kohdassa tarkoitettujen lisäarvopalvelujen lisäksi yhteisötilaajien muilta tahoilta hankkimia palveluja sekä niiden itse tarjoamia palveluja.

Ehdotetun 1 momentin 2 kohdan viestin lähettäjän tai vastaanottajan viestintämahdollisuuksien turvaaminen ehdotetaan mainittavaksi erikseen, koska ei-toivottujen suoramarkkinointiviestien ja muiden vastaavien viestien loppukäyttäjälle tuleva määrä voi nousta niin korkeaksi, että hänen viestintämahdollisuutensa estyvät kokonaan, vaikka tällaisten viestien määrä ei vaikuttaisikaan koko viestintäverkon tai -palvelun toimintaan. Lisäksi tietoturvahyökkäykset on mahdollista kohdistaa tiettyyn käyttäjään, jolloin hänen viestintänsä voi estyä kokonaan. Ehdotettu muutos on tarpeen sen selventämiseksi, että tietoturvatoimiin on mahdollista ryhtyä myös näissä tapauksissa.

Ehdotetun 1 momentin 3 kohtaan esitetään lisättäväksi myös oikeus ryhtyä toimenpiteisiin viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:n mukaisten maksuvälinepetosten valmistelun ehkäisemiseksi. Kyse on niin sanotusta phishingistä, eli suurelle käyttäjäjoukolle toimitettavista viesteistä, joilla pyritään urkkimaan käyttäjien identiteetti- ja maksuvälinetietojen hankkimista laittomiin käyttötarkoituksiin.

Maksuvälinepetoksen valmistelu kattaa tilanteet, joissa maksuvälinepetosrikoksen tekemistä varten joku valmistaa, tuo maahan, hankkii, vastaanottaa tai pitää hallussaan maksuvälinelomakkeen tai valmistaa, tuo maahan, hankkii, vastaanottaa, pitää hallussaan, myy tai luovuttaa erityisesti maksuvälinelomakkeen valmistamiseen soveltuvan välineen tai tarvikkeen taikka erityisesti tietoverkoissa tapahtuvaan maksuliikenteeseen soveltuvan tallenteen, ohjelmiston, välineen tai tarvikkeen.

Rikoslain perusteluissa (HE 38/1997 vp.) todetaan, että lainkohdassa tarkoitetun välineen tai tallenteen olisi oltava sellainen, että sillä voisi joko suorittaa maksuja, tilinostoja tai tilisiirtoja tai sen käyttämisen olisi oltava välttämätön edellytys mainittujen suoritusten

tekemiseksi. On kuitenkin tilanteita, joissa suoritus ei onnistu ilman lisäinformaation esittämistä. Hallituksen esityksen mukaan lisäinformaatiota ovat esimerkiksi erilaiset identifioimiskeinot, joilla maksuvälineen käyttäjä kytketään maksu- tai muuhun tapahtumaan. Laskujen maksaminen verkkopankissa edellyttää pankin antaman asiakasnumeron ilmoittamista sekä joka käyttökerralla vaihtuvan tunnusluvun tai salasanan antamista. Hallituksen esityksen mukaan on perusteltua rinnastaa tällaiset maksuvälineen käyttämisen välttämättömät edellytykset niihin välineisiin ja tallenteisiin, joilla varsinaiset suoritukset tehdään.

Ehdotetuissa 2 ja 3 momentissa säädettäisiin toimenpiteistä, joihin tietoturvasta huolehtimiseksi voidaan ryhtyä. Toimet voisivat kohdistua itse viestien lisäksi myös niiden mahdollisiin liitteisiin.

Ehdotetun 2 momentin 1 kohtaan esitetään lisättävän toimenpiteeksi viestin automaattinen sisällöllinen analyysi. Käytännössä automaattinen haitallisten viestien suodattaminen ja muun tietoturvan ylläpitäminen vaatii viestien jatkuvaa automaattista analysointia. Automaattisessa analyysissa haitalliset ohjelmat ja käskyt tunnistettaisiin ennalta tehtyjen määrittelyjen perusteella, eikä viestin sisältö tulisi tällöin luonnollisen henkilön tietoon.

Voimassa olevan lain 20 §:n 3 momentin mukaan viestin sisältöön saa puuttua ainoastaan teknisin keinoin viestin tarkastamiseksi ja tarkastaminen on sidottu tiettyihin rikostunnusmerkistöihin. Viestin sisältöön puuttumisen sitomisesta rikostunnusmerkistöihin seuraa, että analyysi voidaan tehdä vain silloin, kun teko on tahallinen. Käytännössä haitallisia viestejä ei aina lähetetä tahallisesti. Tietoturvan ylläpitämiseksi myös tahattomasti lähetetyt viestit, jotka aiheuttavat tietoturvalle vaaran, tulisi pystyä analysoimaan.

Ehdotetun 2 momentin 2 kohtaan viestien välittämisen ja vastaanottamisen estämisen lisäksi esitetään uudeksi toimenpiteeksi myös välittämisen tai vastaanottamisen rajoittamista. Lisäksi täsmennettäisiin, että sekä viestien välittämisen tai vastaanottamisen rajoittamisen että estämisen tulee tapahtua automaattisesti ennalta tehtyjen määrittelyjen perusteella. Rajoittaminen mahdollistaisi palvelun täydellistä katkaisemista lievempien toimien toteuttamisen.

Viestien välittämisen ja vastaanottamisen automaattinen rajoittaminen voisi tulla kyseeseen esimerkiksi tilanteessa, jossa jokin yhteydenottotapa tai jokin varmennus- taikka tunnistuskäytäntö osoittautuu vaarallisen heikkouden sisältäväksi ja sen käyttö olisi estettävä muiden viestien välittämiseen puuttumatta. Samoin jos havaitaan haitallisten viestien tulevan tietystä yhteysosoitteesta, voitaisiin kyseisestä osoitteesta tulevien viestien vastaanottamista rajoittaa. Automaattinen rajoittaminen voisi tulla kyseeseen myös silloin, jos jonkin liikennöintitavan määrällinen tai laadullinen kasvaminen uhkaa estää muita liikennöintitapoja. Viestien välittämisen tai vastaanottamisen estäminen saattaisi tulla kyseeseen esimerkiksi silloin, jos tietokone on otettu luvatta haltuun eikä uhkaa voida torjua vähemmän viestintää rajoittavalla keinolla. Kuten estämiseen, myös rajoittamiseen saisi ryhtyä vain, jos toimet ovat välttämättömiä 1 momentissa tarkoitettujen tavoitteiden saavuttamiseksi.

Ehdotetun 2 momentin 3 kohdan mukaan viesteistä saisi automaattisen tietojen käsittelyn avulla poistaa haitalliset tietokoneohjelmat. Poistamisen tulisi tapahtua automaattisesti ennalta tehtyjen määrittelyjen perusteella. Säännöksessä tarkoitetulla tavalla haitallisia olisivat ohjelmat tai käskyt, jotka tarkoituksellisesti aiheuttavat ei-toivottuja tapahtumia tietokoneessa tai tietojärjestelmässä. Tällaiset ohjelmat voivat esimerkiksi antaa ulkopuolisille pääsyn verkkoon tai siihen kytkettyihin tietokoneisiin, muuttaa tai paljastaa ulkopuolisille tietokoneille tallennettuja tietoja tai antaa ulkopuolisille mahdollisuuden hallita tietokonetta.

Ehdotetun 2 momentin 4 kohdan mukaan myös muut, momentissa aiemmin lueteltuihin toimenpiteisiin rinnastuvat tekniset toimenpiteet, olisivat käytettävissä tietoturvasta huolehtimiseksi. Tällaisia toimenpiteitä voisivat olla useiden koneiden liikenteen tunnistamistietojen analysointi kausaliteetin havaitsemiseksi, mikä on tarpeen luvattoman etäohjauksen havaitsemiseksi ja haitallisten komentokäskyjen eristämiseksi sekä viestiliikenteen keinotekoinen hidastaminen tai muut vastaavankaltaiset toimenpiteet.

Ehdotettu uusi 3 momentti sisältäisi oikeuden käsitellä yksittäisen viestin sisältöä manu-

aalisesti, jos on ilmeistä, ettei automaattisen tietojenkäsittelyn avulla pystytä turvaamaan ehdotetussa 1 momentissa tarkoitettujen tavoitteiden toteutumista. Ehdotettu 3 momentti oikeuttaisi viestin sisällön manuaaliseen tarkastamiseen vakavissa uhkatilanteissa, joissa viestin tyypin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn, eikä automaattinen sisällöllinen analyysi riitä tietoturvan takaamiseen.

Jos automaattinen sisällöllinen analyysi on havainnut tietoturvaa uhkaavan viestin, mutta ongelma ei ratkea yksin analyysin perusteella, viestin sisältöä ja tunnistamistietoja saisi käsitellä myös manuaalisesti. Automaattinen sisällöllinen analyysi ei aina täydellisesti tunnista viestissä olevaa haittaohjelmaa tai vahingollista komentoa, jolloin viestintäjärjestelmät saattavat vaarantua. Viestin sisältämän haittaohjelman toimintaperiaate saattaa olla automaattisen analyysin ohjelmalle tuntematon. Tällöin on ensiarvoisen tärkeää selvittää manuaalisesti, mikä aiheutti vaaratilanteen ja miten se vastaisuudessa torjutaan. Tietojärjestelmät voivat myös lähettää toisilleen automaattisia viestejä, joita virhetilanteen sattuessa olisi kyettävä manuaalisesti läpikäymään, jotta virhe saataisiin korjatuksi. Myös silloin, jos tietokone on otettu luvatta etäohjaukseen, voi tilanteen selvittämiseksi olla tarpeen selvittää ohjaukseen liittyvien viestien sisältöä.

Manuaalisesti käsiteltäväksi tulevat viestit olisivat haitallisia viestejä, jotka voivat sisältää esimerkiksi haittaohjelman tai haitallisen käskyn, jolla pyritään lamauttamaan koko verkon tai palvelun toiminta. Jos haitallisia viestejä ei saada poistettua, saattavat niiden sisältämät haittaohjelmat vaarantaa kaikkien verkon käyttäjien viestintämahdollisuudet tai tietokoneille tallennettujen tietojen luottamuksellisuuden. Viestin sisältöön puuttumisesta olisi ilmoitettava viestin lähettäjälle ja vastaanottajalle, jollei ilmoituksella vaarannettaisi 1 momentissa tarkoitettujen tavoitteiden toteutumista. Ilmoitus ei aina edistä tarkoituksen toteutumista, kuten silloin, kun viestissä on sellainen haitallinen koodi, joka lamauttaa tietojärjestelmiä. Koodin haitallisuudesta ilmoittaminen ei palvelisi verkkojen tai palvelujen tietoturvaa taikka viestin vastaanottajan viestintämahdollisuuksien turvaamista. Ilmoittaminen saattaisi päinvastoin tuottaa lisää ongelmatilanteita.

Oikeus viestin sisällön tarkastamiseen ei olisi yleinen tarkastusoikeus, vaan kyse olisi erittäin poikkeuksellisista tilanteista. Ehdotetun 4 momentin mukaan viestin sisällön manuaalisen käsittelyn olisi oltava välttämätöntä tietoturvasta huolehtimiseksi.

Ehdotetun 4 momentin mukaan toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Samoin toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin välttämätöntä.

Ehdotetusta 4 momentista ehdotetaan korvattavaksi yksityiskohtaiset viittaukset palveluista ja viestin vastaanottajan viestintämahdollisuuksien turvaamisesta viittauksella edellä tässä pykälässä säädettyyn. Kyse olisi teknisestä muutoksesta, jolla ei pyritä muuttamaan vallitsevaa oikeustilaa.

Pykälän 5 momenttia ehdotetaan tarkennettavaksi siten, että Viestintäviraston oikeus antaa teknisiä määräyksiä rajattaisiin koskemaan vain teleyrityksiä ja lisäarvopalvelun tarjoajia.

32 §. *Tietosuojavaltuutetun tehtävät.* Ehdotuksella lisättäisiin tietosuojavaltuutetun tehtäviin valvoa 13 a–13 j §:ssä tarkoitettua yhteisötilaajan tunnistamistietojen käsittelyä maksullisen tietoyhteiskunnan palvelun tai viestintäverkon luvattoman käytön taikka viestintäpalvelun ohjeen vastaisen käytön ja yrityssalaisuuksien oikeudettoman paljastamisen tilanteissa. Käytännössä on tarpeen keskittää valvontatoimet tiettyihin asiakokonaisuuksiin. Tietosuojavaltuutetun tehtävänä on valvoa henkilötietolain mukaisesti henkilötietojen käsittelyä ja työelämän tietosuojalakia valvovat työsuojeluviranomaiset yhdessä tietosuojavaltuutetun kanssa. Koska yksi suurimmista yhteisötilaajan ryhmistä on yritykset työnantajina, on johdonmukaista, että tietosuojavaltuutettu valvoo osin myös tämän lain noudattamista.

Ehdotetun pykälän toiseksi momentiksi ehdotetaan lisättäväksi säännös, jonka mukaan 13 a–13 j §:n noudattamisen valvonnasta aiheutuvista toimenpiteistä voidaan periä maksu yhteisötilaajalta. Maksullisista toimenpiteistä ja maksun suuruudesta päätettäisiin oikeusministeriön asetuksella valtion maksuperustelais-

sa (150/1992) säädettyjen perusteiden mukaisesti. Voimavarojen ja niistä aiheutuvien kustannusten täsmällistä arviota tehtäessä tulee kuulla asianomaisia ministeriöitä ja niitä, joita maksuvelvollisuus koskisi. Maksuvelvollisuuden tulee olla oikeassa suhteessa valvottavan kokoon ja toiminnan luonteeseen. Valvonnan maksullisuus on perusteltua, koska 13 a–13 j §:ssä tarkoitettu tunnistamistietojen käsittely on yhteisötilaajalle valinnaista.

33 *§. Ohjaus- ja valvontaviranomaisten oikeus saada tietoja.* Voimassa olevan lain mukaan Viestintävirastolla ja tietosuojavaltuutetulla on oikeus saada tässä laissa säädettyjen tehtävien hoitamiseksi tunnistamistiedot, paikkatiedot ja 20 §:n 2 momentissa tarkoitetut viestit tietyin tarkoin rikostunnusmerkistöihin sidotuin kriteerein. Lain tietoturvaa koskevaa 20 §:ää ehdotetaan muutettavaksi siten, että se sallisi viestien automaattisen sisällöllisen analyysin ja puuttumisen viestin sisältöön tietyissä tilanteissa myös muutoin kuin automaattisen sisällöllisen analyysin keinoin. Tästä syystä viittaus lain tiettyyn momenttiin ehdotetaan kumottavaksi. Kyse on valvovien viranomaisten arvioinnista siitä, että jokin rikostunnusmerkistöistä täyttyy ja voidakseen suorittaa tehtävänsä asianmukaisesti, on sekä tunnistamistietojen ja paikkatietojen että viestien saaminen tietyissä lain noudattamisen valvomisen tilanteissa välttämätöntä.

34 §. *Valvontaviranomaisten vaitiolovelvollisuus.* Ehdotuksella lisättäisiin tietosuojavaltuutetun vaitiolovelvollisuuden piiriin ehdotetussa 13 h §:n momentissa tarkoitetut yhteisötilaajan tunnistamistietojen käsittelystä tietosuojavaltuutetulle annettavat selvitykset.

Ehdotuksella jätettäisiin voimassa olevan lain 34 §:n 1 ja 5 momentti 34 §:ään ja siirrettäisiin 2, 3 ja 4 momentti 34 a §:ään. Kyse on teknisestä muutoksesta.

34 a §. *Valvontaviranomaisten tietojen luovuttaminen.* Ehdotuksella siirrettäisiin voimassa olevan lain 34 §:n 2, 3 ja 4 momentti 34 a §:ään. Kyse on lähinnä teknisestä muutoksesta. Samalla lisättäisiin 34 a § 1 momentissa Viestintävirastolle oikeus salassapitosäännöksen tai muun tietojen luovuttamiskiellon estämättä luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja niille teleyrityksille, lisäarvopalvelun tarjoajille ja yhteisötilaajille, joihin todennäköisesti voi kohdistua tietoturvaloukkaus. Tällöin Viestintävirasto voisi esimerkiksi luovuttaa tiedon siitä IP-osoitteesta, josta tietoturvaan kohdistuva hyökkäys on toteutettu, säännöksessä luetelluille tahoille, jotka puolestaan voivat estää kyseisestä osoitteesta tulevan hyökkäyksen järjestelmissään.

Lisäksi Viestintävirastolle säädettäisiin uuden 3 momentin mukaan oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja muissa valtioissa toimiville organisaatioille, joiden tehtävänä on ennalta ehkäistä viestintäverkkoihin ja -palveluihin kohdistuvia tietoturvaloukkauksia. Kyse on Viestintäviraston CERT-FI (Computer Emergency Response Team FICORA) ryhmää vastaavista muiden valtioiden tietoturvaloukkauksia tai havainnointia koordinoivista tahoista, joiden tehtävinä on tietoturvaloukkauksien ennaltaehkäisy, niiden havainnointi ja ratkaisu sekä tietoturvauhkista tiedottaminen.

