TURUN AMMATTIKORKEAKOULU
ÅBO YRKESHÖGSKOLA

Emilia Aho

Sähköisen viestinnän tietosuojalaki ja sen vaikutukset

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Maaliskuu 2009

TURUN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Koulutusohjelma Tietojenkäsittely	
Tekijä Emilia Aho	
Työn nimi Sähköisen viestinnän tietosuojalaki ja sen vaikutukset	
Suuntautumisvaihtoehto Tietoliikenne	Ohjaaja Esko Vainikka
Aika Maaliskuu 2009	Sivumäärä 61+4 liitettä

Lex Nokialla tarkoitetaan sähköisen viestinnän tietosuojalakia ja siihen liittyviä lakien muutoksia. Uusi tietosuojalaki tuli voimaan 1.6.2009. Uuden lain myötä muun muassa työnantajat pystyvät tarkkailemaan työntekijöiden sähköpostiliikenteen tunnistamistietoja. Tunnistamistietoja ovat viestin ja sen liitteenä olevien tiedostojen koko, kellonaika, liitetiedoston muoto sekä lähettäjä ja vastaanottaja. Uusi laki on saanut osakseen paljon kritiikkiä eri tahoilta. Mielenkiintoista on se, että yksikään yritys ei ole ottanut käyttöön uutta sähköisen viestinnän tietosuojalakia, vaikka laki on ollut voimassa jo yli yhdeksän kuukautta.

Lex Nokiaa ja uutta sähköisen viestinnän tietosuojalakia on kritisoitu sekavaksi, ja lisäksi uuden tietosuojalain on sanottu loukkaavan ihmisten perusoikeuksia. Työn tavoitteena on selventää, mitä Lex Nokia nimi pitää sisällään, mistä kaikki sai alkunsa ja miksi. Työssä otetaan myös huomioon tietoturvaseikat, laki yksityisyyden suojasta työelämässä ja henkilötietolaki. Edellä mainitut liittyvät olennaisesti sähköisen viestinnän tietosuojalakiin. Tarkoituksena on saada aikaan mielikuva siitä, millaisia haittoja ja hyötyjä laista on, onko uusi laki perustuslain vastainen, vaarantuuko työntekijöiden yksityisyyden suoja työelämässä ja mitä vaikutuksia lailla on tietoturvan kannalta.

Työ on hyvin teoriapainotteinen. Teoriaosassa kerrotaan hieman tietoturvafaktoja, laajemmin käsitellään sähköisen viestinnän vanhaa ja uutta tietosuojalakia (liitteenä on molemmat lait), perehdytään työnantajan oikeuksiin ja velvollisuuksiin sekä henkilötietojen käsittelyyn. Empiriaosa kattaa haastattelun sekä lukuisten eri tahojen mielipiteet uudesta sähköisen viestinnän tietosuojalaista.

Yhteenvetona voidaan todeta, että uusi sähköisen viestinnän tietosuojalaki jättää kansalaisten perusoikeudet huomioimatta, laki ei ole riittävän selkeä, lain käyttöönotto vaatii liian paljon toimenpiteitä yrityksissä, asiantuntijoiden lausuntoja ei ole otettu riittävästi huomioon lakia säädettäessä sekä yksityisten oikeudet tulisivat yhtä laajoiksi kuin poliisin oikeudet ovat. Laki saa siis osakseen paljon negatiivista palautetta. Lainsäätäjien tulisikin miettiä, miten lakia voitaisiin muuttaa, jotta yritykset voisivat ottaa sen käyttöön.

Luottamuksellinen: -

Hakusanat: sähköisen viestinnän tietosuojalaki, tietoturva, yksityisyyden suoja, henkilötietolaki

Säilytys: Turun ammattikorkeakoulun kirjasto, Lemminkäisenkatu

TURKU UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

Degree programme Information Technology	
Author Emilia Aho	
Title Protection of Privacy in Electronic Communications and Its Effects	
Specialization line Data Communication	Instructor Esko Vainikka
Date March 2009	Total number of pages 61+4 appendices

Lex Nokia means Protection of Privacy in Electronic Communications and the changes in laws related to it. The new Electronic Communications law came into operation on 1 June 2009. Along with the new law, employers can observe the workers through their email identifications. The identifications are the signal of files' attachment sizes, times, file attachment forms as well as the sender and the receiver. The new law received a lot of criticism from different parties. It is interesting that no firm has taken into use the new Protection of Privacy in Electronic law even though the law has been valid for over nine months.

Lex Nokia and the new Law on Protection of Privacy in Electronic Communications have been criticized being confusing and additionally the new protection of privacy has been told to violate the fundamental rights of citizens. The aim of this work is to clarify what the name Lex Nokia covers, from where everything got started and why. In this thesis the information security issues are also considered as well as the law of privacy in the work place and the law of personal data. The facts mentioned above are essentially connected with the Law on Protection of Privacy in Electronic Communications. The aim is to get an idea of what kind of disadvantages and advantages there are and find out if the new law is contrary to the constitution, endangering the workers' law of privacy in the work place and what the law's effects are from the information security point of view.

The work is very theory oriented. The theory part gives some information on the information security, the old and new information protection laws on Protection of Privacy in Electronic Communications are discussed more extensively (both law files are attached). Employers' rights and duties, as well as dealing with the personal details are made familiar. The empirical part covers the interview and the opinions of several different parties on the new Protection of Privacy in Electronic Communications.

In conclusions it may be said that the new Law on Protection of Privacy in Electronic Communications leaves the fundamental right of citizens in the second place. The law is not clear enough. The introduction of law demands a lot of action in firms' operations. The professionals' statements are not getting enough attention in enacting the law and also the private rights would become equally comprehensive as the police rights. The law gets a lot of negative feedback. Those with legislative power should consider how to change the law in order to make it possible for the firms to use it.

Confidentiality status: -

Keywords: Protection of Privacy in Electronic Communications, Information Security, Privacy Policy, Personal Data Act

Deposit at: Turku University of Applied Sciences Library, Lemminkäisenkatu

SISÄLTÖ

1 JOHDANTO

2000-luvulla tietokoneet ja sähköpostit ovat yleistyneet huimaa vauhtia. Sähköpostin käytön kasvaessa ja tietokoneiden yleistyttyä onkin syytä huolehtia riittävästä tietoturvasta. Tietoturvan tavoitteena on varmistaa, että tietojärjestelmät suojataan riskeiltä, järjestelmiä pystyvät käyttämään vain niiden käyttöön oikeutetut ihmiset ja nämä tiedot ovat näiden henkilöiden käytettävissä, kun he niitä tarvitsevat. (Ruohonen 2002, 2.)

Paljon keskustelua ja kritiikkiä herättänyt Lex Nokia saa aikaan muutoksen aikakauden, jolloin sähköisen viestinnän tietosuojalain soveltamisala muuttuu. Lex Nokialla (voidaan käyttää myös nimitystä Urkintalaki) tarkoitetaan sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muutoksia. (Helsingin Sanomat 2009 [viitattu 15.9.2009.]) Sähköisen viestinnän tietosuojalailla pyritään turvaamaan luottamuksellisuuden ja yksityisyyden suojan toteutuminen, sekä edistetään sähköisen viestinnän tietoturvaa ja sähköisen viestinnän palvelujen tasapainoista kehittymistä. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 15.9.2009].)