Tietojen luovuttaminen edellä mainituille tahoille olisi sallittua ehdotetun 4 momentin mukaan ainoastaan siinä laajuudessa kuin on välttämätöntä tietoturvaloukkauksen ennaltaehkäisemiseksi tai torjumiseksi. Tietojen luovuttamisella ei saisi rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Viestintäverkkoihin ja -palveluihin kohdistuvissa tai niiden avulla toteutetuissa tietoturvaloukkaustilanteissa loukkausten ennaltaehkäiseminen sekä jo tapahtuneiden loukkausten selvittäminen on usein mahdotonta pelkästään suomalaisilta toimijoilta saatavilla olevien tietojen perusteella, koska loukkauksen alullepanija käyttää toimintaansa Suomen rajojen ulkopuolella olevia laitteita. Esimerkiksi niin kutsutuissa phishing tapauksissa yksikään huijausviestejä lähettänyt tietokone ei ole ollut suomalaisessa verkossa. Haittaohjelmilla saastutettua konetta käytetään huijausviestien lähettämisen lisäksi usein myös haittaohjelmien jakeluun, verkko- ja viestintäpalveluihin taikka muihin verkon kautta tarjottaviin palveluihin kohdistuvien palvelunestohyökkäysten tekemiseen sekä tietoturvaloukkauksen tekijän jälkien piilottamiseen. Näiden oikeudettomasti hallintaan otettujen koneiden avulla toteutettujen tietoturvaloukkausten torjumiseksi on vält-

tämätöntä välittää saastuneita koneita koskevia tietoja kohdevaltion viestintäverkkojen ja -palveluiden tietoturvasta vastaaville organisaatioille.

Tietoturvaloukkausten ennaltaehkäisemiseksi vaihdettavat tiedot ovat tyypillisesti sellaisia tietoja, joita ei esimerkiksi Suomessa voida yhdistää ketään luonnollista henkilöä koskeviksi. Mahdollista on, että ulkomailla ne voidaan yhdistää johonkin laitteeseen ja sitä kautta mahdollisesti tuota laitetta hallinnoivaan henkilöön taikka organisaatioon. Usein viestintäverkkoihin ja -palveluihin kohdistuvaa hyökkäystä tai muuta tietoturvaloukkausta palveleva laite on myös oikeudettomasti toisen hallussa eli käytännössä laitteen oikea omistaja ei edes ole tietoinen siitä, että laitetta käytetään tietoturvaloukkausten toteuttamiseen. Tämän kaltaisissa tilanteissa on tietoturvaloukkausten torjumiseksi ja ennaltaehkäisemiseksi välttämätöntä ja oikeasuhtaista luovuttaa tietoja muiden valtioiden tietoturvaloukkausten selvittämistä koordinoiville tahoille, jotta ne voivat välittää tietoa uhkista ja tietoturvaloukkauksiin kytketyistä järjestelmistä oman valtionsa teleyrityksille ja yhteisötilaajille.

Tietojen luovuttamiseen tulisi lähtökohtaisesti pyytää suomalaisen viestinnän osapuolen suostumus, esimerkiksi tietoturvaloukkauksen kohteeksi joutuneen organisaation suostumus. Joissain tapauksissa on kuitenkin välttämätöntä luovuttaa tietoja myös viestintää välittävistä järjestelmistä muutoinkin. Esimerkiksi automaattisilla tunkeutumisen havainnointijärjestelmillä voidaan kerätä tietoja, joista ei yksiselitteisesti voida tunnistaa viestinnän vastaanottajaksi tarkoitettua. Kyse voi olla myös teleyrityksen yleisen viestintäpalvelun tarjoamiseen käytettäviin laitteisiin kertyneistä tiedoista, jotka ovat tietoturvaloukkausten lähdeosoitteita. Tällöinkään luovutettavia tietoja ei voida tunnistaa ketään suomalaista henkilöä koskeviksi. Tarpeellista ei yleensä ole luovuttaa tietoa hyökkäyksen kohteesta, vaan sen lähteestä.

Ehdotettuun 4 momenttiin lisättäisiin, että myös 3 momentissa tarkoitettu oikeus luovuttaa tunnistamistietoja rajoittuisi laajuudeltaan ainoastaan siihen kuin on tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi. Tämän lisäksi luovuttamisella ei saisi rajoittaa luottamuksellisen viestin suojaa enempää kuin on välttämätöntä.

42 §. *Rangaistussäännökset.* Ehdotuksella lisättäisiin lain rangaistussäännöksen 1 momenttiin säännös, jonka mukaan rangaistus 13 g §:n 3 momentissa tarkoitetun työntekijöiden salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 2 §:n 2 momentin mukaan, jollei teosta muualla kuin rikoslain 38 luvun 1 §:ssä säädetä ankarampaa rangaistusta.

Pykälän 2 momenttiin lisättäisiin uusi 9 kohta, jolla säädettäisiin rangaistavaksi sähköisen viestinnän tietosuojarikkomuksena tunnistamistietojen käsittelyn lainmukaisuuden takaavien jälkikäteisten velvoitteiden laiminlyönti.

Yhteisötilaajan tulee täyttää nämä velvoitteet vain, jos hän tulee käsittelemään tunnistamistietoja 13 a–13 j §:ssä tarkoitetulla tavalla. Jos yhteisötilaaja ei tule käsittelemään tunnistamistietoja, hänen ei tarvitse myöskään täyttää 13 a–13 j §:ssä tarkoitettuja velvollisuuksia, eikä niiden toimittamatta jättäminen ole tällöin rangaistavaa.

Ehdotetun uuden 9 kohdan mukaan rangaistavaa olisi 13 f §:ssä tarkoitetun tunnistamistietojen käsittelystä laadittavan selvityksen laatimatta jättäminen tai sen jättäminen antamatta käyttäjälle.

Rangaistavaa olisi myös 13 g §:ssä tarkoitetun työntekijöiden edustajille tunnistamistietojen käsittelystä annettavan selvityksen sekä 13 h §:n 1 kohdassa tarkoitetun tietosuojavaltuutetulle annettavien ennakkoilmoituksen ja 2 momentissa tarkoitetun vuosittaisen selvityksen laiminlyönti.

Tunnistamistietojen lainmukaisuuden takaavien velvoitteiden laiminlyönti olisi rangaistavaa vain tahallisena.

1.2 Laki yksityisyyden suojasta työelämässä

2 §. *Soveltamisala.* Yksityisyyden suojasta työelämässä annetun lain soveltamisalasäännökseen esitetään selventävää viittaussäännöstä sähköisen viestinnän tietosuojalakiin.

21 §. *Yhteistoiminta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä.* Yhteistoiminnassa käsiteltäviin asioihin esitetään lisättäväksi sähköisen viestinnän tietosuojalakiin esitettyjen uusien 13 a–

13 j §:n edellyttämällä tavalla sähköpostin ja muuta sähköistä viestintää koskevien tunnistamistietojen käsittely. Yhteistoimintamenettelyn ja tiedottamisen piiriin kuuluisivat sähköisen viestinnän tietosuojalain 13 a–13 j §:ssä tarkoitetut viestintäverkkojen ja palvelujen käytöstä ja yrityssalaisuuksien käsittelystä annetut ohjeet, tilanteet, joissa käsittely on mahdollista, automaattisen haun yleiset toimintaperiaatteet ja ne tehtävät, joissa tunnistamistietoja voidaan käsitellä.

Yhteistoimintamenettelyssä tulisi käsitellä myös 20 §:ssä tarkoitettujen tietoturvatoimenpiteiden toteuttamisessa noudatettavat keskeiset periaatteet ja käytännöt.

Lisäksi pykälään esitetään lisättäväksi viittaus työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annettuun lakiin, Viittaus on tarpeen sen selventämiseksi, että yllä kuvattujen tunnistamistietojen käsittelyyn liittyvien seikkojen ottaminen käsiteltäväksi yhteistoimintamenettelyssä koskee myös kuntia.

1.3 Laki yhteistoiminnasta yrityksissä

19 §. *Muuhun lainsäädäntöön perustuvien suunnitelmien, periaatteiden ja käytäntöjen käsittely.* Pykälän 4 kohtaan esitetään lisättäväksi sähköisen viestinnän tietosuojalakiin esitettyjen uusien 13 a–13 j §:n edellyttämällä tavalla sähköpostin ja muuta sähköistä viestintää koskevien tunnistamistietojen käsittely.

Yhteistoimintamenettelyssä tulisi käsitellä myös 20 §:ssä tarkoitettujen tietoturvatoimenpiteiden toteuttamisessa noudatettavat keskeiset periaatteet ja käytännöt.

1.4 Laki yhteistoiminnasta valtion virastoissa ja laitoksissa

7 §. *Yhteistoimintamenettelyn piiriin kuuluvat asiat.* Pykälän 11 a kohtaan esitetään lisättäväksi sähköisen viestinnän tietosuojalakiin esitettyjen uusien 13 a–13 j §:n edellyttämällä tavalla sähköpostin ja muuta sähköistä viestintää koskevien tunnistamistietojen käsittely.

Yhteistoimintamenettelyssä tulisi käsitellä myös 20 §:ssä tarkoitettujen tietoturvatoimenpiteiden toteuttamisessa noudatettavat keskeiset käytännöt.

2 Voimaantulo

Lait ehdotetaan tulemaan voimaan 1 päivänä tammikuuta 2009. Esityksessä ehdotetaan muutettavaksi teleyrityksiin, yhteisötilaajiin ja lisäarvopalveluiden tarjoajiin kohdistuvaa sääntelyä. Niille on varattava riittävän pitkä aika henkilöstön kouluttamiseksi ja ohjeistamiseksi sekä tarvittavien menettelyjen läpikäymiseksi.

3 Suhde perustuslakiin ja säätämisjärjestys

Ehdotettuja säännöksiä tulee tarkastella perustuslaissa säädettyjen perusoikeuksien näkökulmasta. Lakiehdotuksessa luottamuksellisen viestin salaisuuteen ja yksityisyyden suojaan liittyvät säännökset ovat ehdotetuissa 9, 12, 12 a, 13, 13 a–13 j ja 14 §:ssä, joissa säädettäisiin tunnistamistietojen käsittelystä sekä 20 §:ssä, jossa säädettäisiin oikeudesta toteuttaa tiettyjä toimenpiteitä tietoturvasta huolehtimiseksi. Ehdotetuista säännöksistä yhteisötilaajien tunnistamistietojen käsittelyä koskevia uusia 13 a–13 j §:ää ja tietoturvaa koskevaa 20 §:ää on syytä tarkastella perusoikeuksien kannalta yksityiskohtaisesti.

Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu ja henkilötietojen suojasta säädetään tarkemmin lailla. Viestinnän luottamuksellisuus on perustuslain 10 §:n 2 momentin nojalla jokaiselle kuuluva perusoikeus. Momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

Kyseiset suojeltavat oikeushyvät eivät kuitenkaan ole ehdottomia, sillä niitä joudutaan tietyissä tilanteissa rajoittamaan. Perustuslain 10 §:n 3 momentin mukaan lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenestyksen aikana. Nämä mahdollisuudet rajoittaa luottamuksellisen viestin suojaa on perusoikeusuudistuksen yhteydessä tarkoitettu

tyhjentäväksi luetteloksi (HE 309/1993 vp, s. 54).

Perustuslain 10 §:n 3 momentin säännös on valtuutustyyppinen lakivaraus, joka sisältää samalla lainsäätäjän toimivaltaa rajoittavia säännöksiä. Säännöksessä on annettu lainsäätäjälle valta säätää tavallisella lailla välttämättömiä rajoituksia muun muassa viestintäsalaisuuteen rajoituslausekkeessa mainittujen yksilön tai yhteiskunnan turvallisuutta vaarantavien rikosten tutkintaan liittyvässä tarkoituksessa.

Luottamuksellisen viestin salaisuuden suojan ensisijaisena tarkoituksena on perusoikeusuudistuksen esitöiden mukaan suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta. Sääntely antaa kuitenkin turvaa muillekin tällaista viestiä koskeville tiedoille, joilla voi olla merkitystä viestin säilymiselle luottamuksellisena. Esimerkkinä perusteluissa on mainittu puhelujen tunnistamistiedot (HE 309/1993 vp, s. 53). Viestin tunnistamistietojen on perustuslakivaliokunnan vakiintuneen käytännön mukaan katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (PeVL 47/1996 vp, s. 4/I, PeVL 7/1997 vp, s. 2/I, PeVL 26/2001 vp, s. 3/II, PeVL 9/2004 vp, s. 4/I, PeVL 10/2004 vp, s. 4/II, PeVL 16/2004 vp, s. 6/I ja PeVL 23/2006 vp, s. 3/I).

Perustuslain 10 § 3 momentin lakivarauksen suhde viestien tunnistamistietoihin ei ole ehdoton. Hallituksen näkemyksen mukaan, perustuslakivaliokunta on katsonut, että oikeutta saada tieto viestin tunnistamistiedoista ei tule arvioida perustuslain 10 § 3 momentin lakivarauksen, vaan perusoikeuksien yleisten rajoittamisedellytysten valossa.

Telemarkkinalain muuttamista koskevassa lausunnossaan perustuslakivaliokunta (PeVL 47/1996 vp, s. 4/I) arvioi kysymystä telelaskun maksamiseen velvollisen oikeudesta saada tunnistamistiedot perusoikeuksien yleisten rajoittamisperusteiden valossa. Valiokunnan mukaan ehdotusta ei tullut arvioida suoraan suhteessa silloisen hallitusmuodon 8 §:n 3 momentissa sallittuihin rajoitusperusteisiin, jotka ainakin ensisijaisesti koskevat julkisen vallan taholta tulevia puuttumisia. Esitystä laiksi yksityisyyden suojasta työelämässä käsitellessään valiokunta arvioi työnantajan oikeutta selvittää, onko työntekijän sähköpostiosoitteeseen tämän poissa ollessa saapunut tai onko hän välittömästi ennen poissaoloaan lähettänyt tai vastaanottanut työnantajalle tarkoitettuja viestejä, joista työnantajan on toimintojensa järjestämisen tai turvaamisen takia välttämätöntä saada tieto. Valiokunta katsoi, että työnantajaa ei voitu pitää sellaisena ulkopuolisena tahona, jota vastaan perustuslain 10 §:n säännöksillä luottamuksellisen viestin salaisuudesta on tarkoitus antaa suojaa (PeVL 10/2004 vp, s. 5/II). Valiokunnan mukaan esityksessä ehdotettujen luottamuksellisen viestinnän salaisuuden rajoituksia oli arvioitava perusoikeuksien yleisten rajoitusedellytysten kannalta.

Yhteisötilaaja, joka usein on myös työnantaja, saisi ehdotettujen 13 a–13 j §:n mukaan tietyin edellytyksin selvittää perustellun epäilyn siitä, onko hänen viestintäverkkoaan käytetty luvattomasti tai onko sen kautta annettu luvattomasti tieto elinkeinotoiminnan kannalta keskeisistä yrityssalaisuuksista. Yhteisötilaaja omistaa omat viestintäverkkonsa ja viestintäpalvelunsa, eikä ole verkostaan välitettävään viestintään nähden samalla tavoin ulkopuolinen taho kuin esimerkiksi teleyritys tai julkista valtaa käyttävä poliisi.

Yhteisötilaaja antaa viestintäpalvelut käyttäjiensä, kuten työntekijöiden, käytettäväksi. Yhteisötilaajien osalta viestintäpalveluiden antaminen käyttäjien käytettäväksi liittyy hyvin kiinteästi yhteisötilaajan pääasiallisen toiminnan mahdollistamiseen. Jos yhteisötilaaja on esimerkiksi yritys, merkittävä osa yhteisötilaajan välittämästä viestinnästä on sellaista, joka liittyy yrityksen toimintaan. Tällöin viestinnän osapuolena on yritys itse. Yhteisötilaaja ei myöskään saisi tunnistamistietoja ulkopuoliselta taholta, koska tiedot kerääntyvät yhteisötilaajan hallussa oleviin omiin laitteisiin. Perustuslakivaliokunta on todennut, että sähköisen viestinnän tietosuojalaki sääntelee pääasiassa yksityisten toimijoiden välisiä suhteita (PeVL 9/2004 vp, s. 2/I). Näin ollen hallitus katsoo, että 13 a–13 j §:ssä ehdotettua tunnistamistietojen käsittelyoikeutta ei tarvitse sitoa tiettyihin rikostunnusmerkistöihin. Ydinalueeseen kohdistumattomia rajoituksia luottamuksellisen viestin suojaan tulee tarkastella perusoikeuksien yleisten rajoitusedellytysten kannalta.

Kun yhteisötilaajan viestintäverkko tai viestintäpalvelu häiriintyy, vasta tunnistamistietojen käsittelyllä päästään selvittämään, onko kyse järjestelmän toimintahäiriöstä tai rikkoontumisesta vai onko joku käyttänyt väärin yhteisötilaajan viestintäverkkoa tai viestintäpalveluja. Jos yhteisötilaaja on joutunut rikoksen kohteeksi, on tunnistamistietojen käsittelyoikeuden salliminen perusteltua, jotta mahdollinen tutkintapyyntö voidaan laatia asianmukaisesti ja siten että taataan samalla toiminnan mahdollisimman häiriötön jatkuminen esitutkinnan aikana. Yrityssalaisuuksiin kohdistuvat rikokset ja luvaton käyttö ovat niin sanottuja asianomistajarikoksia. Rikoslain 28 luvun 15 §:n ja 30 luvun 12 §:n mukaan virallinen syyttäjä ei saa nostaa syytettä, ellei asianomistaja ilmoita rikosta syytteeseen pantavaksi taikka ellei erittäin tärkeä yleinen etu vaadi syytteen nostamista. Esitutkintalain (449/1987) 2 §:n mukaan poliisin tai muun esitutkintaviranomaisen on toimitettava esitutkinta, kun sille tehdyn ilmoituksen perusteella tai muutoin on syytä epäillä, että rikos on tehty. Oikeudenkäynnistä rikosasioissa annetun lain (689/1997) mukaan asianomistajalla on itsenäinen, toissijainen oikeus nostaa syyte häneen kohdistuneesta rikoksesta.

Esitystä valmisteltaessa arvioitiin seikkaperäisesti mahdollisuutta antaa väärinkäytösten selvittäminen yksin poliisin tehtäväksi. Yhteisötilaajien määrän, vikatilanteiden ja väärinkäytösten moninaisuuden, järjestelmien erilaisuuden, ja tehtävän vaatimien resurssien laajuuden vuoksi tätä vaihtoehtoa ei pidetty lainkaan toteuttamiskelpoisena. Kyse on yhteisötilaajien omien viestintäjärjestelmien päivittäiseen ylläpitoon liittyvistä tehtävistä, joista kunkin yhteisötilaajan on välttämätöntä huolehtia itse. Samalla yhteisötilaaja pystyisi rajaamaan mahdollisen poliisille osoitettavan esitutkintapyynnön niin, ettei esitutkinta (ml. poliisin haltuun tutkinnan ajaksi siirrettävät tietokoneet ja palvelimet) vaarantaisi koko yrityksen toiminnan jatkuvuutta. Rikosten esitutkinnan suorittaisi poliisi. Esityksellä ei siirrettäisi poliisin tehtäviä yrityksille.

Samalla on kuitenkin huomattava, että jos yhteisötilaaja käsittelee viestintäverkkonsa tai viestintäpalvelunsa ylläpitoon liittyvissä tehtävissä tai muutoin tunnistamistietoja lain vastaisesti, poliisilla on omat lainmukaiset toimivaltuudet suorittaa asiassa esitutkinta. Tämän lisäksi tietosuojavaltuutettu valvoisi yhteisötilaajien tunnistamistietojen käsittelyä. Tietosuojavaltuutetulla olisi oikeus velvoittaa rikkoja korjaamaan virheensä tai laiminlyöntinsä taikka asettaa velvoitteen noudattamisen tehosteeksi uhkasakon tai uhan, että tekemättä jätetty toimenpide teetetään asianomaisen kustannuksella.

Ehdotettujen 13 a–13 j §:n sääntely vaikuttaisi lähinnä yksityisten oikeussubjektien välisessä suhteessa. Tällöin perusoikeusarviossa korostuu perustuslain 22 §:n säädös julkisen vallan velvollisuudesta turvata perusoikeuksien toteutuminen. Tässä tapauksessa turvaamisvelvollisuus liittyy viestintäverkkojen ja viestintäpalvelujen käyttäjien sekä yhteisötilaajien oikeudet tasapainoisesti yhteen sovittavaan sääntelyratkaisuun. Arvio eri perusoikeuksien yhteensovittamisesta sisältyy arvioon ehdotettujen muutosten hyväksyttävyydestä perusoikeuksien yleisten rajoitusedellytysten kannalta.

Perusoikeuksien kannalta esityksessä on kyse yhteisötilaajien perustuslain 15 §:ssä säädetyn omaisuudensuojan ja 18 §:ssä säädetyn elinkeinonvapauden ja käyttäjien luottamuksellisen viestin salaisuuden yhteensovittamisesta. Sähköisten viestintäverkkojen ja viestintäpalvelujen käytön turvaamisen voidaan arvioida olevan varallisuusarvoinen etuus, joka nykyisessä viestintäkeskeisessä toimintaympäristössä lukeutuu perustuslaissa säädetyn omaisuudensuojan piiriin. Yhteisötilaajan elinkeinotoiminnan kannalta keskeisten yritys-salaisuuksien ja kehittämistyön tulosten luottamuksellisuuden varmistamisen voidaan niin ikään arvioida kuuluvan omaisuudensuojan ja elinkeinonvapauden piiriin. Perustuslakivaliokunta on käsitellyt omaisuudensuojaan liittyviä kysymyksiä muun muassa teletoimintalain muuttamisesta (PeVL 1/1996 vp), telemarkkinalain (PeVL 47/1996 vp, PeVL 34/2000 vp ja PeVL 5/2001 vp) sekä viestintämarkkinoita koskevan lainsäädännön (PeVL 8/2002 vp) muuttamisesta annettuja esityksiä käsitellessään.

Valiokunnan tähänastinen käytäntö voidaan tiivistää siten, että omaisuuden suojaan kohdistuvat erilaiset velvoitteet ovat omaisuuden erityisluonne huomioon ottaen perustuslain mukaisia, jos velvoitteet perustuvat lain täs-

mällisiin säännöksiin ja ovat omistajan kannalta kohtuullisia. Hallitus katsoo, että perustuslakivaliokunta on lausuntokäytännössään pitänyt keskeisenä sitä, että omistajan oma nykyinen ja kohtuullinen tuleva tarve rajoittavat omistajalle asetettavia velvollisuuksia. Sähköisen viestinnän tietosuojalain 4 §:ssä yhteisötilaajille asetettua viestinnän luottamuksellisuuden velvoitetta voidaan tarkastella myös yhteisötilaajien omaisuudensuojaa rajoittavana velvoitteena.

Sähköisen viestinnän tunnistamistietojen käsittelyoikeudesta ehdotetaan säädettäväksi lain tasoisella säädöksellä. Tunnistamistietojen käsittelyyn oikeuttavat tilanteet, käsittelyoikeuden rajat ja käsittelyn lainmukaisuuden varmistavat säännökset ehdotetaan sijoitettaviksi sähköisen viestinnän tietosuojalakiin. Ehdotukset täyttävät siten lailla säätämisen vaatimuksen.

Tunnistamistietojen käsittelyoikeuden edellytyksenä olisi, että viestintäverkon käyttö ja yrityssalaisuuksien luottamuksellisuus olisi ensisijaisesti pyrittävä takaamaan keinoilla, joissa ei puututa lainkaan viestinnän tunnistamistietoihin. Näitä keinoja ovat käyttäjähallinto- ja tietoturvatoimenpiteet ja käyttäjien ohjeistus.

Ehdotetut 13 a–13 j § oikeuttaisivat yhteisötilaajan käsittelemään tunnistamistietoja maksullisen tietoyhteiskunnan palvelun ja viestintäverkon luvattoman käytön tai viestintäpalvelun ohjeen vastaisen käytön selvittämiseksi Tapahtuman tai teon tulisi todennäköisesti aiheuttaa yhteisötilaajalle merkittävää haittaa tai vahinkoa. Säännöksissä on pyritty ennakoimaan tyypillisimmät viestintäverkon tai viestintäpalvelun ohjeen vastaisen tai luvattoman käytön tilanteet. Viestintätekniikan nopean kehityksen vuoksi kaikkia viestintäverkon tai viestintäpalvelun luvattoman käytön tilanteita ei ole mahdollista luetella tyhjentävästi. Tämän vuoksi tunnistamistietojen käsittely säännöksessä tarkoitettuihin esimerkkitapauksiin rinnastettavan muun viestintäverkon luvattoman käytön tai viestintäpalvelun ohjeen vastaisen käytön havaitsemiseksi on syytä sisällyttää säännökseen.

Ehdotuksen mukaan käyttäjiin nähden työnantaja-asemassa olevat yhteisötilaajat saisivat oikeuden tunnistamistietojen käsittelyyn yrityssalaisuuden paljastamisen selvittämiseksi. Epäillyn yrityssalaisuuden paljastamisen tulisi kohdistua yhteisötilaajan tai sen yhteistyökumppanin elinkeinotoiminnan kannalta keskeisiin yrityssalaisuuksiin taikka teknologisen tai muun kehitystyön tuloksiin, jotka todennäköisesti ovat merkittäviä elinkeinotoiminnan käynnistämisen tai sen harjoittamisen kannalta.

Ehdotetun 13 a–13 j §:n yrityssalaisuuden käsite on yhtenevä rikoslain 30 luvun 11 §:n yrityssalaisuuden käsitteen kanssa. Tunnistamistietojen käsittely olisi mahdollista vain, jos kyseessä olisivat elinkeinokeinotoiminnan käynnistämisen tai harjoittamisen kannalta keskeiset yrityssalaisuudet tai kehittämistyön tulokset. Säännöksen yksityiskohtaisissa perusteluissa esimerkkeinä on mainittu muun muassa tiedot, jotka antavat yritykselle kilpailuedun ja joita ei julkisista lähteistä ole selvitettävissä ja joiden käsittelystä ja suojaamisesta elinkeinonharjoittaja on laatinut erityiset ohjeet ja suojaamiskäytännöt. Ehdotetussa säännöksessä yrityssalaisuuden käsitteelle on asetettu rikoslakia korkeampi merkittävyystaso. Rikoslain esitöissä on todettu, että yrityssalaisuuden käsitteen laissa omaksuttua tarkempaan sisällölliseen rajaukseen ei ole tarvetta, koska elinkeinotoiminnassa tarvitaan mitä erilaatuisempaa kilpailijoilta suojattavaa tietoa (HE 66/1988 vp, s. 92).

Yrityssalaisuuksien osalta käsittelyoikeus kohdistuisi vain sellaisten henkilöiden tunnistamistietoihin, joilla on yhteisötilaajan hyväksymällä tavalla pääsy yrityssalaisuuksiin. Tunnistamistietojen käsittelyn edellytyksenä olisi erityisen yrityssalaisuuksien käsittelyohjeen laatiminen. Näin ollen ehdotettu käsittelyoikeus tulisi sovellettavaksi vain sellaisiin yhteisötilaajiin, joiden normaaliin toimintaan säännöksessä tarkoitettujen yrityssalaisuuksien käsittely kuuluu.

Ehdotetuissa 13 a–13 j §:ssä esitetyt käsittelyoikeudet on rajattu koskemaan vain yhteisötilaajien toiminnan olennaisesti vaarantavia uhkia. Käsiteltäväksi saisi ottaa vain ne tiedot, jotka ovat välttämättömiä väärinkäytöksen selvittämiseksi. Lähtökohtaisesti tunnistamistietoja saisi käsitellä automaattisen hakutoiminnon avulla ennakolta määriteltyjen hakuperusteiden perusteella. Automaattisessa haussa yksittäisten viestintäverkon käyttäjien viestien tunnistamistiedot eivät tulisi kenenkään

ulkopuolisen henkilön tietoon. Automaattisen haun tarkoituksena on erottaa manuaalisesti käsiteltäväksi vain väärinkäytöksiin liittyvien viestien tunnistamistiedot. Tavanomaisten viestien tunnistamistiedot eivät tällöin altistuisi käsittelylle. Pelkän automaattisen hakutoiminnon avulla tehtävän tunnistamistietojen käsittelyn ei voida katsoa puuttuvan niiden viestintää harjoittavien luottamuksellisen viestin suojaan, joiden viestintää koskevia tunnistamistietoja ei lainkaan oteta luonnollisen henkilön tekemään manuaaliseen käsittelyyn.

Tunnistamistiedot saisi ottaa yksittäistapauksessa manuaaliseen käsittelyyn vain, jos on perusteltu syy epäillä väärinkäytöksen tapahtuneen. Perusteltu syy olisi automaattisessa hakutoiminnossa sallituissa hakukriteereissä havaittu poikkeama tai 13 d §:ssä yksilöity seikka.

Ehdotettu käsittelyoikeus kohdistuisi vain yhteisötilaajan omiin järjestelmiin kertyviin tunnistamistietoihin. Internetissä toimivien suojattujen sähköposti- ja verkkopankkipalveluiden käytöstä selviäisi ainoastaan käytetyn palvelun osoite, käyttämisaika ja käytön kesto. Yhteisötilaajilla on mahdollisuus halutessaan estää ulkopuolisten tarjoamien palvelujen käyttö omista järjestelmistään. Puhelinpalveluihin liittyvät tunnistamistiedot on rajattu käsittelyoikeuden ulkopuolelle. Käsittelyoikeus ei anna oikeutta puuttua viestien sisältöön.

Perustuslakivaliokunta kiinnitti huomiota sähköisen viestinnän tietosuojalain esityksen yhteydessä käsittelyn määritelmän laaja-alaisuuteen (muun muassa PeVL 9/2004 vp, s. 3/I). Valiokunta totesi kuitenkin, että ehdotuksen 8 §:n 3 momentin tarkoitussidonnaisuuden vaatimus lieventää laaja-alaiseen käsittelyn määritelmään liittyviä ongelmia. Mainittu 8 §:n 3 momentti rajoittaisi ja ohjaisi myös ehdotettujen säännösten nojalla tapahtuvaa tunnistamistietojen käsittelyä. Ehdotettua sääntelyä voidaan pitää säänneltävä asiakokonaisuus huomioon ottaen tarkkarajaisena.

Ehdotetulla 13 a–13 j §:n mukaisella tunnistamistietojen käsittelyoikeudella pyritään turvaamaan yhteisötilaajien viestintäverkkojen ja palvelujen käyttö niille suunniteltuun tarkoitukseen. Sähköisten viestintäverkkojen ja palvelujen käytön turvaamisen voitaneen arvioida olevan varallisuusarvoinen etuus, joka nykyisessä viestintäkeskeisessä toimintaympäristössä lukeutuu perustuslain 15 §:ssä säädetyn omaisuudensuojan piiriin. Useimmille yhteisötilaajille mahdollisuus käyttää viestintäverkkoaan ja viestintäpalveluitaan on niiden toiminnan edellytys. Vähäistä haittaa aiheuttava luvaton tai ohjeiden vastainen käyttö ei oikeuttaisi tunnistamistietojen käsittelyyn, vaan käsittelyoikeus on rajattu vain sellaisiin väärinkäytöksiin, jotka aiheuttavat yhteisötilaajalle merkittävää haittaa. Väärinkäytöksen tulee vaarantaa, vaikeuttaa tai hidastaa viestintäverkon tai -palvelujen käyttöä niille suunniteltuun käyttötarkoitukseen. Tilanteessa, jossa on kysymys yhteisötilaajan varallisuuspiirin kuuluvan verkon luvattomasta käyttämisestä, voidaan yhteisötilaajalla katsoa olevan perusoikeusjärjestelmän kannalta hyväksyttävä intressi suojata omaisuuttaan luvattomalta käyttämiseltä.

Ehdotetulla 13 a–13 j §:n mukaisella tunnistamistietojen käsittelyoikeudella pyritään suojaamaan myös teknologisen tai muun kehittämistyön tuloksia ja elinkeinotoiminnan kannalta keskeisiä yrityssalaisuuksia. Yhteisötilaajan elinkeinotoiminnan kannalta keskeisten yrityssalaisuuksien ja kehittämistyön tulosten luottamuksellisuuden varmistamisen voidaan niin ikään arvioida kuuluvan perustuslain 15 §:ssä säädetyn omaisuudensuojan sekä perustuslain 18 §:ssä säädetyn elinkeinon vapauden piiriin. Yrityksen elinkeinotoiminnan kannalta merkittävien kehitystyön tulosten tai keskeisten yrityssalaisuuksien oikeudettomalla paljastamisella saattaa olla yritykselle hyvin laaja-kantoiset seuraukset, jotka voivat äärimäisessä tapauksessa johtaa toiminnan lakkaamiseen. Yrityssalaisuuksien paljastaminen voi välillisesti vaikuttaa kielteisesti koko kansantalouden kehittymiseen. Yrityssalaisuuksien luottamuksellisuuden turvaamisen voidaan katsoa olevan perusoikeusjärjestelmän kannalta hyväksyttävä intressi.

Ehdotetuissa 13 a–13 j §:ssä esitetyt yhteisötilaajien tunnistamistietojen käsittelyoikeuksien muutokset eivät antaisi oikeutta ottaa selville viestien sisältöjä. Pelkkiin viestien tunnistamistietoihin rajautuva käsittelyoikeus ei ulottuisi luottamuksellisen viestin salaisuuden ydinalueelle.