Tämän työn tarkoituksena on tutkia vaarantaako uusi laki työntekijöiden yksityisyyden suojan työelämässä, sotiiko laki perustuslain asetuksia vastaan ja heikkeneekö vai parantuuko tietoturva uuden lain myötä. Toiseksi näkökulmaksi otan uudistuksen hyvät puolet eli pohdin minkälaiset tahot laista hyötyvät ja millaista hyötyä ne siitä saavat. Laki yksityisyyden suojasta työelämässä sääntelee muun muassa työntekijöitä koskevien henkilötietojen käsittelyä, teknistä valvontaa työpaikalla sekä työntekijöiden sähköpostiviestien hakemista ja näiden viestien avaamista. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 15.9.2009].)

Tavoitteenani on selventää mitä Lex Nokia tosiaan tarkoittaa ja minkälaista kritiikkiä uusi laki on osakseen saanut. Lehtien lööpeistä voi lukea edelleen kirjoituksia, joissa puidaan uutta sähköisen viestinnän tietosuojalakia. Mielestäni lehtien lööpit raapaisevat Lex Nokia-asiaa vain pintapuolisesti, mutta minä haluan tutkia asiaa tarkemmin. Oma tutkielmani aiheesta ei varmasti ole ensimmäinen eikä viimeinen, jossa asiasta

keskustellaan. Lähteinä käytän kahta tänä vuonna kirjoitettua teosta ja hieman vanhempia teoksia. Näiden lisäksi verkkojulkaisuja ja lehtiartikkeleita on saatavilla runsaasti. Pyrin ottamaan työhöni mahdollisimman paljon eri tahojen mielipiteitä asiasta. Tällä tavoin saan omien mielipiteitteni tueksi myös muiden ihmisten mielipiteitä. Oman sanansa asiasta ovat lausuneet ainakin eduskunta päättäessään uuden sähköisen viestinnän tietosuojalain läpimenosta, perustuslakivaliokunta, oikeusoppineet sekä muut valtion tahot.

Opiskelen Turun ammattikorkeakoulussa viimeistä vuotta tietojenkäsittelyn koulutusohjelman opintolinjalla. Opinnäytetyöni toimeksiantaja on Turun ammattikorkeakoulu, Lemminkäisenkadun koulutusyksikkö. Työn tilaajana ja samalla opinnäytetyöni valvojana toimii yliopettaja EskoVainikka. Koulutusohjelmamme sisältää kursseja, jotka liittyvät tietoturva-asioihin. Opinnäytetyötäni olisi tarkoitus käyttää soveltuvin osin opetuksessa.

2 TIETOTURVA

2.1 Määritelmä

Tietoturvan voidaan sanoa olevan perusta tärkeiden ja luottamuksellisten tietojen käsittelylle. Tietoturva on tärkeä elementti niin yrityksille kuin yksityisille ihmisillekin. Yksilöt pyrkivät suojaamaan omia tiedostojaan ja sähköpostiviestejään. Yrityksissä taas halutaan suojella henkilöstöön, palkkoihin, tuotteisiin ja myyntilukuihin liittyviä tietoja. Tietoturvan voidaan sanoa kattavan kaiken sen, mikä liittyy tietojen saatavuuteen, oikeellisuuteen sekä tietojen luottamuksellisuuden säilymiseen. (Järvinen 2002, 21.)

Tietoturvaan liittyy läheisesti tietosuoja. Tietosuojasta voidaan puhua myös nimellä yksityisyyden suoja. Edellä mainituilla tarkoitetaan yksilön henkilötietojen ja henkilökohtaiseen toimintaan liittyvien tietojenkäsittelyn ja keräämisen rajoittamista niin, ettei henkilön yksityisyys vaarantuisi. Tänä päivänä jopa yksittäiset henkilöt ja pienet yritykset joutuvat pohtimaan tietoturvakysymyksiä, koska tietokoneiden tarve kasvaa kaiken aikaa ja kehitys tuo mukanaan yhä suurempia tietoturvariskejä. (Järvinen 2002, 21.) Tietoturvan tavoitteena on suojata tietojärjestelmä odotetuilta ja odottamattomilta riskeiltä. Tämän lisäksi tietoturvan tavoitteena on varmistaa, että suojattavat tiedot ovat vain niiden käytettävissä, joilla on oikeus käyttää tietoja, ja että nämä tiedot ovat käyttäjien saatavilla silloin, kun he niitä tarvitsevat. (Ruohonen 2002, 2.)

Tietoturvallisuudesta puhuttaessa voidaan myös sanoa sen olevan teknisiä ja hallinnollisia toimia. Nämä toimet tulee suunnitella huolella ja toteuttaa siten, että huomioidaan lainsäädännön vaatimukset ja rajoitukset. Hyvän tietoturvallisuuden voidaan sanoa olevan osa organisaatiokulttuuria, jossa kaikki ymmärtävät tietoturvallisuuden merkityksen ja työskentelevät sen saavuttamiseksi ja ylläpitämiseksi. (Laaksonen, Nevasalo & Tomula 2006, 17-18.)

Suomessa ei ainakaan vielä ole tietoturvaa koskevaa erillislakia, missä olisi säädelty yhteisöjen ja yksittäisten tietokoneenkäyttäjien tietoturvavelvoitteista tai -oikeuksista.

Julkisuudessa on kuitenkin ollut keskustelua lain säätämisestä, mutta lainsäätäjät ja yritykset ovat pitäneet yhteisenä kantana, että tällaista lainsäädäntöä ei tarvita. Lainsäätäjä on nähnyt parempana vaihtoehtona sen, että tietoturvavelvoitteet määritellään osana muiden lakien sisältöä. Nämä muut lait ovat henkilötietolaki, laki yksityisyyden suojasta työelämässä ja sähköisen viestinnän tietosuojalaki. Tällainen ”hajasijoittelu” kuitenkin vaikeuttaa tietoturvatyön toteuttamista. Suomen lainsäädännössä tietoturvan lainsäädöllinen kehys alkaa perustuslain määritelmistä ja päättyy päätöksiin, jotka ministerit tekevät. Perustuslaissa on määritelty kansalaisten perusoikeudet, ja perustuslaki määrittelee yksityisyydensuojan, joka tulee ottaa huomioon tietoturvatoimenpiteitä tehtäessä. (Laaksonen et al. 2006, 21, 27-28.)

2.2 Periaatteet

Tietoturvaa voidaan kuvata kolmella kirjaimella C-I-A. C tarkoittaa tässä tiedon luottamuksellisuutta (confidentality), I tarkoittaa eheyttä (integrity) ja A saatavuutta (availability). Lisäksi voidaan puhua todentamisesta (authentication), pääsynvalvonnasta (access control) sekä toimien kiistämättömyydestä (non-repudiation). (Järvinen 2002, 22-27.)

Mitä C-I-A periaatteella tarkoitetaan? C-I-A periaatteella pyritään luottamuksellisuuteen, joka merkitsee sitä, että ulkopuolinen henkilö ei pääse käyttämään tietoa, jota ei ole tarkoitettu hänelle. Lisäksi tietoja voivat lukea ja muokata vain ne, joilla on oikeus päästä kyseisiin tietoihin käsiksi. Ensin on suoritettava todennus, jotta tietoihin käsiksi pääsevät käyttäjät voidaan tunnistaa. Jotta tieto pysyy ulkopuolisilta suojattuna, tarvitaan salausmenetelmää. Salausmenetelmän avulla voidaan varmistaa, että tieto ei paljastu vaikka joku onnistuisi salakuuntelemaan tiedonsiirtoyhteyttä tai varastaisi tietokoneen. (Järvinen 2002, 22.)