Yhteisötilaajilla on perusteltu tarve turvata viestintäverkkojensa ja viestintäpalveluidensa käyttö niiden oman toimintansa tarpeisiin. Yh-

teisötilaajilla on myös perusteltu tarve turvata omien ja yhteistyökumppaneidensa yrityssalaisuuksien luottamuksellisuus. Aineeton omaisuus, kuten kehitteillä olevat tuotteet ja palvelut, tietotaitoon perustuvat toimintatavat ja muut yrityssalaisuudet saattavat muodostavat etenkin korkean teknologian yritysten varallisuudesta merkittävän osan.

Ehdotetun sääntelyn mukaan ensisijaisena keinona viestintäverkon ja viestintäpalveluiden suojaamisessa ja yrityssalaisuuksien luottamuksellisuuden turvaamisessa olisivat keinot, joilla ei puututa käyttäjien viestintään. Näitä ovat verkkojen käyttäjille annetut ohjeet ja tietoturvatoimenpiteet. Lähtökohtaisesti tunnistamistietoja saisi käsitellä automaattisen hakutoiminnon avulla. Hakutoiminnon määrittelyn perusteella ihmisvoimin käsiteltäviksi erottuisivat vain kooltaan, tyypiltään tai muutoin poikkeuksellisten viestien tunnistamistiedot.

Viestintäverkkojen ja viestintäpalveluiden ohjeiden mukainen käyttö voidaan turvata vain osaksi tietohallinnollisin toimenpitein. Väärinkäytösten selvittäminen edellyttää kuitenkin myös tunnistamistietojen käsittelyä. Yrityssalaisuuksien oikeudettoman paljastamisen selvittämisessä ovat myös käytettävissä tietohallinnolliset keinot, kuten käyttäjätietolokien tarkastaminen, pääsyä rajoittaviin järjestelmiin kirjautuvien tietojen tarkastaminen sekä järjestelmien teknisessä ylläpidossa kerätyt tiedot. Näistä tiedoista käy ilmi, kuka on tallentanut mitäkin tietoja, missä muodossa, koska ja mille tallenteelle, kuten kovalevylle tai siirrettävälle tallenteelle. Siirrettäviä tallenteita ovat esimerkiksi muistitikut ja cd-levyt. Myös aineiston muuta käsittelyä, kuten tulostamista koskevat tiedot, voidaan tallentaa. Näiden tietojen käsittelylle sähköisen viestinnän tietosuojalaissa ei aseteta rajoituksia. Toisaalta näiden tietojen avulla pystytään vain poikkeuksellisesti selvittämään yrityssalaisuuden paljastaminen kokonaisuudessaan.

Ehdotukseen sisältyy useita yhteisötilaajille esitettyjä velvollisuuksia, jotka varmistaisivat tunnistamistietojen käsittelyn lainmukaisuuden ja näin mahdollisimman vähäisen puuttumisen viestinnän luottamuksellisuuteen. Tunnistamistietojen käsittelyoikeuden rajauksilla käsittelyoikeus on kohdennettu vain väärinkäytöksiin liittyvien viestien tunnistamistietoihin. Tunnistamistietoja käsiteltäessä paljastuu myös tieto viestin vastaanottajasta. Perustuslakivaliokunta ei pitänyt ongelmallisena yksityisyyden suojasta työelämässä annetun esityksen perusteluissa (HE 162/2003 vp, s. 70) mainittua seikkaa, että työnantajalle kuuluvien viestien erottelussa nähtäväksi tulevat myös luottamuksellisiksi tarkoitettujen sekä lähetettyjen että vastaanotettujen viestien osapuolia ja otsikkoja koskevat tiedot. Tässä esityksessä yhteisötilaajan tietoon tulisivat vain niiden väärinkäytöksiin liittyvien viestien osapuolia koskevat tiedot, jotka otetaan manuaalisesti käsiteltäviksi.

Tunnistamistietojen käsittelyssä noudatettavat menettelyt ja käytännöt on ilmoitettava käyttäjille. Käyttäjille annettavien tietojen perusteella heillä on itse mahdollisuus vaikuttaa siihen, altistuuko tieto viestin vastaanottajasta mahdollisesti käsittelylle.

Ehdotettuun käsittelyoikeuteen liittyvät menettelyt sekä tietosuojavaltuutetun valvontasuoritteiden maksullisuus myös osaltaan ohjaavat yhteisötilaajia siten, että käsittelyoikeuteen turvaudutaan vain jos se on välttämätöntä.

Ehdotettu tunnistamistietojen käsittelyoikeus on välttämätön, jotta yhteisötilaajat voisivat nopeasti selvittää epäillyn viestintäjärjestelmiensä luvattoman tai ohjeen vastaisen käytön sekä yrityssalaisuuksien luvattoman paljastamisen. Yrityssalaisuuksien osalta tietohallinnollisten toimien avulla pystytään alustavasti rajaamaan epäilyksen alaisten joukkoa selvittämällä ketkä ovat tietoja käsitelleet. Tunnistamistietojen käsittely on välttämätöntä, jotta saadaan tieto siitä, onko joku ollut yhteydessä esimerkiksi tahoon, jolle yrityssalaisuus on luvatta annettu. Samalla yhteisötilaaja pystyisi rajaamaan epäiltyjen piiriä ja näin turvaamaan toimintansa jatkumisen.

Ilman ehdotettua käsittelyoikeutta yhteisötilaajat eivät pysty tarvittaviin toimenpiteisiin yrityssalaisuuksiin liittyvien väärinkäytösten havaitsemiseksi ja niiden aiheuttamien vahinkojen torjumiseksi tai rajoittamiseksi. Ehdotuksen mukaan tunnistamistietoja saisi käsitellä vain tilanteissa, jotka saattavat vahingoittaa yksityisen elinkeinotoiminnan kannalta keskeistä yrityssalaisuutta tai viestintäjärjestelmien toimintaa. Rajoitukset ovat näin ollen välttämättömiä painavan yhteiskunnallisen tar-

peen saavuttamiseksi sekä laajuudeltaan oikeassa suhteessa perusoikeuksien suojaamiin oikeushyviin ja rajoitusten taustalla olevien yhteiskunnallisten intressien painoarvoon.

Tunnistamistietojen manuaalisessa käsittelyssä tunnistamistiedot tulisivat niitä käsittelevien henkilöiden tietoon. Tällaisesta käsittelystä tulisi aina laatia ehdotetun 13 f §:n mukainen käsittelyyn osallistuneiden henkilöiden allekirjoittama selvitys, josta kävisi ilmi käsittelyn peruste ja syy, minkä vuoksi tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty. Selvityksestä olisi lisäksi käytävä ilmi käsittelyn ajankohta, kesto ja käsittelijät sekä käsittelystä päättänyt henkilö. Selvitys tulisi antaa viestintäverkon tai viestintäpalvelun käyttäjälle, heti kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta. Tunnistamistietojen käsittelyyn osallistuneita koskisi lain 5 §:n mukainen vaitiolovelvollisuus ja hyväksikäyttökielto.

Yhteisötilaajien tulisi myös toimittaa tietosuojavaltuutetulle vuosittain tunnistamistietojen manuaalisesta käsittelystä selvitys, josta kävisi ilmi, montako kertaa tunnistamistietoja on manuaalisesti käsitelty ja millä perusteella käsittelyyn on ryhdytty. Sama tieto tulisi työpaikoilla henkilöstöryhmien edustajille.

Ehdotettua käsittelyoikeutta valvova tietosuojavaltuutettu toimii virkavastuulla. Tietosuojavaltuutettu voi lain 41 §:n mukaan velvoittaa rikkojan korjaamaan virheensä tai laiminlyöntinsä taikka asettaa velvoitteen noudattamisen tehosteeksi uhkasakon tai uhan, että tekemättä jätetty toimenpide teetetään asianomaisen kustannuksella. Jos rikkomus on vakava, asetettava uhka voi koskea myös sitä, että toiminta keskeytetään osaksi tai kokonaan. Tietosuojavaltuutettu voi myös saattaa käsiteltävänään olevan asian esitutkinnan kohteeksi.

Tunnistamistietojen käsittely 13 a–13 j §:n ja 8 §:n käsittelysääntöjen vastaisesti täyttää rikoslain 38 luvun 3 §:ssä ja 4 §:ssä säädetyn viestintäsalaisuuden loukkaamisen tai törkeän viestintäsalaisuuden loukkaamisen tunnusmerkistön. Tunnistamistietojen käsittelyn asianmukaisuuden takaavien 13 b–13 c §:ssä tarkoitettujen ennakollisten velvoitteiden laiminlyönti täyttää lain 42 §:n 2 momentin 5 kohdassa tarkoitetun sähköisen viestinnän tietosuojarikkomuksen tunnusmerkistön. Ehdotetulla 42 §:n 2 momentin uudella 9 kohdalla säädettäisiin rangaistavaksi sähköisen viestinnän tietosuojarikkomuksena tunnistamistietojen käsittelyn lainmukaisuuden takaavien jälkikäteisten velvoitteiden laiminlyönti.

Ehdotettujen 13 a–13 j §:n mukaisessa tunnistamistietojen käsittelyssä on kyse samankaltaisesta tilanteista kuin yksityisyyden suojasta työelämässä annetussa laissa tarkoitetuissa kameravalvonnassa ja sähköpostiviestien esille hakemisessa ja avaamisessa. Nyt ehdotetuissa säännöksissä ei puututa viestin sisältöön. Perustuslakivaliokunta piti yksityisyyden suojasta annetun lain osalta riittävinä oikeusturvatakeina yhteistoimintamenettelyä, viranomaisvalvontaa sekä väärinkäytösten rangaistavuutta (PeVL 10/2004 vp, s. 4/I ja 5/II). Ehdotetun tunnistamistietojen käsittelyn oikeusturvatakeiden voidaan arvioida olevan verrattavissa yksityisyyden suojasta työelämässä annetun lain oikeusturvajärjestelyihin.

Ehdotetut muutokset ovat Suomea sitovien kansainvälisten ihmisoikeusvelvoitteiden mukaisia. Euroopan neuvoston ihmisoikeussopimus tai Euroopan neuvoston tietosuojasopimus eivät aseta rajoituksia ehdotetuille muutoksille. Myös EY:n sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohta sallii ehdotetun kaltaisen sääntelyn. Euroopan neuvoston ihmisoikeustuomioistuin on ottanut kannan viestinnän seurantaan 3 päivänä huhtikuuta 2007 antamassaan tuomiossa asiassa Copland v. Yhdistynyt kuningaskunta. Tapauksessa julkisen oppilaitoksen työntekijän puheluja, sähköposteja ja internetin käyttöä oli seurattu. Toiminnan salliva säädös tuli Yhdistyneessä kuningaskunnassa voimaan tapahtuneen seurannan jälkeen. Ihmisoikeustuomioistuin ei sinänsä sulkenut pois mahdollisuutta, että työntekijän puhelimen, sähköpostin ja internetin käytön valvonta voisi joissakin olosuhteissa olla Euroopan neuvoston ihmisoikeussopimuksessa tarkoitetulla tavalla välttämätöntä demokraattisessa yhteiskunnassa tavoiteltaessa hyväksyttävää päämäärää.

Perustuslakivaliokunta on tietoturvan osalta todennut, että tietoliikenteen ja tietoturvallisuuden vaarantumista voidaan nykyaikana pitää riskinä yksilön ja yhteiskunnan laajasti ymmärretyn turvallisuuden kannalta (PeVL 9/2004 vp, s. 4/I). Esitetty 20 §:n muutos saattaisi tietoturvasäännöksen vastaamaan nykyi-

siä tarpeita. Muutos on välttämätön, jotta teleyritykset, lisäarvopalvelun tarjoajat ja yhteisötilaajat voisivat tarkoituksenmukaisesti huolehtia häiriöiden poistamisesta, viestintämahdollisuuksien turvaamisesta ja maksuvälinepetosten ehkäisemisestä.

Perustuslakivaliokunta on pitänyt mahdollisena puuttumista viestien sisältöön tietoturvan varmistamiseksi tietyin tarkkarajaisuusedellytyksin (PeVL 9/2004 vp, s. 4/II). Tietoturvalliset viestintäyhteydet ovat välttämätön edellytys yhteiskunnan elintärkeiden toimintojen turvaamiseksi. Riittävien toimintamahdollisuuksien turvaaminen on välttämätöntä myös sananvapauden, hengen ja terveyden sekä omaisuuden suojan toteutumisen kannalta. Tietoturvauhkien jatkuva muuttuminen ja ongelmien vaikutusten laaja-alaistuminen tekee väistämättömäksi arvioida käytettävissä olevien toimenpiteiden tehokkuutta uudelleen.

Tehokkaan tietoturvasta huolehtimisen edellytyksenä on se, että viestejä voidaan analysoida automaattisesti. Tarkastelu tapahtuu tällöin automaattisesti ennalta määriteltyjen tekijöiden perusteella, eivätkä viestien sisällöt paljastu ulkopuolisille luonnollisille henkilöille. Kaikesta sähköpostiliikenteestä valtaosan arvioidaan olevan niin sanottua roskapostia. Tästä syystä automaattiseen tietojenkäsittelyyn perustuvien tietoturvatoimenpiteiden tulee olla käytettävissä aiempaa joustavammin, jotta viestintäverkkojen käyttäjien viestintämahdollisuudet voidaan turvata.

Ehdotetun 20 §:n 3 momentin mukaan kaikkein vakavimmissa tietoturvaa vaarantavissa tapauksissa viestin sisältöä saisi käsitellä myös manuaalisesti. Manuaalisesta käsittelystä tulisi ilmoittaa viestin lähettäjälle ja vastaanottajalle, ellei sillä vaarannettaisi tietoturvan toteutumista. Manuaalisesti käsiteltäväksi tulevat viestit olisivat haitallisia viestejä, jotka voivat sisältää esimerkiksi uuden automaattisille suodatuksille tuntemattoman haittaohjelman tai haitallisen käskyn.

Jos haitallisia viestejä ei saada poistettua, saattavat niiden sisältämät haittaohjelmat vaarantaa kaikkien verkon käyttäjien viestintämahdollisuudet sekä tietokoneille tallennettujen tietojen luottamuksellisuuden. Viestien manuaalinen käsittely olisi tarpeen tietoturvauhan lähteen tai hyökkäyksen toiminnallisuuden ja rakenteen selvittämiseksi. Haittaohjelmien sitomisesta rikoslakiin on syytä luopua, koska tällöin esimerkiksi teolta puuttuva tahallisuus asettaa toimenpiteiden käytön epävarmaksi.

Viestien automaattinen sisällöllinen analyysi ei altistaisi viestien tietoja ulkopuolisten henkilöiden tarkastelulle. Automaattinen analyysi on tehokas tapa huolehtia tietoturvasta mahdollisimman pienellä puuttumisella viestintään.

Ehdotettu tietoturvasäännöksen muutos on tarpeen, jotta tietoturvasta voidaan tarkoituksenmukaisesti huolehtia, ja jotta käyttäjien viestintämahdollisuudet ja tietosuoja voidaan turvata. Viestin sisältöön puuttuminen muuten kuin automaattisen tietojen käsittelyn keinoin on rajattu koskemaan tilanteita, joissa on ilmeistä, että viesti sisältää haittaohjelman tai haitallisen käskyn. Ilmoitusta viestin sisällön tutkimisesta ei ole syytä säätää kaikissa tilanteissa ehdottomaksi. Viesti saattaa esimerkiksi sisältää haitallisen koodin, joka lamauttaa tietojärjestelmiä. Koodin haitallisuudesta ilmoittaminen ei palvelisi verkkojen tai palvelujen tietoturvaa taikka viestin vastaanottajan viestintämahdollisuuksien turvaamista eikä luottamuksellisen viestin salaisuutta. Ilmoittaminen saattaisi päinvastoin tuottaa lisää ongelmatilanteita.

Ehdotetun muutoksen voidaan arvioida olevan tarkkarajainen. Puuttuminen haitallisten viestien sisältöön liittyy hyvin painavaan yhteiskunnalliseen intressiin. Perusoikeusjärjestelmän kannalta arvioiden ei ole painavaa intressiä suojata sellaisten viestien luottamuksellisuutta, joilla pyritään esimerkiksi saamaan oikeudetta selville käyttäjien tietoja tai ottamaan haltuun tietokoneita palvelunestohyökkäysten toteuttamiseksi. Puuttuminen viestin sisältöön on mahdollista vain, jos automaattisella analyysillä tietoturvasta ei pystytä huolehtimaan. Ehdotettu sääntely on oikeassa suhteessa perustuslaissa turvattujen yksityisyyden suojan ja luottamuksellisen viestin salaisuuden suojan kanssa. Tietoturvakäytännöt tulisi ottaa yhteistoimintamenettelyssä käsiteltäviksi, jolloin yhteisötilaajan soveltamat käytännöt tulisivat käyttäjien tietoon.

Säätämisjärjestyksen arviointi

Ehdotetuista tunnistamistietojen käsittelyoikeuksien muutoksista aiheutuvaa puuttumista luottamuksellisten viestien tunnistamistietoihin tulee arvioida perusoikeuksien yleisten rajoitusedellytysten kannalta. Ehdotettu sääntely on lain tasoista ja tarkkarajaista. Tunnistamistietoihin puuttumisella on hyväksyttävä syy, eivätkä rajoitukset ulottuisi luottamuksellisen viestin salaisuuden ydinalueelle. Viestintäverkkojen ja viestintäpalveluiden käyttö sekä yrityssalaisuudet tulisi ensisijaisesti turvata tietoturvasta huolehtimalla ja käyttäjille annettavilla ohjeilla. Tunnistamistietojen automaattisen käsittelyn avulla ja tietohallinnollisilla toimenpiteillä manuaalisesti käsiteltäviksi eroteltaisiin vain väärinkäytöksiin liittyvien viestien tunnistamistiedot.

Tunnistamistietojen käsittelyn menettelyistä ja käytännöistä tulisi tiedottaa käyttäjille. Tieto tunnistamistietojen manuaalisesta käsittelystä tulisi aina antaa käyttäjälle itselleen, kootusti tiedot tulisi ilmoittaa henkilöstön edustajille. Tunnistamistietojen käsittelyä valvoisi tietosuojavaltuutettu. Valvonta perustuisi ilmoituksiin ja tietosuojavaltuutetulla oleviin toimivaltuuksiin. Ehdotetun sääntelyn oikeusturvatakeet ovat asianmukaiset ja sääntely on yhdenmukaista Suomea sitovien ihmisoikeusvelvoitteiden kanssa.

Perustuslakivaliokunta on pitänyt mahdollisena puuttumista viestien sisältöön tietoturvan varmistamiseksi tietyin tarkkarajaisuusedellytyksin. Ehdotettu tietoturvasäännöksen muutos on tarkkarajainen ja oikeassa suhteessa perustuslaissa turvattujen yksityisyyden suojan ja luottamuksellisen viestin salaisuuden suojan kanssa. Edellä kerrotuilla perusteilla katsotaan, että lakiehdotukset voidaan käsitellä tavallisessa lainsäätämisjärjestyksessä. Kuitenkin pidetään tärkeänä, että esityksestä hankitaan perustuslakivaliokunnan lausunto.

Edellä esitetyn perusteella annetaan Eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

1.

Laki

sähköisen viestinnän tietosuojalain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 16 päivänä kesäkuuta 2004 annetun sähköisen viestinnän tietosuojalain (516/2004) 9, 12–14 20 ja 32 §, 33 §:n 3 momentin johdantokappale, 34 § ja 42 § sekä

lisätään lakiin uusi 12 a, 13 a–13 j ja 34 a § seuraavasti:

9 §

Tunnistamistietojen käsittely palvelujen toteuttamiseksi ja käyttämiseksi

Tunnistamistietoja saa käsitellä siinä määrin kuin se on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun toteuttamiseksi ja käyttämiseksi sekä jäljempänä säädetyllä tavalla tietoturvasta huolehtimiseksi.

Tunnistamistietoja saa käsitellä vain teleyrityksen, lisäarvopalvelun tarjoajan, yhteisötilaajan ja tilaajana olevan oikeushenkilön palveluksessa oleva sekä näiden lukuun toimiva luonnollinen henkilö, jonka tehtävänä on käsitellä tietoja tässä luvussa erikseen säädettyjen tarkoitusten toteuttamiseksi.

12 §

Käsittely teknistä kehittämistä varten

Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä tunnistamistietoja verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun teknistä kehittämistä varten.

Yhteisötilaaja voi käsitellä tunnistamistietoja oman viestintäverkkonsa ja siihen liitetyn oman palvelunsa teknistä kehittämistä varten.

Ennen 1 ja 2 momentissa tarkoitetun käsittelyn aloittamista tilaajalle tai käyttäjälle on ilmoitettava, mitä tunnistamistietoja käsitellään ja kuinka kauan niiden käsittely kestää. Ilmoitus voi olla kertaluonteinen.

12 a §

Käsittely tilastollista analyysiä varten

Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun tunnistamistietoja ja yhteisötilaaja voi käsitellä viestintäverkkonsa tai siihen liitetyn palvelunsa tunnistamistietoja automaattisen tietojenkäsittelyn avulla tilastollista analyysiä varten, jos:

1) analyysiä ei voida muuten tuottaa ilman kohtuutonta vaivaa; ja

2) analyysistä ei voida tunnistaa yksittäistä luonnollista henkilöä.

Mitä 1 momentissa, säädetään, koskee myös tilaajana olevan oikeushenkilön oikeutta käsitellä liittymänsä ja päätelaitteensa tunnistamistietoja.

13 §

Teleyrityksen ja lisäarvopalvelun tarjoajan käsittelyoikeus väärinkäytöstapauksissa

Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä tunnistamistietoja verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun maksullisen palvelun käyttöä maksutta tai muiden siihen rinnastuvien käyttöä koskevien väärinkäytösten havaitsemiseksi, estämiseksi ja selvittämiseksi.

Viestintävirasto voi antaa tarkempia määräyksiä 1 momentissa tarkoitetun tunnistamistietojen käsittelyn teknisestä toteuttamisesta.

13 a §

Yhteisötilaajan käsittelyoikeus väärinkäytöstapauksissa

Yhteisötilaajalla on oikeus käsitellä tunnistamistietoja maksullisen tietoyhteiskunnan palvelun tai viestintäverkon luvattoman käytön, viestintäpalvelun ohjeen vastaisen käytön taikka yrityssalaisuuksien paljastamisen selvittämiseksi siten kuin 13 b–13 j §:ssä säädetään.

Viestintäverkon luvatonta käyttöä tai viestintäpalvelun ohjeen vastaista käyttöä on laitteen, ohjelman tai palvelun asentaminen yhteisötilaajan viestintäverkkoon taikka muu näihin rinnastuva viestintäverkon tai viestintäpalvelun käyttö, jos se on käytöstä laadittujen 13 b §:n 3 momentissa tarkoitettujen ohjeiden vastaista.

Edellä 1 momentissa tarkoitettu oikeus ei koske kiinteän tai matkapuhelinverkon puhelinpalvelujen tunnistamistietoja.

13 b §

Yhteisötilaajan huolehtimisvelvollisuus väärinkäytöstapauksissa

Yhteisötilaajan on ennen tunnistamistietojen käsittelyn aloittamista maksullisen tietoyhteiskunnan palvelun tai viestintäverkon luvattoman käytön taikka viestintäpalvelun ohjeen vastaisen käytön ehkäisemiseksi:

1) rajoitettava pääsyä viestintäverkkoonsa ja viestintäpalveluunsa ja niiden käyttöön sekä ryhdyttävä muihin toimenpiteisiin viestintäverkkonsa ja viestintäpalvelunsa käytön suojaamiseksi asianmukaisin tietoturvallisuustoimenpitein; ja

2) määriteltävä, minkälaisia viestejä sen viestintäverkon kautta saa välittää ja hakea, sekä miten sen viestintäverkkoa ja viestintäpalvelua saa muutoin käyttää ja minkälaisiin kohdeosoitteisiin viestintää ei saa harjoittaa.

Yhteisötilaajan on ennen tunnistamistietojen käsittelyn aloittamista yrityssalaisuuksien paljastamisen ehkäisemiseksi:

1) rajoitettava pääsyä yrityssalaisuuksiin ja ryhdyttävä muihin toimenpiteisiin tietojen asianmukaiseksi suojaamiseksi; ja

2) määriteltävä, miten yrityssalaisuuksia saa viestintäverkossa siirtää, luovuttaa tai muutoin käsitellä ja minkälaisiin kohdeosoitteisiin yrityssalaisuuksia käsittelemään oikeutetut henkilöt eivät ole oikeutettuja lähettämään viestejä.

Yhteisötilaajan on 1 ja 2 momentissa tarkoitettujen väärinkäytösten ehkäisemiseksi annettava kirjalliset ohjeet viestintäverkon tai viestintäpalvelun käyttäjälle.

13 c §

Yhteisötilaajan suunnittelu- ja yhteistoimintavelvoite väärinkäytöstapauksissa

Yhteisötilaajan on ennen 13 a §:n 1 momentissa tarkoitetun tunnistamistietojen käsittelyn aloittamista nimettävä ne henkilöt, joiden tehtäviin tunnistamistietojen käsittely kuuluu tai määriteltävä mainitut tehtävät. Tunnistamistietoja voivat käsitellä vain yhteisötilaajan viestintäverkon ja viestintäpalvelun ylläpidosta ja tietoturvasta sekä turvallisuudesta huolehtivat henkilöt.

Jos yhteisötilaaja on yhteistoimintalainsäädännön piiriin kuuluva työnantaja, on hänen:

1) käsiteltävä 13 a–13 j §:ssä tarkoitetussa tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt yhteistoiminnasta yrityksissä annetun lain (334/2007) 4 luvussa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa (651/1988) ja työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa (449/2007) tarkoitetussa yhteistoimintamenettelyssä; ja

2) tiedotettava tunnistamistietojen käsittelystä tekemänsä päätökset työntekijöille tai heidän edustajilleen siten kuin yksityisyyden suojasta työelämässä annetun lain (759/2004) 21 §:n 2 momentissa säädetään.

Jos yhteisötilaaja on työnantaja, joka ei kuulu yhteistoimintalainsäädännön piiriin, on hänen kuultava työntekijöitä 2 momentin 1 kohdassa tarkoitetuista seikoista ja tiedotettava niistä työntekijöille siten kuin yksityisyyden suojasta työelämässä annetun lain 21 §:n 1 ja 2 momentissa säädetään.

Jos yhteisötilaaja ei ole työnantaja, on yhteisötilaajan tiedotettava käyttäjille 13 a–13 j §:ssä tarkoitetussa tunnistamistietojen käsittelyssä noudatettavista menettelyistä ja käytännöistä.

13 d §

Yhteisötilaajan käsittelyoikeuden edellytykset väärinkäytöstapauksissa

Yhteisötilaaja saa käsitellä tunnistamistietoja automaattisen hakutoiminnon avulla, joka voi perustua viestien kokoon, yhteenlasketuun kokoon, tyyppiin, määrään, yhteystapaan tai kohdeosoitteisiin.

Yhteisötilaaja saa käsitellä tunnistamistietoja manuaalisesti, jos on perusteltu syy epäillä, että viestintäverkkoa, viestintäpalvelua tai maksullista tietoyhteiskunnan palvelua käytetään 13 b §:n 3 momentissa tarkoitettujen ohjeiden vastaisesti tai että yrityssalaisuus on luvattomasti annettu ulkopuoliselle ja jos:

1) automaattisen hakutoiminnon avulla on havaittu viestinnässä poikkeama;

2) maksullisen tietoyhteiskunnan palvelun käytön kustannukset ovat nousseet epätavallisen korkeiksi;

3) viestintäverkossa havaitaan sinne oikeudetta asennettu laite, ohjelma tai palvelu;

4) yrityssalaisuus julkaistaan tai sitä käytetään luvatta; taikka

5) yhteisötilaajalla on yksittäistapauksessa muun 1–4 kohtaan rinnastuvan, yleisesti havaittavissa olevan seikan perusteella syy epäillä, että viestintäverkkoa, viestintäpalvelua tai maksullista tietoyhteiskunnan palvelua käytetään 13 b §:n 3 momentissa tarkoitettujen ohjeiden vastaisesti tai että yrityssalaisuus on luvattomasti annettu ulkopuoliselle.

Edellä 1 ja 2 momentissa tarkoitetun käsittelyn edellytyksenä on, että:

1) tapahtuma tai teko todennäköisesti aiheuttaa yhteisötilaajalle merkittävää haittaa tai vahinkoa; taikka

2) epäilty yrityssalaisuuden paljastaminen kohdistuu yhteisötilaajan tai sen yhteistyökumppanin elinkeinotoiminnan kannalta keskeisiin yrityssalaisuuksiin taikka teknologisen tai muun kehittämistyön tuloksiin, jotka todennäköisesti ovat merkittäviä elinkeinotoiminnan käynnistämisen tai sen harjoittamisen kannalta.

Edellä 2 momentissa tarkoitetun käsittelyn edellytyksenä on lisäksi, että tiedot ovat välttämättömiä väärinkäytöksen ja siitä vastuussa olevien selvittämiseksi sekä luvattoman tai ohjeen vastaisen käytön lopettamiseksi.

13 e §

Käsittelyoikeuden erityiset rajoitukset väärinkäytöstapauksissa

Automaattista hakua ei saa kohdistaa eikä tunnistamistietoja saa hakea esille eikä ottaa manuaalisesti käsiteltäviksi oikeudenkäymiskaaren 17 luvun 24 §:n 2 ja 3 momentissa tarkoitettujen tietojen selville saamiseksi.

Yrityssalaisuuksien paljastamisen selvittämiseksi työnantajana oleva yhteisötilaaja voi käsitellä vain sellaisten käyttäjiensä tunnistamistietoja, joille yhteisötilaaja on antanut tai joilla muutoin on yhteisötilaajan hyväksymällä tavalla pääsy yrityssalaisuuksiin.

13 f §

Yhteisötilaajan tiedonantovelvollisuus käyttäjälle väärinkäytöstapauksissa

Yhteisötilaajan on laadittava 13 d §:n 1 ja 2 momentissa tarkoitetusta manuaalisesta tunnistamistietojen käsittelystä selvitys, josta käy ilmi:

1) käsittelyn peruste, ajankohta ja kesto;

2) syy, minkä vuoksi tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty;

3) käsittelijät; sekä

4) käsittelystä päättänyt henkilö.

Käsittelyyn osallistuneiden henkilöiden on allekirjoitettava selvitys. Selvitys on säilytettävä vähintään kaksi vuotta 13 d §:ssä tarkoitetun käsittelyn päättymisestä.

Edellä 1 momentissa tarkoitettu selvitys on annettava tiedoksi käsittelyn kohteena olevan viestintäverkon tai viestintäpalvelun käyttäjälle heti, kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta. Selvitystä ei kuitenkaan tarvitse antaa niille käyttäjille, joiden tunnistamistietoja on käsitelty massamuotoisesti siten, että käyttäjien tunnistamistiedot eivät ole tulleet käsittelijän tietoon. Käyttäjällä on oikeus lakiin tai sopimukseen perustuvan salassapitovelvollisuuden estämättä luovuttaa selvitys ja sen yhteydessä saamansa tiedot etujaan tai oikeuksiaan koskevan asian käsittelyä varten.

13 g §

Yhteisötilaajan tiedonantovelvollisuus työntekijöiden edustajalle väärinkäytöstapauksissa

Jos yhteisötilaaja on työnantaja, sen on annettava työntekijöiden edustajalle vuosittain 13 d §:n 2 momentissa tarkoitetusta tunnistamistietojen manuaalisesta käsittelystä selvitys, josta on käytävä ilmi, millä perusteella ja kuinka monta kertaa tunnistamistietoja on vuoden aikana käsitelty.

Edellä 1 momentissa tarkoitettu selvitys on annettava työ- tai virkaehtosopimuksen perusteella valitulle luottamusmiehelle tai, jos tällaista ei ole valittu, työsopimuslain (55/2001) 13 luvun 3 §:ssä tarkoitetulle luottamusvaltuutetulle. Jos jonkin henkilöstöryhmän työntekijät eivät ole valinneet luottamusmiestä tai luottamusvaltuutettua, on selvitys annettava yhteistoiminnasta yrityksissä annetun lain 8 §:ssä tai työnantajan ja henkilöstön välisestä yhteistoiminasta kunnissa annetun lain 3 §:ssä tarkoitetulle yhteistoimintaedustajalle taikka yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain 6 §:n 2 momentissa tarkoitetulle edustajalle. Jos näitäkään ei ole valittu, selvitys on annettava kaikille tähän henkilöstöryhmään kuuluville työntekijöille.

Työntekijöiden edustajien ja 2 momentissa tarkoitettujen työntekijöiden on pidettävä salassa tietoonsa saamat yrityssalaisuuden loukkaukset ja epäilyt yrityssalaisuuden loukkaamisesta koko työsuhteen voimassaoloajan. Virkamiehen ja muun viranomaisen palveluksessa toimivan salassapitovelvollisuudesta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) ja muualla laissa säädetään. Mitä edellä säädetään, ei estä tietojen luovuttamista valvontaviranomaiselle.

13 h §

Ennakkoilmoitus ja vuosittainen selvitys tietosuojavaltuutetulle väärinkäytöstapauksissa

Yhteisötilaajan on ilmoitettava ennalta tietosuojavaltuutetulle tunnistamistietojen käsittelyn aloittamisesta. Ennakkoilmoituksesta on käytävä ilmi:

1) 13 d §:ssä tarkoitetussa tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt;

2) 13 c §:n 1 momentissa tarkoitetut tehtävät; ja

3) miten yhteisötilaaja on järjestänyt 13 c §:n 2 momentin 2 kohdassa tai 3 momentissa tarkoitetun käsittelyä edeltävän tiedottamisvelvollisuutensa.

Yhteisötilaajan on annettava tietosuojavaltuutetulle vuosittain jälkikäteen selvitys tunnistamistietojen manuaalisesta käsittelystä. Selvityksestä on käytävä ilmi, millä perusteella ja kuinka monta kertaa tunnistamistietoja on vuoden aikana käsitelty.