C-I-A periaatteella pyritään myös tiedon eheyteen, joka tarkoittaa sitä, että ulkopuolinen taho ei pysty luvatta muuttaman tietoja, kuten poistamaan tiedostoja tai tekemään niihin muutoksia. Eheys on tärkeää muun muassa silloin, kun tietoja arkistoidaan. Ar-

kistointi on suoritettava niin, että kukaan ei pysty muuttamaan tietoja myöhemmin. (Järvinen 2002, 22-24.)

Kolmantena periaatteena voidaan puhua tietojen ja palvelujen saatavuudesta, jolla tarkoitetaan tietojärjestelmien toiminnan turvaamista. Tietokoneiden ja yhteyksien pitää toimia aina silloin, kun niitä halutaan käyttää. Tiedon saatavuuteen saattaa kohdistua myös ongelmia sellaisissa tapauksissa, kun tiedostot ovat esimerkiksi 10 - 15 vuotta vanhoja. Tällöin tiedostojen avaamiseen tarvittavia sovelluksia ei ehkä ole enää tallella tai silloin käytetyt ohjelmat eivät toimi nykyaikaisissa koneissa. (Järvinen 2002, 24.)

Tietoturvan muihin osa-alueisiin kuuluvat todentaminen, pääsynvalvonta ja kiistämättömyys. Todentamisella (authentication) voidaan varmistua olion aitoudesta eli siitä, että olio on juuri se mitä pitääkin. Todentamisen voidaan sanoa olevan arkipäiväinen ilmiö. Sähköpostissa todentaminen perustuu lähettäjäosoitteeseen, mutta tällainen todentamistapa on turvaton, koska kuka tahansa voi väärentää osoitteen. Pääsynvalvonnalla (access control) tarkoitetaan sitä, että vain todennetut henkilöt pääsevät järjestelmän tietoihin käsiksi. Nykypäivänä on paljon sähköistä kaupankäyntiä ja tällöin kauppiaan on voitava todistaa, että tavara on lähetetty häneltä tilaajalle. Tällöin voidaan puhua kiistämättömyydestä (non-repudiation). (Järvinen 2002, 24-28.)

2.3 Tietoturvallisuuden parantaminen

Jotta mahdollisia tietoturvariskejä voidaan pienentää tai poistaa kokonaan, ne on ensin tunnistettava. On ymmärrettävä millaisia tietoturvariskejä esimerkiksi tietokoneeseen tai sähköpostiin liittyy. Tietämättömyyttä tai välinpitämättömyyttä voidaan pitää seikkoina, joista tietoturvaongelmat yleensä johtuvat. (Keskusrikospoliisi 2008, 15.)

Ensimmäinen keino parantaa tietoturvallisuutta on rajata käyttöoikeudet vain määrätylle ryhmälle eli yrityksissä esimerkiksi työntekijöille, jotka tosiasiassa tarvitsevat tietokonetta. Käyttöoikeuden rajaamisen jälkeen on hyvä ottaa käyttöön salasana- ja käyttäjätunnusyhdistelmä, jotka ovat henkilökohtaisia eivätkä ole ulkopuolisten tiedossa. Turvallisuutta voidaan parantaa myös pitämällä tietokoneen ohjelmisto ajan

tasalla ja käyttämällä palomuuria. Olennaisena osana tietoturvan parantamisessa on henkilöstön kouluttaminen ja työntekijöiden luotettavuus. (Keskusrikospoliisi 2008, 15).

Tehokas tapa suojata salassa pidettäviä yrityksen tietoja on turvallisuuskulttuurin ja henkilöstöpolitiikan rakentaminen. Työntekijöitä tulisi perehdyttää siihen, mikä on luottamuksellista tietoa ja mikä ei. Yrityssalaisuuksien ei pitäisi olla kaikkien työntekijöiden nähtävillä. Työntekijöiden siirtyessä kilpailevien yritysten palvelukseen yrityssalaisuuksia saattaa tällä tavoin siirtyä uudelle työnantajalle. Tyytymätön työntekijä ja työsuhteen päättyminen esimerkiksi irtisanomisen johdosta lisäävät turvallisuusriskejä. Työntekijä voi näissä tapauksissa vuotaa yrityssalaisuuksia, kopioida luvatta tietoja tai hävittää tarpeellista tietoa. Jotta yrityssalaisuuksia pystytään edes jotenkin suojelemaan, työntekijän kanssa voidaan tehdä salassapitosopimus. (Saario 2009, 8-9.)

Lainsäädäntö luo puitteet tietoturvallisuuden tehokkaalle valvonnalle. ”Vanhan” sähköisen viestinnän tietosuojalain mukaan yritykset eivät saa itse selvittää viestintäverkkoihin kohdistuneita tai niiden avulla tapahtuneita väärinkäytöksiä. (Keskusrikospoliisi 2008, 17.) ”Uusi” sähköisen viestinnän tietosuojalaki antaa yhteisötilaajille oikeuden käsitellä tunnistamistietoja, mikäli epäillään yrityssalaisuuksien luvatonta paljastamista. (HE 48/2008[viitattu 23.9.2009].)

Suomessa tietoturvan taso on hyvä verrattuna moneen muuhun maahan. Suomessa on myös laaja tietoturvateollisuus, sanoo tietoturvayritys F-Securen tutkimusjohtaja Mikko Hyppönen. Kansallisen tietoturvastrategian mukaan Suomesta on povattu tietoturvan edelläkävijämaata vuonna 2015. (Lagus 2009, 24.)

2.4 Tilastotietoa yrityksiin kohdistuvista tietomurroista

Voidaan sanoa että jokaisella yrityksellä on koosta tai toimialasta riippumatta tietoa, joka luokitellaan yrityssalaisuuden piiriin. Toisinaan yritysten ei ole helppo tunnistaa suojattavaa tietoa ja luokitella sitä asianmukaisin tavoin. Yrityksen henkilöstön pitäisi arvioida, mikä tieto suojataan ja miten se tehdään sekä mitkä ovat seuraamukset, jos

tietoa ei suojata. Mikäli yritys joutuu tietomurron kohteeksi, se saattaa aiheuttaa yrityksen maineen ja kilpailuaseman menetyksen. Tietomurron voi tehdä ulkopuolinen henkilö tai yrityksen työntekijä. (Yritysten rikosturvallisuus 2008, 22.)

Joka neljännessä yrityksessä on havaittu, että ulkopuolinen on luvattomasti yrittänyt päästä käsiksi tietoverkkoon. Lähes joka toisessa suuressa yrityksessä on havaittu murtautumisyritys yrityksen tietoverkkoon. Miksi sitten isompiin yrityksiin yritetään murtautua tai hakkeroitua useammin? Syy lienee siinä, että isommat yritykset ovat tunnettuja ja siten kiinnostavia kohteita. Mikäli hakkeroija onnistuu pääsemään käsiksi tietoverkkoon, on myös teon julkisuus suurempi. Noin kuudesosa pienien tai keskikokoisten yritysten työntekijöistä ja 11 % suurten yritysten työntekijöistä ei osannut sanoa, onko yritysten tietoverkkoon yritetty murtautua. Vaikka edellä mainitut tilastot kertovat, että tietomurron yrityksiä tapahtuu paljon, suurin osa murroista jää yritykseksi. Vain kolme prosenttia yrityksistä on joutunut todellisen tietomurron kohteeksi, ja suurissa yrityksissä vastaava luku on yksi prosentti. (Yritysten rikosturvallisuus 2008, 22-23.)