13 i §

Yhteisötilaajan oikeus säilyttää tunnistamistietoja väärinkäytöstapauksissa

Mitä 13 a–13 h §:ssä säädetään, ei oikeuta yhteisötilaajaa säilyttämään tunnistamistietoja rekisterissä kauempaa kuin lain mukaan muutoin on sallittua.

13 j §

Yhteisötilaajan oikeus tietojen luovuttamiseen väärinkäytöstapauksissa

Sen estämättä, mitä 8 §:n 3 momentissa säädetään, yhteisötilaajalla on oikeus luovuttaa asianomistajana tekemänsä rikosilmoituksen tai tutkintapyynnön yhteydessä poliisille käsiteltäviksi 13 a–13 i §:n mukaisesti saamansa yhteisötilaajan viestintäverkon tai viestintäpalvelun käyttäjän viestejä koskevat tunnistamistiedot.

14 §

Käsittely teknisen vian tai virheen havaitsemiseksi

Teleyritys, lisäarvopalvelun tarjoaja ja yhteisötilaaja voi käsitellä tunnistamistietoja, jos se on tarpeen viestinnän välittämisessä tapahtuneen teknisen vian tai virheen havaitsemiseksi, estämiseksi tai selvittämiseksi.

20 §

Toimenpiteet tietoturvan toteuttamiseksi

Teleyrityksellä, lisäarvopalvelun tarjoajalla ja yhteisötilaajalla sekä niiden lukuun toimivalla on oikeus ryhtyä 2 momentissa tarkoitettuihin välttämättömiin toimiin tietoturvasta huolehtimiseksi:

1) viestintäverkkojen tai niihin liitettyjen palvelujen tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;

2) viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi; tai

3) viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain (39/1889) 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.

Edellä 1 momentissa tarkoitetut toimet voivat käsittää:

1) viestin automaattisen sisällöllisen analyysin;

2) viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen;

3) tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä; sekä

4) muut näihin rinnastettavat teknisluonteiset toimenpiteet.

Jos viestin tyypin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn eikä viestin automaattisella sisällöllisellä analyysillä pystytä turvaamaan 1 momentissa tarkoitettujen tavoitteiden toteutumista, yksittäisen viestin sisältöä saa käsitellä manuaalisesti. Manuaalisesta viestin sisällön käsittelystä on ilmoitettava viestin lähettäjälle ja vastaanottajalle, ellei ilmoittamisella todennäköisesti vaaranneta 1 momentissa tarkoitettujen tavoitteiden toteutumista.

Tässä pykälässä tarkoitetut toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä 1 momentissa tarkoitettujen tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää ole tässä pykälässä säädettyjä edellytyksiä.

Viestintävirasto voi antaa teleyrityksille ja lisäarvopalvelun tarjoajille tarkempia määräyksiä tässä pykälässä tarkoitettujen toimenpiteiden teknisestä toteuttamisesta.

32 §

Tietosuojavaltuutetun tehtävät

Tietosuojavaltuutetun tehtävänä on valvoa:

1) 13 a–13 j §:ssä tarkoitettua yhteisötilaajan tunnistamistietojen käsittelyä;

2) 4 luvussa tarkoitettua paikkatietojen käsittelyä;

3) 25 §:ssä tarkoitettuja puhelinluetteloita ja muita tilaajaluetteloita sekä numerotiedotusta koskevien säännösten noudattamista;

4) 7 lukuun sisältyvien suoramarkkinointia koskevien säännösten noudattamista;

5) 9 lukuun sisältyvien tiedonsaantioikeuksia ja vaitiolovelvollisuutta koskevien säännösten noudattamista paikkatietojen osalta.

Edellä 1 momentin 1 kohdassa tarkoitetuista valvontatehtävistä voidaan periä maksu yhteisötilaajalta. Maksullisista toimenpiteistä ja maksun suuruudesta päätetään oikeusministeriön asetuksella valtion maksuperustelaissa (150/1992) säädettyjen perusteiden mukaisesti.

33 §

Ohjaus- ja valvontaviranomaisten oikeus saada tietoja

— — — — — — — — — — — — — —

Viestintävirastolla ja tietosuojavaltuutetulla on oikeus saada tässä laissa säädettyjen tehtävien hoitamiseksi tunnistamistiedot, paikkatiedot ja viestit, jos ne ovat tarpeen käsittelyä, 7 §:ssä tarkoitettujen tietojen käyttöä tai suoramarkkinointia koskevien säännösten valvomiseksi taikka merkittävien tietoturvaloukkausten tai -uhkien selvittämiseksi. Edellytyksenä on lisäksi, että Viestintäviraston tai tietosuojavaltuutetun arvion mukaan on syytä epäillä jonkin seuraavista tunnusmerkistöistä täyttyvän:

— — — — — — — — — — — — — —

34 §

Valvontaviranomaisten vaitiolovelvollisuus

Viestintäviraston ja tietosuojavaltuutetun 33 §:n 3 momentin nojalla saamat tiedot luottamuksellisista viesteistä, tunnistamistiedoista ja paikkatiedoista sekä tietosuojavaltuutetun 13 h §:n nojalla saamat tiedot on pidettävä salassa.

Muilta osin valvontaviranomaisten tietojen salassapidosta säädetään viranomaisten toiminnan julkisuudesta annetussa laissa.

34 a §

Valvontaviranomaisten tietojen luovuttaminen

Viestintävirastolla ja tietosuojavaltuutetulla on muun kuin 34 §:n 1 momentissa säädetyn salassapitovelvollisuuden tai muun tietojen luovuttamista koskevan rajoituksen estämättä oikeus luovuttaa tässä laissa säädettyjä tehtäviä suorittaessaan saamiaan 33 §:n 1 momentissa tarkoitettuja tietoja liikenne- ja viestintäministeriölle.

Viestintävirastolla on 34 §:n 1 momentissa tarkoitetun salassapitosäännöksen tai muun tietojen luovuttamista koskevan rajoituksen estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja niille teleyrityksille, lisäarvopalvelun tarjoajille ja yhteisötilaajille, joita on käytetty hyväksi tietoturvaloukkauksessa, jotka ovat joutuneet tietoturvaloukkauksen kohteiksi tai joihin todennäköisesti voi kohdistua tietoturvaloukkaus, jos Viestintäviraston arvion mukaan on syytä epäillä, että jokin 33 §:n 3 momentin 1–10 kohdassa mainittu tunnusmerkistö toteutuu.

Viestintävirastolla on 34 §:n 1 momentissa säädetyn salassapitosäännöksen estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja muussa valtiossa toimivalle viranomaiselle tai muulle taholle, jonka tehtävänä on ennalta ehkäistä tai selvittää viestintäverkkoihin ja -palveluihin kohdistuvia tietoturvaloukkauksia.

Viestintävirastolla on oikeus luovuttaa 2 ja 3 momentissa tarkoitettuja tunnistamistietoja ainoastaan siinä laajuudessa kuin se on tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi. Tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

42 §

Rangaistussäännökset

Rangaistus viestintäsalaisuuden loukkaamisesta ja törkeästä viestintäsalaisuuden loukkaamisesta säädetään rikoslain 38 luvun 3 ja 4 §:ssä sekä rangaistus tietomurrosta rikoslain 38 luvun 8 §:ssä. Rangaistus 5 §:ssä säädetyn vaitiolovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan tai siitä muualla säädetä ankarampaa rangaistusta. Rangaistus 13 g §:n 3 momentissa säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 2 §:n 2 momentin mukaan, jollei teosta muualla kuin rikoslain 38 luvun 1 §:ssä säädetä ankarampaa rangaistusta.

Joka tahallaan

1) rikkoo 6 §:n 2 momentissa säädettyä teknisen suojauksen purkavan järjestelmän tai sen osan hallussapitoa, maahantuontia, valmistamista tai levittämistä koskevaa kieltoa,

2) laiminlyö 7 §:ssä säädetyt velvollisuudet,

3) laiminlyö 19 §:ssä säädetyn velvollisuuden huolehtia palvelujensa tai tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta,

4) laiminlyö 21 §:n 2 momentissa tai 35 §:n 4 momentissa säädetyn ilmoitusvelvollisuuden,

5) käsittelee tunnistamistietoja tai paikkatietoja 3 ja 4 luvussa säädetyn vastaisesti,

6) laiminlyö, mitä 24 §:ssä säädetään laskun yhteyskohtaisesta erittelystä,

7) laiminlyö, mitä 25 §:ssä säädetään puhelinluetteloihin ja muihin tilaajaluetteloihin sisältyvien henkilötietojen käsittelystä, tilaajalle luettelon tarkoituksesta ja käytöstä ilmoittamisesta, tietojen poistamisesta ja korjaami-

sesta, kielto-oikeuksista tai oikeushenkilöiden oikeuksista,

8) harjoittaa suoramarkkinointia 7 luvussa säädetyn vastaisesti, tai

9) laiminlyö, mitä 13 f–13 h §:ssä säädetään selvityksen tai ennakkoilmoituksen laatimisesta ja antamisesta käyttäjälle, työntekijöiden edustajalle tai tietosuojavaltuutetulle

on tuomittava *sähköisen viestinnän tietosuojarikkomuksesta* sakkoon, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.

Rangaistusta ei tuomita, jos rikkomus on vähäinen.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

2.

Laki

yksityisyyden suojasta työelämässä annetun lain 2 ja 21 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan yksityisyyden suojasta työelämässä 13 päivänä elokuuta 2004 annetun lain (759/2004) 2 §:n 3 momentti ja 21 §:n 1 momentti, sellaisena kuin niistä viimeksi mainittu on laissa 457/2007, seuraavasti:

2 §

Soveltamisala

— — — — — — — — — — — — — — —

Työnantajan oikeudesta tilaajana saada maksuvelvollisuuden selvittämiseksi työntekijän käyttöön annettua liittymää koskevat tunnistamistiedot ja oikeudesta käsitellä työntekijän sähköisen viestinnän tunnistamistietoja viestintäverkon luvattoman käytön tai viestintäpalvelun ohjeen vastaisen käytön tilanteissa ja yrityssalaisuuksien suojaamiseksi säädetään sähköisen viestinnän tietosuojalaissa (516/2004). Mitä mainitussa laissa säädetään paikkatietopalvelun käyttäjästä, sovelletaan työntekijään, jonka käyttöön työnantaja antaa paikkatietopalvelun. Henkilötietojen käsittelyyn sovelletaan henkilötietolakia (523/1999), jollei tässä laissa toisin säädetä.

— — — — — — — — — — — — — — —

21 §

Yhteistoiminta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä

Työntekijöihin kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja valvonnassa käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely kuuluvat yhteistoiminnasta yrityksissä annetussa laissa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa sekä työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluiksi edellä mainituista asioista.

— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

3.

Laki

yhteistoiminnasta yrityksissä annetun lain 19 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan yhteistoiminnasta yrityksissä 30 päivänä maaliskuuta 2007 annetun lain (334/2007) 19 §:n 4 kohta seuraavasti:

19 §	4) sähköpostin ja tietoverkon käytön periaatteet sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely;
Muuhun lainsäädäntöön perustuvien suunnitelmien, periaatteiden ja käytäntöjen käsittely	— — — — — — — — — — — — — — — —
Yhteistoimintaneuvotteluissa tulee käsitellä:	Tämä laki tulee voimaan päivänä kuuta 20 .
— — — — — — — — — — — — — — — —	

———

4.

Laki

yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain 7 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan yhteistoiminnasta valtion virastoissa ja laitoksissa 1 päivänä heinäkuuta 1988 annetun lain (651/1988) 7 §:n 11 a kohta, sellaisena kuin se on laissa 762/2004, seuraavasti:

7 §

Yhteistoimintamenettelyn piiriin kuuluvat asiat

Yhteistoimintamenettelyn piiriin kuuluvat:

— — — — — — — — — — — — — — —

11 a) henkilöstöön kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät, sähköpostin ja tietoverkon käyttö sekä virkamiehen ja työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely;

— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

Helsingissä 28 päivänä maaliskuuta 2008

Tasavallan Presidentti

TARJA HALONEN

Viestintäministeri *Suvi Lindén*

Liite
Rinnakkaistekstit

Laki

sähköisen viestinnän tietosuojalain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan 16 päivänä kesäkuuta 2004 annetun sähköisen viestinnän tietosuojalain (516/2004) 9, 12–14 20 ja 32 §, 33 §:n 3 momentin johdantokappale, 34 § ja 42 § sekä

lisätään lakiin uusi 12 a, 13 a–13 j ja 34 a § seuraavasti:

Voimassa oleva laki	*Ehdotus*
9 §	9 §
Tunnistamistietojen käsittely palvelujen toteuttamiseksi ja käyttämiseksi	*Tunnistamistietojen käsittely palvelujen toteuttamiseksi ja käyttämiseksi*
Tunnistamistietoja saa käsitellä siinä määrin kuin se on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun toteuttamiseksi ja käyttämiseksi sekä *näiden* tietoturvasta huolehtimiseksi.	Tunnistamistietoja saa käsitellä siinä määrin kuin se on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun toteuttamiseksi ja käyttämiseksi sekä *jäljempänä säädetyllä tavalla* tietoturvasta huolehtimiseksi.
Tunnistamistietoja saa käsitellä vain teleyrityksen, lisäarvopalvelun tarjoajan ja yhteisötilaajan palveluksessa oleva sekä näiden lukuun toimiva luonnollinen henkilö, jonka tehtävänä on käsitellä tietoja *1 momentissa ja 10–14 §:ssä* erikseen säädettyjen tarkoitusten toteuttamiseksi.	Tunnistamistietoja saa käsitellä vain teleyrityksen, lisäarvopalvelun tarjoajan, yhteisötilaajan *ja tilaajana olevan oikeushenkilön* palveluksessa oleva sekä näiden lukuun toimiva luonnollinen henkilö, jonka tehtävänä on käsitellä tietoja *tässä luvussa* erikseen säädettyjen tarkoitusten toteuttamiseksi.
12 §	12 §
Käsittely teknistä kehittämistä varten	*Käsittely teknistä kehittämistä varten*
Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä tunnistamistietoja palvelujen teknistä kehittämistä varten.	Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä tunnistamistietoja *verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun* teknistä kehittämistä varten.
Ennen 1 momentissa tarkoitetun käsittelyn aloittamista teleyrityksen ja lisäarvopalvelun tarjoajan on ilmoitettava tilaajalle tai käyttäjälle, millaisia tunnistamistietoja käsitellään ja kuinka kauan niiden käsittely kestää.	
Yhteisötilaaja voi käsitellä tunnistamistietoja oman toimintansa teknistä kehittämistä varten.	Yhteisötilaaja voi käsitellä tunnistamistietoja oman *viestintäverkkonsa ja siihen liitetyn oman palvelunsa* teknistä kehittämistä varten.

Voimassa oleva laki

Ehdotus

Ennen 1 *ja 2* momentissa tarkoitetun käsittelyn aloittamista tilaajalle tai käyttäjälle on ilmoitettava, mitä tunnistamistietoja käsitellään ja kuinka kauan niiden käsittely kestää. *Ilmoitus voi olla kertaluonteinen.*

12 a §

Käsittely tilastollista analyysiä varten

Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun tunnistamistietoja ja yhteisötilaaja voi käsitellä viestintäverkkonsa tai siihen liitetyn palvelunsa tunnistamistietoja automaattisen tietojenkäsittelyn avulla tilastollista analyysiä varten, jos:

1) analyysiä ei voida muuten tuottaa ilman kohtuutonta vaivaa; ja

2) analyysistä ei voida tunnistaa yksittäistä luonnollista henkilöä.

Mitä 1 momentissa, säädetään, koskee myös tilaajana olevan oikeushenkilön oikeutta käsitellä liittymänsä ja päätelaitteensa tunnistamistietoja.

13 §

Käsittely väärinkäytöstapauksissa

Teleyritys, lisäarvopalvelun tarjoaja ja *yhteisötilaaja* voi käsitellä tunnistamistietoja, jos se on tarpeen verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun *yksittäisten* maksullisten palvelujen käyttöä maksutta tai muiden siihen rinnastuvien käyttöä koskevien väärinkäytösten havaitsemiseksi, estämiseksi ja selvittämiseksi *sekä esitutkintaan saattamiseksi*.

13 §

Teleyrityksen ja lisäarvopalvelun tarjoajan käsittelyoikeus *väärinkäytöstapauksissa*

Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä tunnistamistietoja verkkopalvelun, viestintäpalvelun tai lisäarvopalvelun maksullisen palvelun käyttöä maksutta tai muiden siihen rinnastuvien käyttöä koskevien väärinkäytösten havaitsemiseksi, estämiseksi ja selvittämiseksi.

Viestintävirasto voi antaa tarkempia määräyksiä 1 momentissa tarkoitetun tunnistamistietojen käsittelyn teknisestä toteuttamisesta.

13 a §

Yhteisötilaajan käsittelyoikeus väärinkäytöstapauksissa

Yhteisötilaajalla on oikeus käsitellä tunnistamistietoja maksullisen tietoyhteiskunnan

Voimassa oleva laki | Ehdotus

palvelun tai viestintäverkon luvattoman käytön, viestintäpalvelun ohjeen vastaisen käytön taikka yrityssalaisuuksien paljastamisen selvittämiseksi siten kuin 13 b–13 j §:ssä säädetään.

Viestintäverkon luvatonta käyttöä tai viestintäpalvelun ohjeen vastaista käyttöä on laitteen, ohjelman tai palvelun asentaminen yhteisötilaajan viestintäverkkoon taikka muu näihin rinnastuva viestintäverkon tai viestintäpalvelun käyttö, jos se on käytöstä laadittujen 13 b §:n 3 momentissa tarkoitettujen ohjeiden vastaista.

Edellä 1 momentissa tarkoitettu oikeus ei koske kiinteän tai matkapuhelinverkon puhelinpalvelujen tunnistamistietoja.

13 b §

Yhteisötilaajan huolehtimisvelvollisuus väärinkäytöstapauksissa

Yhteisötilaajan on ennen tunnistamistietojen käsittelyn aloittamista maksullisen tietoyhteiskunnan palvelun tai viestintäverkon luvattoman käytön taikka viestintäpalvelun ohjeen vastaisen käytön ehkäisemiseksi:

1) rajoitettava pääsyä viestintäverkkoonsa ja viestintäpalveluunsa ja niiden käyttöön sekä ryhdyttävä muihin toimenpiteisiin viestintäverkkonsa ja viestintäpalvelunsa käytön suojaamiseksi asianmukaisin tietoturvallisuustoimenpitein; ja

2) määriteltävä, minkälaisia viestejä sen viestintäverkon kautta saa välittää ja hakea, sekä miten sen viestintäverkkoa ja viestintäpalvelua saa muutoin käyttää ja minkälaisiin kohdeosoitteisiin viestintää ei saa harjoittaa.

Yhteisötilaajan on ennen tunnistamistietojen käsittelyn aloittamista yrityssalaisuuksien paljastamisen ehkäisemiseksi:

1) rajoitettava pääsyä yrityssalaisuuksiin ja ryhdyttävä muihin toimenpiteisiin tietojen asianmukaiseksi suojaamiseksi; ja

2) määriteltävä, miten yrityssalaisuuksia saa viestintäverkossa siirtää, luovuttaa tai muutoin käsitellä ja minkälaisiin kohdeosoitteisiin yrityssalaisuuksia käsittelemään oikeutetut henkilöt eivät ole oikeutettuja lähettämään viestejä.

Yhteisötilaajan on 1 ja 2 momentissa tarkoi-

Voimassa oleva laki

Ehdotus

tettujen väärinkäytösten ehkäisemiseksi annettava kirjalliset ohjeet viestintäverkon tai viestintäpalvelun käyttäjälle.

13 c §

Yhteisötilaajan suunnittelu- ja yhteistoimintavelvoite väärinkäytöstapauksissa

Yhteisötilaajan on ennen 13 a §:n 1 momentissa tarkoitetun tunnistamistietojen käsittelyn aloittamista nimettävä ne henkilöt, joiden tehtäviin tunnistamistietojen käsittely kuuluu tai määriteltävä mainitut tehtävät. Tunnistamistietoja voivat käsitellä vain yhteisötilaajan viestintäverkon ja viestintäpalvelun ylläpidosta ja tietoturvasta sekä turvallisuudesta huolehtivat henkilöt.

Jos yhteisötilaaja on yhteistoimintalainsäädännön piiriin kuuluva työnantaja, on hänen:

1) käsiteltävä 13 a–13 j §:ssä tarkoitetussa tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt yhteistoiminnasta yrityksissä annetun lain (334/2007) 4 luvussa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa (651/1988) ja työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa (449/2007) tarkoitetussa yhteistoimintamenettelyssä; ja

2) tiedotettava tunnistamistietojen käsittelystä tekemänsä päätökset työntekijöille tai heidän edustajilleen siten kuin yksityisyyden suojasta työelämässä annetun lain (759/2004) 21 §:n 2 momentissa säädetään.

Jos yhteisötilaaja on työnantaja, joka ei kuulu yhteistoimintalainsäädännön piiriin, on hänen kuultava työntekijöitä 2 momentin 1 kohdassa tarkoitetuista seikoista ja tiedotettava niistä työntekijöille siten kuin yksityisyyden suojasta työelämässä annetun lain 21 §:n 1 ja 2 momentissa säädetään.

Jos yhteisötilaaja ei ole työnantaja, on yhteisötilaajan tiedotettava käyttäjille 13 a–13 j §:ssä tarkoitetussa tunnistamistietojen käsittelyssä noudatettavista menettelyistä ja käytännöistä.

Voimassa oleva laki *Ehdotus*

13 d §

Yhteisötilaajan käsittelyoikeuden edellytykset väärinkäytöstapauksissa

Yhteisötilaaja saa käsitellä tunnistamistietoja automaattisen hakutoiminnon avulla, joka voi perustua viestien kokoon, yhteenlaskettuun kokoon, tyyppiin, määrään, yhteystapaan tai kohdeosoitteisiin.

Yhteisötilaaja saa käsitellä tunnistamistietoja manuaalisesti, jos on perusteltu syy epäillä, että viestintäverkkoa, viestintäpalvelua tai maksullista tietoyhteiskunnan palvelua käytetään 13 b §:n 3 momentissa tarkoitettujen ohjeiden vastaisesti tai että yrityssalaisuus on luvattomasti annettu ulkopuoliselle ja jos:

1) automaattisen hakutoiminnon avulla on havaittu viestinnässä poikkeama;

2) maksullisen tietoyhteiskunnan palvelun käytön kustannukset ovat nousseet epätavallisen korkeiksi;

3) viestintäverkossa havaitaan sinne oikeudetta asennettu laite, ohjelma tai palvelu;

4) yrityssalaisuus julkaistaan tai sitä käytetään luvatta; taikka

5) yhteisötilaajalla on yksittäistapauksessa muun 1–4 kohtaan rinnastuvan, yleisesti havaittavissa olevan seikan perusteella syy epäillä, että viestintäverkkoa, viestintäpalvelua tai maksullista tietoyhteiskunnan palvelua käytetään 13 b §:n 3 momentissa tarkoitettujen ohjeiden vastaisesti tai että yrityssalaisuus on luvattomasti annettu ulkopuoliselle.

Edellä 1 ja 2 momentissa tarkoitetun käsittelyn edellytyksenä on, että:

1) tapahtuma tai teko todennäköisesti aiheuttaa yhteisötilaajalle merkittävää haittaa tai vahinkoa; taikka

2) epäilty yrityssalaisuuden paljastaminen kohdistuu yhteisötilaajan tai sen yhteistyökumppanin elinkeinotoiminnan kannalta keskeisiin yrityssalaisuuksiin taikka teknologisen tai muun kehittämistyön tuloksiin, jotka todennäköisesti ovat merkittäviä elinkeinotoiminnan käynnistämisen tai sen harjoittamisen kannalta.

Edellä 2 momentissa tarkoitetun käsittelyn

Voimassa oleva laki | *Ehdotus*

edellytyksenä on lisäksi, että tiedot ovat välttämättömiä väärinkäytöksen ja siitä vastuussa olevien selvittämiseksi sekä luvattoman tai ohjeen vastaisen käytön lopettamiseksi.

13 e §

Käsittelyoikeuden erityiset rajoitukset väärinkäytöstapauksissa

Automaattista hakua ei saa kohdistaa eikä tunnistamistietoja saa hakea esille eikä ottaa manuaalisesti käsiteltäviksi oikeudenkäymiskaaren (4/1734) 17 luvun 24 §:n 2 ja 3 momentissa tarkoitettujen tietojen selville saamiseksi.

Yrityssalaisuuksien paljastamisen selvittämiseksi työnantajana oleva yhteisötilaaja voi käsitellä vain sellaisten käyttäjiensä tunnistamistietoja, joille yhteisötilaaja on antanut tai joilla muutoin on yhteisötilaajan hyväksymällä tavalla pääsy yrityssalaisuuksiin.

13 f §

Yhteisötilaajan tiedonantovelvollisuus käyttäjälle väärinkäytöstapauksissa

Yhteisötilaajan on laadittava 13 d §:n 1 ja 2 momentissa tarkoitetusta manuaalisesta tunnistamistietojen käsittelystä selvitys, josta käy ilmi:

1) käsittelyn peruste, ajankohta ja kesto;

2) syy, minkä vuoksi tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty;

3) käsittelijät; sekä

4) käsittelystä päättänyt henkilö.

Käsittelyyn osallistuneiden henkilöiden on allekirjoitettava selvitys. Selvitys on säilytettävä vähintään kaksi vuotta 13 d §:ssä tarkoitetun käsittelyn päättymisestä.

Edellä 1 momentissa tarkoitettu selvitys on annettava tiedoksi käsittelyn kohteena olevan viestintäverkon tai viestintäpalvelun käyttäjälle heti, kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta. Selvitystä ei kuitenkaan tarvitse antaa niille käyttäjille, joiden tunnistamistietoja on käsitelty massamuotoisesti siten, että käyttäjien tunnistamistiedot

Voimassa oleva laki *Ehdotus*

eivät ole tulleet käsittelijän tietoon. Käyttäjällä on oikeus lakiin tai sopimukseen perustuvan salassapitovelvollisuuden estämättä luovuttaa selvitys ja sen yhteydessä saamansa tiedot etujaan tai oikeuksiaan koskevan asian käsittelyä varten.

13 g §

Yhteisötilaajan tiedonantovelvollisuus työntekijöiden edustajalle väärinkäytöstapauksissa

Jos yhteisötilaaja on työnantaja, sen on annettava työntekijöiden edustajalle vuosittain 13 d §:n 2 momentissa tarkoitetusta tunnistamistietojen manuaalisesta käsittelystä selvitys, josta on käytävä ilmi, millä perusteella ja kuinka monta kertaa tunnistamistietoja on vuoden aikana käsitelty.

Edellä 1 momentissa tarkoitettu selvitys on annettava työ- tai virkaehtosopimuksen perusteella valitulle luottamusmiehelle tai, jos tällaista ei ole valittu, työsopimuslain (55/2001) 13 luvun 3 §:ssä tarkoitetulle luottamusvaltuutetulle. Jos jonkin henkilöstöryhmän työntekijät eivät ole valinneet luottamusmiestä tai luottamusvaltuutettua, on selvitys annettava yhteistoiminnasta yrityksissä annetun lain 8 §:ssä tai työnantajan ja henkilöstön välisestä yhteistoiminasta kunnissa annetun lain 3 §:ssä tarkoitetulle yhteistoimintaedustajalle taikka yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain 6 §:n 2 momentissa tarkoitetulle edustajalle. Jos näitäkään ei ole valittu, selvitys on annettava kaikille tähän henkilöstöryhmään kuuluville työntekijöille.

Työntekijöiden edustajien ja 2 momentissa tarkoitettujen työntekijöiden on pidettävä salassa tietoonsa saamat yrityssalaisuuden loukkaukset ja epäilyt yrityssalaisuuden loukkaamisesta koko työsuhteen voimassaoloajan. Virkamiehen ja muun viranomaisen palveluksessa toimivan salassapitovelvollisuudesta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) ja muualla laissa säädetään. Mitä edellä säädetään, ei estä tietojen luovuttamista valvontaviranomaiselle.

Voimassa oleva laki

Ehdotus

13 h §

Ennakkoilmoitus ja vuosittainen selvitys tietosuojavaltuutetulle väärinkäytöstapauksissa

Yhteisötilaajan on ilmoitettava ennalta tietosuojavaltuutetulle tunnistamistietojen käsittelyn aloittamisesta. Ennakkoilmoituksesta on käytävä ilmi:

1) 13 d §:ssä tarkoitetussa tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt;

2) 13 c §:n 1 momentissa tarkoitetut tehtävät; ja

3) miten yhteisötilaaja järjestänyt 13 c §:n 2 momentin 2 kohdassa tai 3 momentissa tarkoitetun käsittelyä edeltävän tiedottamisvelvollisuutensa.

Yhteisötilaajan on annettava tietosuojavaltuutetulle vuosittain jälkikäteen selvitys tunnistamistietojen manuaalisesta käsittelystä. Selvityksestä on käytävä ilmi, millä perusteella ja kuinka monta kertaa tunnistamistietoja on vuoden aikana käsitelty.

13 i §

Yhteisötilaajan oikeus säilyttää tunnistamistietoja väärinkäytöstapauksissa

Mitä edellä 13 a–13 h §:ssä säädetään, ei oikeuta yhteisötilaajaa säilyttämään tunnistamistietoja rekisterissä kauempaa kuin lain mukaan muutoin on sallittua.

.

13 j §

Yhteisötilaajan oikeus tietojen luovuttamiseen väärinkäytöstapauksissa

Sen estämättä, mitä 8 §:n 3 momentissa säädetään, yhteisötilaajalla on oikeus luovuttaa asianomistajana tekemänsä rikosilmoituksen tai tutkintapyynnön yhteydessä poliisille käsiteltäviksi 13 a–13 i §:n mukaisesti saamansa yhteisötilaajan viestintäverkon tai viestintäpalvelun käyttäjän viestejä koskevat tunnistamistiedot.

Voimassa oleva laki	*Ehdotus*
14 §	14 §
Käsittely teknisen vian tai virheen havaitsemiseksi	*Käsittely teknisen vian tai virheen havaitsemiseksi*
Teleyritys, lisäarvopalvelun tarjoaja ja yhteisötilaaja voi käsitellä tunnistamistietoja, jos se on tarpeen viestinnän välittämisessä tapahtuneen teknisen vian tai virheen havaitsemiseksi.	Teleyritys, lisäarvopalvelun tarjoaja ja yhteisötilaaja voi käsitellä tunnistamistietoja, jos se on tarpeen viestinnän välittämisessä tapahtuneen teknisen vian tai virheen havaitsemiseksi, *estämiseksi ja selvittämiseksi*.
20 §	20 §
Toimenpiteet tietoturvan toteuttamiseksi	*Toimenpiteet tietoturvan toteuttamiseksi*
Tietoturvaloukkausten torjumiseksi ja tietoturvaan kohdistuvien häiriöiden poistamiseksi teleyrityksellä, lisäarvopalvelun tarjoajalla tai yhteisötilaajalla ja näiden lukuun toimivalla on oikeus ryhtyä välttämättömiin toimiin 19 §:ssä tarkoitetun tietoturvan varmistamiseksi: 1) estämällä sähköpostiviestien, tekstiviestien ja muiden vastaavien viestien välittäminen ja vastaanottaminen; 2) poistamalla tietoturvaa vaarantavat haittaohjelmat viesteistä; sekä 3) toteuttamalla muut näihin rinnastettavat teknisluonteiset toimet.	*Teleyrityksellä, lisäarvopalvelun tarjoajalla ja yhteisötilaajalla sekä niiden lukuun toimivalla on oikeus ryhtyä 2 momentissa tarkoitettuihin välttämättömiin toimiin tietoturvasta huolehtimiseksi:* *1) viestintäverkkojen tai niihin liitettyjen palvelujen tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;* *2) viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi; tai* *3) viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain (39/1889) 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.*
Edellä 1 momentissa tarkoitettuihin toimiin saa ryhtyä vain, jos toimet ovat välttämättömiä verkkopalvelujen tai viestintäpalvelujen taikka viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi.	*Edellä 1 momentissa tarkoitetut toimet voivat käsittää:* *1) viestin automaattisen sisällöllisen analyysin;* *2) viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen;* *3) tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä; sekä* *4) muut näihin rinnastettavat teknisluonteiset toimenpiteet.*
Viestin sisältöön saa puuttua ainoastaan teknisin keinoin viestin tarkastamiseksi ja poistamiseksi, jos on todennäköisiä syitä epäillä viestin sisältävän sellaisen tietokoneohjelman tai ohjelmakäskyjen sarjan, jota tarkoitetaan rikoslain (39/1889) 34 luvun 9 a §:n 1 kohdassa tai jos on todennäköisiä syitä	*Jos viestin tyypin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai ohjelmakäskyn eikä viestin automaattisella sisällöllisellä analyysillä pystytä turvaamaan 1 momentissa tarkoitettujen tavoitteiden toteutumista, yksittäisen viestin sisältöä*