Yrityksiin kohdistuu useita muitakin riskejä kuin tietoverkkoon murtautuminen. Eräs näistä riskeistä on, että henkilökuntaan kuuluva on mennyt kertomaan yrityksen yksityisasioista luvatta kolmannelle osapuolelle. Toisena riskinä voidaan pitää sitä, että käyttäjä luovuttaa luvatta yksityisasiaa sisältävän asiakirjan kolmannelle taholle. Kolmantena riskinä pidetään tiedostojen tahallista tuhoamista ja neljäntenä yritykseen liittyvää tietojen luvatonta muuttamista tai väärentämistä. Suuressa osassa yrityksiä ainakin yksi edellä mainituista riskeistä on toteutunut. (Yritysten rikosturvallisuus 2008, 26.)

Tietoturvasta ja siihen liittyvistä riskeistä puhuttaessa voidaan puhua myös sähköisen viestinnän tietosuojalaista. Sähköisen viestinnän tietosuojalaista on puhuttu paljon viime kuukausina. Lakia on ehdotettu muutettavaksi ja lainmuutos astui voimaan kesällä 2009.

3 SÄHKÖISEN VIESTINNÄN TIETOSUOJALAKI

3.1 Määritelmät

Sähköisen viestinnän tietosuojalain avulla pyritään turvaamaan viestien luottamuksellisuus ja yksityisyyden suojan toteutuminen. Edellä mainitun lisäksi sen avulla edistetään sähköisen viestinnän tietoturvaa ja sähköisen viestinnän palvelujen tasapainoista kehittymistä. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 23.9.2009].) Otan esille muutamia tärkeimpiä sähköisen viestinnän tietosuojalain määritelmiä, joita käsittelen työssäni.

Viesti. Viestillä tarkoitetaan osapuolten välistä tai vapaasti valikoituvalle vastaanottajajoukolle välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, viestiä jossa on puhetta tai muuta vastaavaa viestiä.
Viestintäverkko. Järjestelmä joka koostuu toisiinsa liitetyistä johtimista ja laitteista.
Teleyritys. Teleyrityksellä tarkoitetaan verkkoyritystä tai palveluyritystä.
Verkkopalvelu. Verkkopalvelulla tarkoitetaan viestien siirtämistä, jakelemista tai tarjolla pitämistä viestintäverkossa. Käyttäjäpiiriä ei ole rajoitettu.
Tunnistamistieto. Tietoa, joka yhdistetään tilaajaan tai käyttäjään. Tunnistamistietoa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.
Paikkatieto. Ilmaisee liittymän tai laitteen maantieteellisen sijainnin.
Tilaaja. Oikeushenkilöä tai luonnollista henkilöä voidaan kutsua tilaajaksi. Tällainen henkilö on tehnyt sopimuksen viestintäpalvelun tai lisäarvopalvelun toimittamisesta.
Yhteisötilaaja. Yritys tai yhteisö, joka käsittelee käyttäjien luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja.
Tietoturva. Toimia, joilla varmistetaan että tiedot ovat niiden saatavilla, jotka ovat oikeutettuja tiedon käyttöön. Tietoja eivät voi muuttaa kuin siihen oikeutetut ihmiset, ja tiedot ovat hyödynnettävissä, kun niitä tarvitaan. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 23.9.2009].)

3.2 Laki alkuperäisenä

Yksityisyys ja luottamuksellisuus. Lain mukaan viesti, tunnistamistiedot (myös verkkosivustojen selaamisesta kertyvät tiedot) ja paikkatiedot ovat luottamuksellisia, jollei toisin säädetä. Mikäli viesti on kaikkien vastaanotettavissa, se ei ole luottamuksellinen. Tunnistamistiedot, jotka liittyvät viestiin ovat kuitenkin luottamuksellisia. Vaitiolovelvollisuudesta voidaan puhua siinä yhteydessä, kun ihminen on saanut tiedon luottamuksellisesta viestistä tai tunnistamistiedosta. Tällöin hän ei saa ilman toisen osapuolen suostumusta ilmaista tai käyttää hyväksi viestin sisältöä tai tunnistamistietoa. Sama pätee myös paikkatietoihin. Käyttäjä voi suojata viestit ja tunnistamistiedot haluamallaan tavalla, ja tätä varten on tarjolla teknisiä mahdollisuuksia. Suojaus ei kuitenkaan saa häiritä verkkopalvelun ja viestintäpalvelun käyttöä ja toteuttamista. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 23.9.2009].)

Viestien ja tunnistamistietojen käsittely. Viestin lähettäjä tai vastaanottaja voi käsitellä omia viestejään ja niihin liittyviä tunnistamistietoja. Jos kyse on luottamuksellisesta viestistä tai tunnistamistiedosta, tällaisia viestejä saa käsitellä vain viestin lähettäjän tai vastaanottajan suostumuksella. Käsittelyä voi tapahtua myös laskutusta, markkinointia, teknistä kehittämistä, väärinkäytöstä, teknisen vian tai virheen havaitsemista ja tietojen tallentamista varten. Näissä tapauksissa käsittely on sallittua vain tarkoituksen edellyttämässä laajuudessa. Pitää ottaa huomioon myös se, että luottamuksellisen viestin ja yksityisyyden suojaa ei saa rajoittaa enempää kuin on välttämätöntä. Lisäksi tunnistamistietoja saa luovuttaa vain niille, joilla on oikeus käsitellä tietoja. Käsittelyn jälkeen on noudatettava tarkkaavaisuutta viestien ja tunnistamistietojen kanssa. Ne on hävitettävä tai on huolehdittava, ettei niitä voi yhdistää tilaajaan tai käyttäjään. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 23.9.2009].)

Paikkatiedot. Teleyritykset, lisäarvopalvelun tilaajat ja yhteisötilaajat sekä näiden lukuun toimivat henkilöt saavat käsitellä paikkatietoja, mikäli ne tarjoavat tai hyödyntävät lisäarvopalveluja. Säännöksiä ei kuitenkaan sovelleta paikkatietoihin, jos niitä ei voida yhdistää tilaajaan tai käyttäjään, ellei laissa toisin säädetä. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 23.9.2009].)

Viestinnän tietoturva. Teleyrityksellä, lisäarvopalvelun tarjoajalla tai yhteisötilaajalla on oikeus huolehtia tietoturvasta. Heillä on oikeus ryhtyä toimiin, jotta tietoturvan tasosta voidaan olla varmoja. Nämä tahot voivat estää sähköpostien, tekstiviestien ja muiden viestien välittämisen ja vastaanottamisen tai he voivat poistaa tietoturvaa uhkaavat haittaohjelmat ja toteuttaa muut teknisluonteiset toimet, jotka ovat tarpeen. Pitää ottaa huomioon, että toimiin saa ryhtyä vain, mikäli ne ovat välttämättömiä verkkopalvelujen, viestintäpalvelujen tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi. Viestin sisältöön saa puuttua teknisin keinoin, jos on syytä epäillä viestin sisältävän tietokoneohjelman tai ohjelmakäskyjen sarjan tai viestiä käytetään tietoliikenteen häirintään. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 23.9.2009].)

Ohjaus ja valvonta. Viestintävirasto valvoo lain ja sen nojalla annettujen säännösten ja määräysten noudattamista. Lisäksi se kerää tietoa tietoturvaloukkauksista ja niihin liittyvistä uhista sekä tiedottaa tietoturva-asioista. Tietosuojavaltuutettu puolestaan valvoo paikkatietojen käsittelyä, puhelinluetteloita, suoramarkkinointia koskevien säännösten noudattamista sekä tiedonsaantioikeuksia ja vaitiolovelvollisuutta paikkatietojen osalta. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 23.9.2009].)

Tiedonsaantioikeus. Liikenne- ja viestintäministeriöllä, viestintävirastolla ja tietosuojavaltuutetulla on oikeus saada välttämättömät tiedot salassapitosäännösten tai muiden rajoitusten estämättä, jotta kyseiset tahot pystyvät hoitamaan laissa säädetyt tehtävät. Tiedot he saavat muun muassa teleyritykseltä, lisäarvopalvelun tarjoajalta, yhteisötilaajalta, teleurakoitsijalta, palvelun tarjoajalta ja suoramarkkinoinnin harjoittajalta. Kaikki tiedot, jotka he ovat saaneet, on pidettävä salassa. Nämä tahot saavat kuitenkin ilmaista joitakin tietoja hätäilmoituksia vastaanottaville viranomaisille sekä poliisille. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [viitattu 23.9.2009].)

3.3 Muutoksen aikakausi

3.3.1 Lähtökohdat

Kaikki alkoi jo huhtikuussa 2005, jolloin keskusrikospoliisi sai rikosilmoituksen. Rikosilmoituksen oli tehnyt matkapuhelinjätti Nokia, joka on maailman suurin matkapuhelimien valmistaja. Nokian verotuotot ovat 1.3 miljardia euroa ja se työllistää 16 000 ihmistä. Rikosilmoituksessa epäiltiin, että kiinalaiselle Huawei-yhtiölle oli vuodettu Nokian yrityssalaisuuksia. Helmikuussa 2005 Cannesissa järjestettiin tietoliikennealan messut. Messuilla Nokian työntekijä huomasi, että kiinalaisen kilpailijan Huawein verkkolaitteessa oli jo ominaisuuksia, joita Nokia esitteli messuilla vasta ensi kertaa julkisesti. (Welp 2009 [viitattu 30.9.2009].)

Jotta Nokia saisi selville ketkä ovat paljastaneet tietoja julkisuuteen, Nokialla alettiin penkoa työntekijöiden sähköpostin tunnistamistietoja. Oikeusoppineet olivat sitä mieltä, että tietojen penkominen ei ollut laillista. Nokia loukkasi työntekijöiden perusoikeutta, johon kuuluu luottamuksellinen viestintä. Yhtiön johto oli kuitenkin sitä mieltä, että laki on väärässä, ei Nokia. Nokia vaati lainmuutosta. Mikäli lakia ei muutettaisi, yhtiö uhkasi lähteä Suomesta ja viedä mukanaan valtavat verotuotot sekä 16 000 ihmistä menettäisi työpaikkansa. Nokian antama uhkaus sai poliitikkoihin vauhtia ja näin sai alkunsa Lex Nokia. Lex Nokiaa voidaan kutsua myös Urkintalaiksi. Urkintalaki nimityksen ovat antaneet kansalaisjärjestöt, jotka vastustavat Lex Nokiaa. (Welp 2009 [viitattu 30.9.2009].)

3.3.2 Seuraukset yhteiskunnan kannalta

Millaisen lakiesityksen hallitus esitti eduskunnalle? Lainmuutos koskisi vain sähköposteja, jotka on lähetetty yrityksen tietokoneelta. Laki antaisi työnantajalle oikeuden tarkkailla työntekijöiden lähettämien sähköpostien tunnistamistietoja. Tunnistamistietoja ovat viestin lähettäjä ja vastaanottaja, viestin ja sen liitteenä olevien tiedostojen koko, kellonaika ja liitetiedoston muoto. Työnantajan suorittaessa kyseistä tarkkailua, hänen ei tarvitse pyytää keneltäkään lupaa, mikäli uusi sähköisen viestinnän tie-

tosuojalaki astuu voimaan. Niin sanottu urkintaoikeus tulisi työnantajien lisäksi virastoille, kirjastoille, yliopistoille, kouluille ja jopa taloyhtiöihin, joilla on oma viestintäverkko. Isännöitsijä voisi tarkkailla asukkaiden internetin käyttöä, jos on syytä epäillä, että verkkoa käytetään taloyhtiön sääntöjen vastaisesti. (Welp 2009 [viitattu 30.9.2009].)

Uudella sähköisen viestinnän tietosuojalailla olisi sekä hyvät että huonot puolensa. Sen ristiriitana voitaisiin pitää sitä, että tunnistamistiedot eivät kerro, onko viestissä yrityssalaisuuksia vai ei. Uusi laki ei antaisi työnantajille mahdollisuutta lukea viestejä. (Welp 2009 [viitattu 30.9.2009].) Mutta mitä hyötyä pelkistä tunnistetiedoista on, kun viestin sisältöä ei voi selvittää? Työnantajat voivat tehdä uskottavan rikosilmoituksen poliisille yrityssalaisuuksien loukkaamisesta. Rikosilmoitusta antaessaan heidän ei tarvitse pelätä, että he antavat perättömän ilmiannon, koska heillä on kuitenkin sähköpostin tunnistetiedot hallussaan. (Alinen a 2009, 45.)

Ennen sähköpostien seurannan aloittamista yritysten tulisi parantaa tietoturvaa, tiedottaa seurannan aloittamisesta työntekijöille ja tehdä ilmoitus tietosuojavaltuutetulle, joka valvoo toimintaa (LIITE 2-4). Yritysten tulisi myös raportoida seurannan tuloksista vuosittain tietosuojavaltuutetulle. Jotta seuranta voitaisiin ylipäätään aloittaa, yrityssalaisuuksien liiketaloudellisen merkityksen pitää olla tarpeeksi suuri. (Alinen a 2009, 45.)

Uusi sähköisen viestinnän tietosuojalaki saattaisi säännöksen vastaamaan paremmin nykyisiä tarpeita, muun muassa viestintäverkkojen ja palvelujen tietoturvasta huolehtimiseksi. Yhteiskunnan eri toiminnot ovat riippuvaisia viestintäverkoista, viestintäpalveluista ja tietojärjestelmistä. (HE 48/2008 [viitattu 30.9.2009].)

Esityksellä olisi luultavasti positiivisia taloudellisia vaikutuksia teleyrityksille, yhteisötilaajille (yritys tai yhteisö), viranomaisille ja kuluttajille. Tiedonsaantia ja käsittelyä koskevat yksiselitteiset ja selkeät säännökset vähentäisivät turhia prosesseja ja säästäisivät toimijoiden resursseja. Uusi lakiehdotus tarjoaisi paremmat edellytykset

sähköiselle asioinnille ja sähköisiä palveluja käyttävien kuluttajien asema paranisi ja viranomaisten asema vastaavasti helpottuisi. (HE 48/2008 [viitattu 30.9.2009].)