Voimassa oleva laki	*Ehdotus*
epäillä, että viestiä käytetään rikoslain 38 luvun 5 §:ssä säädettyyn tietoliikenteen häirintään.	*saa käsitellä manuaalisesti. Manuaalisesta viestin sisällön käsittelystä on ilmoitettava viestin lähettäjälle ja vastaanottajalle, ellei ilmoittamisella todennäköisesti vaaranneta 1 momentissa tarkoitettujen tavoitteiden toteutumista.*
Toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä verkkopalvelujen tai viestintäpalvelujen taikka viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi. Toimenpiteet on lopetettava heti, kun niiden toteuttamiselle ei enää ole tässä pykälässä säädettyjä edellytyksiä.	*Tässä pykälässä tarkoitetut toimenpiteet on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteutettaessa ei saa rajoittaa sananvapautta taikka luottamuksellisen viestin tai yksityisyyden suojaa enempää kuin on välttämätöntä 1 momentissa tarkoitettujen tavoitteiden turvaamiseksi. Toimenpiteet on lopetettava, jos niiden toteuttamiselle ei enää ole tässä pykälässä säädettyjä edellytyksiä.*
Viestintävirasto voi antaa tarkempia määräyksiä tietoturvaloukkausten tässä pykälässä tarkoitetusta teknisestä torjumisesta ja tietoturvaan kohdistuvien häiriöiden poistamisesta.	*Viestintävirasto voi antaa teleyrityksille ja lisäarvopalvelun tarjoajille tarkempia määräyksiä tässä pykälässä tarkoitettujen toimenpiteiden teknisestä toteuttamisesta.*
32 §	32 §
Tietosuojavaltuutetun tehtävät	*Tietosuojavaltuutetun tehtävät*
Tietosuojavaltuutetun tehtävänä on valvoa:	Tietosuojavaltuutetun tehtävänä on valvoa:
1) edellä 4 luvussa tarkoitettua paikkatietojen käsittelyä;	1) *13 a–13 j §:ssä tarkoitettua yhteisötilaajan tunnistamistietojen käsittelyä*;
	2) 4 luvussa tarkoitettua paikkatietojen käsittelyä;
2) edellä 25 §:ssä tarkoitettuja puhelinluetteloita ja muita tilaajaluetteloita sekä numerotiedotusta koskevien säännösten noudattamista;	*3)* 25 §:ssä tarkoitettuja puhelinluetteloita ja muita tilaajaluetteloita sekä numerotiedotusta koskevien säännösten noudattamista;
3) edellä 7 lukuun sisältyvien suoramarkkinointia koskevien säännösten noudattamista; sekä	*4)* 7 lukuun sisältyvien suoramarkkinointia koskevien säännösten noudattamista;
4) jäljempänä 9 lukuun sisältyvien tiedonsaantioikeuksia ja vaitiolovelvollisuutta koskevien säännösten noudattamista paikkatietojen osalta.	*5)* 9 lukuun sisältyvien tiedonsaantioikeuksia ja vaitiolovelvollisuutta koskevien säännösten noudattamista paikkatietojen osalta.
	Edellä 1 momentin 1 kohdassa tarkoitetuista valvontatehtävistä voidaan periä maksu yhteisötilaajalta. Maksullisista toimenpiteistä ja maksun suuruudesta päätetään oikeusministeriön asetuksella valtion maksuperustelaissa (150/1992) säädettyjen perusteiden mukaisesti.

Voimassa oleva laki	*Ehdotus*
33 §	33 §
Ohjaus- ja valvontaviranomaisten ***tiedonsaantioikeus***	*Ohjaus- ja valvontaviranomaisten* ***oikeus saada tietoja***
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Viestintävirastolla ja tietosuojavaltuutetulla on oikeus saada tässä laissa säädettyjen tehtävien hoitamiseksi tunnistamistiedot, paikkatiedot ja *20 §:n 2 momentissa tarkoitetut* viestit, jos ne ovat tarpeen käsittelyä, 7 §:ssä tarkoitettujen tietojen käyttöä tai suoramarkkinointia koskevien säännösten *noudattamisen* valvomiseksi tai merkittävien tietoturvaloukkausten ja -uhkien selvittämiseksi ja jos Viestintäviraston tai tietosuojavaltuutetun arvion mukaan on syytä epäillä, että jokin seuraavista tunnusmerkistöistä täyttyy:	Viestintävirastolla ja tietosuojavaltuutetulla on oikeus saada tässä laissa säädettyjen tehtävien hoitamiseksi tunnistamistiedot, paikkatiedot ja viestit, jos ne ovat tarpeen käsittelyä, 7 §:ssä tarkoitettujen tietojen käyttöä tai suoramarkkinointia koskevien säännösten valvomiseksi taikka merkittävien tietoturvaloukkausten tai -uhkien selvittämiseksi. *Edellytyksenä on lisäksi, että* Viestintäviraston tai tietosuojavaltuutetun arvion mukaan on syytä epäillä *jonkin seuraavista tunnusmerkistöistä täyttyvän*:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
34 §	34 §
Valvontaviranomaisten vaitiolovelvollisuus ***ja tietojen luovuttaminen***	*Valvontaviranomaisten vaitiolovelvollisuus*
Viestintäviraston ja tietosuojavaltuutetun 33 §:n 3 momentin nojalla saamat tiedot luottamuksellisista viesteistä, tunnistamistiedoista ja paikkatiedoista on pidettävä salassa.	Viestintäviraston ja tietosuojavaltuutetun 33 §:n 3 momentin nojalla saamat tiedot luottamuksellisista viesteistä, tunnistamistiedoista ja paikkatiedoista *sekä tietosuojavaltuutetun 13 h §:n momentin nojalla saamat tiedot* on pidettävä salassa.
Viestintävirastolla ja tietosuojavaltuutetulla on muun kuin 1 momentissa tarkoitetun salassapitosäännöksen tai muun tietojen luovuttamista koskevan rajoituksen estämättä oikeus luovuttaa tässä laissa säädettyjä tehtäviä suorittaessaan saamiaan 33 §:n 1 momentissa tarkoitettuja tietoja liikenne- ja viestintäministeriölle.	(*34 a §:n 1 momentti*)
Viestintävirastolla on 1 momentissa tarkoitetun salassapitosäännöksen tai muun tietojen luovuttamista koskevan rajoituksen estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja niille teleyrityksille, lisäarvopalvelun tarjoajille ja yhteisötilaajille, joita on käytetty hyväksi tietoturvaloukkauksessa tai jotka ovat joutuneet tietoturvaloukkauksen kohteiksi, jos Viestintäviraston arvion mukaan on syytä epäillä, että	(*34 a §:n 2 momentti*)

Voimassa oleva laki	*Ehdotus*
jokin edellä 33 §:n 3 momentin 1–10 kohdassa mainittu tunnusmerkistö täyttyy.	
Viestintävirastolla on oikeus luovuttaa 3 momentissa tarkoitettuja tunnistamistietoja ainoastaan siinä laajuudessa kuin se on tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi.	(*34 a §:n 3 momentti*)
Muilta osin valvontaviranomaisen tietojen salassapidosta *on voimassa, mitä* viranomaisen toiminnan julkisuudesta annetussa laissa (621/1999) säädetään.	Muilta osin valvontaviranomaisten tietojen salassapidosta *säädetään* viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään.
	34 a §
	Valvontaviranomaisten tietojen luovuttaminen
(*34 §:n 2 momentti*)	*Viestintävirastolla ja tietosuojavaltuutetulla on muun kuin 34 §:n 1 momentissa säädetyn salassapitosäännöksen tai muun tietojen luovuttamista koskevan rajoituksen estämättä oikeus luovuttaa tässä laissa säädettyjä tehtäviä suorittaessaan saamiaan 33 §:n 1 momentissa tarkoitettuja tietoja liikenne- ja viestintäministeriölle.*
(*34 §:n 3 momentti*)	*Viestintävirastolla on 34 §:n 1 momentissa tarkoitetun salassapitosäännöksen tai muun tietojen luovuttamista koskevan rajoituksen estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja niille teleyrityksille, lisäarvopalvelun tarjoajille ja yhteisötilaajille, joita on käytetty hyväksi tietoturvaloukkauksessa, jotka ovat joutuneet tietoturvaloukkauksen kohteiksi tai joihin todennäköisesti voi kohdistua tietoturvaloukkaus, jos Viestintäviraston arvion mukaan on syytä epäillä, että jokin 33 §:n 3 momentin 1–10 kohdassa mainittu tunnusmerkistö toteutuu.*
(*34 §:n 2 momentti*)	*Viestintävirastolla on 34 §:n 1 momentissa säädetyn salassapitosäännöksen estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan tunnistamistietoja muussa valtiossa toimivalle viranomaiselle tai muulle taholle, jonka tehtävänä on ennalta ehkäistä tai selvittää viestintäverkkoihin ja -palveluihin kohdistuvia tietoturvaloukkauksia.*
	Viestintävirastolla on oikeus luovuttaa 2 ja 3 momentissa tarkoitettuja tunnistamistietoja

Voimassa oleva laki

Ehdotus

ainoastaan siinä laajuudessa kuin se on tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi. Tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

42§

Rangaistussäännökset

Rangaistus viestintäsalaisuuden loukkaamisesta ja törkeästä viestintäsalaisuuden loukkaamisesta säädetään rikoslain 38 luvun 3 ja 4 §:ssä sekä rangaistus tietomurrosta rikoslain 38 luvun 8 §:ssä. Rangaistus 5 §:ssä säädetyn vaitiolovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan tai siitä muualla säädetä ankarampaa rangaistusta.

Joka tahallaan

1) rikkoo 6 §:n 2 momentissa säädettyä teknisen suojauksen purkavan järjestelmän tai sen osan hallussapitoa, maahantuontia, valmistamista tai levittämistä koskevaa kieltoa,

2) laiminlyö 7 §:ssä säädetyt velvollisuudet,

3) laiminlyö 19 §:ssä säädetyn velvollisuuden huolehtia palvelujensa tai tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta,

4) laiminlyö 21 §:n 2 momentissa tai 35 §:n 4 momentissa säädetyn ilmoitusvelvollisuuden,

5) käsittelee tunnistamistietoja tai paikkatietoja 3 ja 4 luvussa säädetyn vastaisesti,

6) laiminlyö, mitä 24 §:ssä säädetään laskun yhteyskohtaisesta erittelystä,

7) laiminlyö, mitä 25 §:ssä säädetään puhelinluetteloihin ja muihin tilaajaluetteloihin sisältyvien henkilötietojen käsittelystä, tilaajalle luettelon tarkoituksesta ja käytöstä ilmoittamisesta, tietojen poistamisesta ja korjaamisesta, kielto-oikeuksista tai oikeushenkilöiden

42 §

Rangaistussäännökset

Rangaistus viestintäsalaisuuden loukkaamisesta ja törkeästä viestintäsalaisuuden loukkaamisesta säädetään rikoslain 38 luvun 3 ja 4 §:ssä sekä rangaistus tietomurrosta rikoslain 38 luvun 8 §:ssä. Rangaistus 5 §:ssä säädetyn vaitiolovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan tai siitä muualla säädetä ankarampaa rangaistusta. *Rangaistus 13 g §:n 3 momentissa säädetyn salassapitovelvollisuuden rikkomisesta tuomitaan rikoslain 38 luvun 2 §:n 2 momentin mukaan, jollei teosta muualla kuin rikoslain 38 luvun 1 §:ssä säädetä ankarampaa rangaistusta.*

Joka tahallaan

1) rikkoo 6 §:n 2 momentissa säädettyä teknisen suojauksen purkavan järjestelmän tai sen osan hallussapitoa, maahantuontia, valmistamista tai levittämistä koskevaa kieltoa,

2) laiminlyö 7 §:ssä säädetyt velvollisuudet,

3) laiminlyö 19 §:ssä säädetyn velvollisuuden huolehtia palvelujensa tai tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta,

4) laiminlyö 21 §:n 2 momentissa tai 35 §:n 4 momentissa säädetyn ilmoitusvelvollisuuden,

5) käsittelee tunnistamistietoja tai paikkatietoja 3 ja 4 luvussa säädetyn vastaisesti,

6) laiminlyö, mitä 24 §:ssä säädetään laskun yhteyskohtaisesta erittelystä,

7) laiminlyö, mitä 25 §:ssä säädetään puhelinluetteloihin ja muihin tilaajaluetteloihin sisältyvien henkilötietojen käsittelystä, tilaajalle luettelon tarkoituksesta ja käytöstä ilmoittamisesta, tietojen poistamisesta ja korjaamisesta, kielto-oikeuksista tai oikeushenkilöi-

Voimassa oleva laki	*Ehdotus*
oikeuksista, *tai*	den oikeuksista,
8) harjoittaa suoramarkkinointia 7 luvussa säädetyn vastaisesti,	8) harjoittaa suoramarkkinointia 7 luvussa säädetyn vastaisesti, *tai*
	9) laiminlyö, mitä 13 f–13 h §:ssä säädetään selvityksen tai ennakkoilmoituksen laatimisesta ja antamisesta käyttäjälle, työntekijöiden edustajalle tai tietosuojavaltuutetulle
on tuomittava *sähköisen viestinnän tietosuojarikkomuksesta* sakkoon, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.	on tuomittava *sähköisen viestinnän tietosuojarikkomuksesta* sakkoon, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.
Rangaistusta ei tuomita, jos rikkomus on vähäinen.	Rangaistusta ei tuomita, jos rikkomus on vähäinen.
	———
	Tämä laki tulee voimaan päivänä kuuta 20 .

———

2.

Laki

yksityisyyden suojasta työelämässä annetun lain 2 ja 21 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan yksityisyyden suojasta työelämässä 13 päivänä elokuuta 2004 annetun lain (759/2004) 2 §:n 3 momentti ja 21 §:n 1 momentti, sellaisena kuin se on laissa 457/2007 seuraavasti:

Voimassa oleva laki	*Ehdotus*
1 luku	1 luku
Yleiset säännökset	**Yleiset säännökset**
2 §	2 §
Soveltamisala	*Soveltamisala*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
Henkilötietojen käsittelyyn sovelletaan henkilötietolakia (523/1999) ja sähköisen viestinnän tietosuojalakia (516/2004), jollei tässä laissa toisin säädetä.	*Työnantajan oikeudesta tilaajana saada maksuvelvollisuuden selvittämiseksi työntekijän käyttöön annettua liittymää koskevat tunnistamistiedot ja oikeudesta käsitellä työntekijän sähköisen viestinnän tunnistamistietoja viestintäverkon luvattoman käytön tai viestintäpalvelun ohjeen vastaisen käytön tilanteissa ja yrityssalaisuuksien suojaamiseksi säädetään sähköisen viestinnän tietosuojalaissa (516/2004). Mitä mainitussa laissa säädetään paikkatietopalvelun käyttäjästä, sovelletaan työntekijään, jonka käyttöön työnantaja antaa paikkatietopalvelun.* Henkilötietojen käsittelyyn sovelletaan henkilötietolakia (523/1999), jollei tässä laissa toisin säädetä.
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
7 luku	7 luku
Erinäisiä säännöksiä	**Erinäisiä säännöksiä**
21 §	21 §
Yhteistoiminta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä	*Yhteistoiminta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä*
Työntekijöihin kohdistuvan kameravalvon-	Työntekijöihin kohdistuvan kameravalvon-

Voimassa oleva laki	*Ehdotus*
nan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö kuuluvat yhteistoiminnasta yrityksissä annetussa laissa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa sekä työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi edellä mainituista asioista.	nan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö *sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely* kuuluvat yhteistoiminnasta yrityksissä annetussa laissa, yhteistoiminnasta valtion virastoissa ja laitoksissa annetussa laissa sekä työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa annetussa laissa tarkoitetun yhteistoimintamenettelyn piiriin. Muissa kuin yhteistoimintalainsäädännön piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä työnantajan on ennen päätöksentekoa varattava työntekijöille tai heidän edustajilleen tilaisuus tulla kuulluksi edellä mainituista asioista.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 20 .

3.

Laki

yhteistoiminnasta yrityksissä annetun lain 19 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan yhteistoiminnasta yrityksissä 30 päivänä maaliskuuta 2007 annetun lain (334/2007) 19 §:n 4 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
19 §	19 §
Muuhun lainsäädäntöön perustuvien suunnitelmien, periaatteiden ja käytäntöjen käsittely	*Muuhun lainsäädäntöön perustuvien suunnitelmien, periaatteiden ja käytäntöjen käsittely*
Yhteistoimintaneuvotteluissa tulee käsitellä:	Yhteistoimintaneuvotteluissa tulee käsitellä:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
4) sähköpostin ja tietoverkon käytön periaatteet;	4) sähköpostin ja tietoverkon käytön periaatteet *sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely*;
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

4.

Laki

yhteistoiminnasta valtion virastoissa ja laitoksissa annetun lain 7 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan yhteistoiminnasta valtion virastoissa ja laitoksissa 1 päivänä heinäkuuta 1988 annetun lain (651/1988) 7 §:n 11 a kohta, sellaisena kuin se on laissa 762/2004, seuraavasti:

Voimassa oleva laki	*Ehdotus*
7 §	7 §
Yhteistoimintamenettelyn piiriin kuuluvat asiat	*Yhteistoimintamenettelyn piiriin kuuluvat asiat*
Yhteistoimintamenettelyn piiriin kuuluvat:	Yhteistoimintamenettelyn piiriin kuuluvat:
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
11 a) henkilöstöön kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja tietoverkon käyttö; (13.8.2004/762)	11 a) henkilöstöön kohdistuvan kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja tietoverkon käyttö *sekä virkamiehen ja työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely*;
	— — — — — — — — — — — — — — —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____