Uudella lailla olisi myös vaikutuksia yritystoiminnan kannalta. Uuden lain myötä tunnistamistiedon käsittelyoikeudet selkeytyisivät, mikä poistaisi tulkintaepäselvyyksiä. Yhteisötilaajat pystyisivät paremmin torjumaan viestintäverkkojen ja palvelujen ohjeiden vastaisesti tapahtuvaa tai luvatonta käyttöä. Uudistuksella pystyttäisiin turvaamaan aiempaa paremmin tuotekehitystyön jatkuminen tietovuodoista huolimatta, kun yhteisötilaaja pystyisi rajaamaan tietovuodosta epäiltyjen piiriä. Teleyritykset voisivat luovuttaa tunnistamistietoja yhteisötilaajille tilastollista analyysiä varten ja tämän seurauksena teleyrityksille tulisi uusia liiketoimintamahdollisuuksia. Teleyritykset, lisäarvopalveluja tarjoavat yritykset ja yhteisötilaajat saisivat mahdollisuuden kehittää toimintaansa, torjua rikollisuutta sekä ylläpitää tietoturvaa. (HE 48/2008 [viitattu 30.9.2009].)

Uuden sähköisen viestinnän tietosuojalain vaikutukset ulottuisivat myös viranomaisten toimintaan. Uudessa ehdotuksessa muutettaisiin Viestintäviraston ja tietosuojavaltuutetun tehtävänjakoa sellaisissa tapauksissa, joissa on kyse yhteisötilaajien tunnistamistietojen käsittelystä väärinkäytöstapauksissa. Säännösten täsmentämisen myötä Viestintävirasto ja tietosuojavaltuutettu saisivat työlleen selkeämmät puitteet, mikä tehostaisi lain valvontaa ja sen tavoitteiden toteutumista. Ehdotuksen myötä myös kansainvälistä yhteistyötä edistettäisiin. Viestintävirastolle annettaisiin tällöin oikeudet luovuttaa tietoturvaloukkauksia koskevia tunnistamistietoja muissa valtioissa toimiville CERT-FI yksikköä vastaaville elimille, jotka ennalta ehkäisevät ja selvittävät viestintäverkkoihin ja - palveluihin kohdistuvia tietoturvaloukkauksia. (HE 48/2008 [viitattu 30.9.2009].)

Yhteiskunnalliset vaikutukset olisivat huomattavia. Uuden lain myötä täsmentyisivät viestinnän eri osapuolten oikeudet ja velvollisuudet. Erityisesti kuluttajien ja yritysten luottamus sähköiseen viestintään ja sähköiseen liiketoiminta- ja asiointiympäristöön kohenisi. Lisäksi yritysten ja yhteisötilaajien toimintamahdollisuudet paranisivat ja voitaisiin huolehtia aiempaa paremmin yhteisötilaajien järjestelmien käytettävyydestä

ja tietoturvasta. Samalla yksityisyyden suojaa koskevat lain alkuperäiset tavoitteet tulisi täytettyä. Yrityssalaisuuksien suojan parantaminen lisäisi yritysten toimintamahdollisuuksia, ja edistäisi taloudellista kehitystä sekä hyvinvointia. Toimintamahdollisuuksien paraneminen kotimaassa edesauttaisi kansainvälistä toimintaa. (HE 48/2008 2009 [viitattu 30.9.2009].)

Tietoyhteiskunnan kannalta vaikutukset olisivat vähäisemmät. Pitkällä aikavälillä viestintäverkon käytön suunnittelu, tietoturvariskeiltä suojautuminen ja yritysten kannalta tärkeän tietoaineiston suojaaminen parantuisivat. (HE 48/2008 [viitattu 30.9.2009].)

On itsestään selvää, että uudella lailla olisi myös vaikutuksia yksilön asemaan. Yksityisen viestinnän ja sähköisen asioinnin sekä yhteisötilaajien tarpeita sovitellaan yhteen siten, että yhteisötilaajat (yritys tai yhteisö) voivat sallia viestintäverkkojen käytön myös henkilökohtaisten asioiden hoitamiseen, ilman että yhteisötilaajien pitäisi tinkiä verkon turvallisuudesta. Työntekijöille on tiedotettava, missä tilanteissa yhteisötilaaja saa tutkia sähköpostiliikennettä. Viestin sisältöä yhteisötilaaja ei saa tutkia. (HE 48/2008 [viitattu 30.9.2009].)

Millainen on työntekijöiden suoja? Onko työntekijöillä mahdollisuutta sanoa oma mielipide lainmuutoksesta? Käsittääkseni työntekijöiden mielipiteitä asiassa ei ole kuunneltu, mikä olisi ollut järkevää, koska lakimuutos kohdistuu juuri työntekijöihin ja heidän käyttämään sähköpostiin. Avoimeksi, vaille vastausta minulle jää kysymys, ketkä puolustavat työntekijöiden etua, ovatko ne työsuojeluvaltuutetut?

Uudistettu tietosuojalaki tulee koskemaan alle sataa yritystä Suomessa. Lainmuutoksen tarkoituksena on yllyttää yrityksiä huolehtimaan entistä paremmin tietoturvastaan. Yritykset antavat yleensä työntekijöiden käyttöön tietokoneen, mikä tarkoittaa sitä, että yritys omistaa tietokoneen. Tietokoneen omistajalla tulee olla mahdollisuus opastaa tietokoneen käyttöä ja valvoa, että työntekijät noudattavat sääntöjä. (Himanen 2009 [viitattu 30.9.2009].)

Työnantajien ja työntekijöiden tulee sopia pelisäännöistä, kuten siitä että minkälaisia automaattisia hakutoimintoja koneisiin voidaan asentaa. Automaattisten hakutoimintojen avulla pyritään paljastamaan väärinkäytöksiä. Jos haku löytää poikkeavia tietoja, niin siitä on ilmoitettava työntekijälle, ja vain ne henkilöt pääsevät käsiteltäviin tietoihin käsiksi, joilla on siihen ennalta sovittu lupa. Työnantaja ei kuitenkaan voi haun avulla seurata, mihin työntekijä on ottanut yhteyttä. Hakua ei ole sallittua kohdistaa myöskään siten, että sen avulla saataisiin selville lähdesuojan piiriin kuuluvia tietoja. (Himanen 2009 [viitattu 30.9.2009].)

Automaattinen käsittely voidaan ottaa käyttöön, kun ennakkovelvoitteet on täytetty ja edellytykset tunnistamistietojen käsittelylle ovat täyttyneet. Automaattista hakua ei saa käyttää yksittäisten viestinnän osapuolten seurantaan, vaan kyseessä tulee olla väärinkäytöksiin viittaavien poikkeaminen havaitseminen. Automaattista hakua käytettäessä yksittäisen käyttäjän tunnistamistiedot eivät saa paljastua tunnistamistietojen käsittelijälle. Tunnistamistietoja voidaan käsitellä myös manuaalisesti. Manuaalinen käsittely tapahtuu ihmistyövoimin tietyn käyttäjän yhteysosoitteen tai tietyn käyttäjäjoukon yhteysosoitteiden tunnistamistietoihin. Manuaalisen käsittelyn voidaan sanoa olevan väärinkäytösepäilyn tapauskohtaista selvittämistä. Tunnistamistiedot, joista aiheutuu merkittävää haittaa tai vahinkoa tai keskeisen yrityssalaisuuden paljastumista, saa ottaa manuaalisesti käsiteltäviksi. Lisäksi manuaalisen käsittelyn edellytyksenä on, että tiedot ovat välttämättömiä väärinkäytöksen tai siitä vastuussa olevan selvittämiseksi tai luvattoman käytön lopettamiseksi. (Asiaa tietosuojasta 1/2009 [viitattu 15.2.2010].)

3.3.3 Sähköisen viestinnän tietosuojalaki nyt

Eduskunta hyväksyi uuden sähköisen viestinnän tietosuojalain ja se tuli voimaan 1.6.2009. Uuden lain mukaan yhteisötilaajat saavat käsitellä tunnistamistietoja yhteisötilaajan oman tietoliikenneverkon ja siihen liitettyjen palvelujen luvattoman käytön estämiseksi. Elinkeinonharjoittajat saavat myös käsitellä tunnistamistietoja, jotta voitaisiin estää yrityssalaisuuksien oikeudeton paljastaminen. Laki ei salli yhteisötilaajien kajota itse viestien sisältöön. Millaisia tunnistetietoja saa sitten käsitellä? Käsittelyoi-

keus koskee tapauksia, joissa tietoja käsitellään luvatta tai yrityssalaisuuksien paljastamista viestintäverkossa, viestintäpalvelussa tai maksullisessa tietoyhteiskunnan palvelussa. (Karppinen 2009, 9.)

Mielenkiintoinen kysymys on, voidaanko uudella tietosuojalailla estää sekä ulkopuolelta tulevia että työyhteisön sisäpuolelta tulevia uhkia. Työyhteisön sisäpuolisiin uhkiin voidaan lukea työntekijän liiallinen avoimuus yrityksen asioista, eli työntekijä levittää yrityksen sisäisiä tietoja ulkopuolisille. Lisäksi työntekijä voi tallentaa muistitikulle yrityssalaisuutena pidettävää tietoa. Sisäpuolisia uhkia voivat olla myös työntekijän huolimattomuus ja välinpitämättömyys yrityksen asioita kohtaan. Sähköisen viestinnän tietosuojalain uudistuksella ei voida puuttua edellä mainittuihin asioihin, koska uusi laki koskee vain tunnistamistietojen käsittelyä sähköpostiin liittyvissä tilanteissa. Ulkopuolisia uhkia voivat olla hakkerit, jotka yrittävät päästä yrityksen tietoihin käsiksi. Lisäksi erilaiset tietokonevirukset, ja mahdolliset tietokonekaappaukset voivat vaarantaa yrityksen tietoturvallisuutta. Ulkopuolisiin uhkiin ei voida myöskään puuttua uudella lailla.

Viestintäverkon ja viestintäpalvelun luvatonta käyttöä on sähköisen viestinnän tietosuojalain 13a §:n 2 momentin mukaan laitteen, ohjelman tai palvelun asentaminen yhteisötilaajan viestintäverkkoon, jollekin sivulliselle oikeudettomasti pääsyn avaaminen yhteisötilaajan viestintäverkkoon tai viestintäpalveluun tai jokin muu näihin rinnastettavissa oleva viestintäverkon tai viestintäpalvelun käyttäminen. Jotta käyttö voidaan luokitella luvattomaksi, sen tulee olla käyttäjille väärinkäytösten ehkäisemiseksi annettujen kirjallisten ohjeiden vastaista. Yrityssalaisuudella voidaan tarkoittaa liike- tai ammattisalaisuutta tai muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittajan tulee pitää salassa. Mikäli elinkeinonharjoittaja ilmaisee tiedon, se voisi olla omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle. Keskeisiin yrityssalaisuuksiin voidaan lukea tiedot, jotka antavat yritykselle kilpailuedun ja joita ei pysty selvittämään julkisista lähteistä sekä tiedot, jotka ovat merkittäviä elinkeinotoiminnan käynnistämisen ja sen harjoittamisen kannalta. (Asiaa tietosuojasta 1/2009 [viitattu 15.2.2010].)

Ennen kuin yhteisötilaaja voi aloittaa tunnistamistietojen käsittelyn, sen on täytettävä huolehtimis-, suunnittelu- ja yhteistoimintavelvoitteet sekä tehtävä ennakkoilmoitus tietosuojavaltuutetulle. Yhteisötilaajan on määriteltävä minkälaisia viestejä sen viestintäverkon kautta saa lähettää ja hakea. Lisäksi sen on määriteltävä miten viestintäverkkoa ja – palvelua saa muutoin käyttää, ja millaisiin kohdeosoitteisiin viestintää ei saa harjoittaa. Pääsyä viestintäverkkoon ja – palveluihin on rajoitettava, ja nämä on suojattava tietoturvatoimenpitein. Tunnistamistietoihin kohdistuvaa valvontaa voidaan suorittaa vain silloin, kun luvatonta toimintaa ei voida estää etukäteistoimilla. (Karppinen 2009, 9-10.)

Huolehtimisvelvollisuuteen kuuluu se, että yhteisötilaaja ei voi aloittaa tunnistamistietojen käsittelyä ennen kuin se on ottanut käyttöön kaikki asianmukaiset lain sallimat tietohallinnolliset keinot. Tietohallinnollisilla keinoilla voidaan pyrkiä estämään tietoyhteiskunnan palvelujen, viestintäpalvelujen ja viestintäverkon luvaton käyttö tai yrityssalaisuuksien paljastaminen ulkopuolisille ihmisille. Erillinen huolehtimisvelvollisuus ennen tunnistamistietojen käsittelyä korostaa yhteisötilaajan velvollisuutta suojata oma viestintäverkko, viestintäpalvelu ja yrityssalaisuutensa paremmin kuin mitä yleisissä huolehtimisvelvollisuuksissa edellytetään. Huolehtimisvelvollisuuden noudattamisesta voidaan sanoa konkretisoituvan myös käyttäjille tunnistamistietojen käsittely edellytyksenä olevan haitan tai vahingon aiheutumisen kriteeriä, tai keskeisen yrityssalaisuuden määritelmää. (Asiaa tietosuojasta 1/2009 [viitattu 15.2.2010].)

Suunnitteluvaihe pitää sisällään sen, että ennen tunnistamistietojen käsittelyn aloittamista yhteisötilaajan tulee nimetä ne henkilöt, joiden tehtäviin tunnistamistietojen käsittely kuuluu tai ainakin hänen tulee määritellä kyseiset tehtävät tai toimintayksiköt. Tunnistamistietojen käsittely voidaan luovuttaa ulkopuolisen palveluntarjoajan toteutettavaksi. Edellä mainitussa tilanteessa yhteisötilaaja määrittelee palveluntarjoajan tehtävät ja toiminnot ja huolehtii siitä, että tunnistamistietojen käsittelyoikeudelle väärinkäytöstapauksissa asetetut edellytykset täyttyvät. Yhteistoiminta- ja kuulemismenettelyn piiriin voidaan lukea seuraavat käsittelyn keskeiset kysymykset: mikä on tunnistamistietojen käsittelyn tarkoitus, millaisia ovat viestintäverkon käytöstä laaditut ohjeet, ketkä ovat tunnistamistietojen käsittelijät ja mitkä ovat heidän tehtävänsä, mit-

kä ovat automaattisen haun toimintaperiaatteet ja tunnistamistietojen manuaalisen käsittelyn edellytykset. (Asiaa tietosuojasta 1/2009 [viitattu 15.2.2010].)

Laissa on määritelty rajoituksia tunnistamistietojen käsittelylle. Jotta viestinnän osapuolten henkilöllisyys ei paljastuisi, tunnistamistietojen käsittelyn pitää tapahtua automaattisten hakutoimintojen välityksellä. Käsittelyä ei saa kohdistaa mihinkään tiettyyn ryhmään tai käyttäjään. Yhteisötilaajalla pitää olla myös epäily, jotta hän voi kohdistaa valvonnan juuri tiettyihin henkilöihin. Epäily syntyy yleensä automaattisen hakutoiminnan havaitseman poikkeaman perusteella. (Karppinen 2009, 10.)

Yritykset, jotka haluavat käsitellä tunnistamistietoja yrityssalaisuuksien paljastumisen ehkäisemiseksi, joutuvat noudattamaan lain määräämiä lisävelvoitteita. Tällaisten yritysten on yksilöitävä keskeiset yrityssalaisuudet ja määriteltävä, miten näitä salaisuuksia saa käsitellä viestintäverkossa. Lisäksi yritysten on selvennettävä, minkälaisiin kohdeosoitteisiin yrityssalaisuuksia käsittelemään oikeutetut ihmiset eivät saa lähettää viestejä. (Karppinen 2009, 10.)

Mikäli yhteisötilaaja käsittelee johonkin henkilöön tai ryhmään liittyviä tunnistamistietoja, sen on kerrottava siitä käsittelyn kohteelle heti, kun se voidaan vielä tehdä vaarantamatta väärinkäytöksen selvittämistä. Käsittelyn kohteelle on kerrottava käsittelyn ajankohta, sen kesto, perusteet ja mainittava henkilöt, jotka ovat osallistuneet käsittelyyn. Yhteisötilaajan on säilytettävä edellä mainitut tiedot kaksi vuotta. Tietosuojavaltuutetut valvovat väärinkäytöstapauksia. Ennen kuin yhteisötilaaja voi aloittaa tunnistamistietojen käsittelyn, sen on tehtävä tietosuojavaltuutetulle ilmoitus. Ilmoituksessa tulee käydä ilmi ennakkotoimet, käyttäjille annetut kirjalliset viestintäverkon ja – palvelujen käyttöohjeet ja keskeisten yrityssalaisuuksien käsittelyohjeet. Mikäli yritys on joutunut tekemään yksittäiseen ryhmään tai henkilöön kohdistuvia tunnistamistietojen käsittelyjä, yrityksen on raportoitava tästä tietosuojavaltuutetulle vuosittain erillisellä lomakkeella. (Karppinen 2009, 10.) Liitteeksi olen laittanut kolme lomaketta, joilla voidaan raportoida tunnistamistietojen käsittelyn liittyviä tiedoksiantoja. Liitteet ovat Ennakkoilmoitus tunnistamistietojen käsittelyn aloittamisesta, selvitys muutoksista

tunnistamistietojen käsittelyssä ja selvitys tunnistamistietojen manuaalisesta käsittelystä. (Karppinen 2009, 10.)

Vanha sähköisen viestinnän tietosuojalaki (516/2004) annettiin 16 päivänä kesäkuuta 2004. Uuden lain myötä sen pykäliin tuli muutoksia. Muutokset ovat seuraavanlaisia: 9, 12-14, 20 ja 32§, 33§:n 3 momentin johdantokappale, 34§ ja 42§. Lisäksi lakiin lisätään 12a, 13a-13j ja 34a §. (Eduskunta 2009 [viitattu 30.9.2009].) Voimassaoleva laki ja lakiehdotukset ovat liitteenä LIITE 1.

3.3.4 Perustuslain ristiriidat sähköisen viestinnän tietosuojalain kanssa

Perustuslain 10§:ssä määritellään yksityisyyden suoja seuraavalla tavalla:
”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. 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 tai kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.” (Perustuslaki 11.6.1999/731 [online, viitattu 30.9.2009.)

Voidaan sanoa, että viestin salaisuuden loukkaamattomuus ei tarkoita ehdotonta suojaa viestinnälle. Joissakin lain säätelemissä tapauksissa viestinnän suoja voidaan menettää, kuten esimerkiksi rikollisen toiminnan yhteydessä. Esitutkintaviranomaiset voivat saada luottamuksellista tietoa esimerkiksi väärinkäytöstapausten yhteydessä. (Laaksonen et al. 2006, 28.)

Koska uusi sähköisen viestinnän tietosuojalaki ei anna yhteisötilaajien kajota viestin sisältöön, laki ei riko perustuslain asettamaa yksityisyyden suojaa. Eri asia on, kokevatko työntekijät sen niin, että heidän yksityisyyttään rikotaan, koska työnantajat pystyvät nyt tarkkailemaan sähköpostiviestien tunnistamistietoja. Toisaalta työntekijöiden työsähköpostissa ei pitäisi olla mitään henkilökohtaisia ja salattavia sähköpostivieste-

jä. Olen sitä mieltä, että työntekijöitä pitää informoida riittävästi uudesta lakimuutoksesta. Näin vältytään monilta mieltä askarruttavilta kysymyksiltä. Mikäli työnantaja jostain syystä joutuu puuttumaan työntekijän sähköpostiliikenteeseen, olisi oleellista, että työntekijällä on jo etukäteen tiedossa asiat, millä perusteilla sähköpostiin liittyviin asioihin voidaan puuttua.

3.4 Uudistuksen kritiikkiä ennen lain hyväksymistä

3.4.1 Eduskunnan kanta

Eduskunta puoltaa uuden sähköisen viestinnän tietosuojalain voimaantuloa. Eduskunta hyväksyi muutoksen äänin 96-56 eli enemmistö kannatti lakiuudistusta. Sinä päivänä, kun äänestys tapahtui, poissa oli 47 kansanedustajaa. Poissaolleiden kansanedustajien suurta määrää selittää osaksi se, että kaksi eduskunnan valiokuntaa oli ulkomailla työmatkalla. Erityisesti vihreiden puolue oli lakiuudistusta vastaan. Eduskunnan äänestystuloksen jälkeen laki vietiin presidentin vahvistettavaksi. (YLE uutiset [viitattu 6.10.2009].)

Helsingin Sanomien toimittaja haastatteli heti eduskuntakäsittelyn jälkeen kahta vihreiden edustajaa. Kansanedustaja Jyrki Kasvi totesi haastattelussa että harmittaa, koska lainmuutoksessa on kyse periaatteellisista ongelmista. Vihreiden eduskuntaryhmän puheenjohtaja Anni Sinnemäki keskittyi puhumaan haastattelussa ainoastaan edustajien poissaolosta. Häneltä myös kysyttiin syytä, miksi niin moni on poissa. Sinnemäki totesi, että heidän ryhmässään on ollut kritiikkiä lakia kohtaan. Osa kansanedustajista oli virkamatkalla ja osa ei tullut paikalle, koska heillä ei ole halua tukea uutta lakiehdotusta. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

3.4.2 Elinkeinoelämän keskusliiton suhtautuminen asiaan

1.2.2009 julkaistun artikkelin mukaan Nokialle uuden lain säätäminen olisi ollut niin tärkeää, että se on jopa painostanut lainmuutokseen osallisina olevia ihmisiä. Elinkeinoelämän keskusliitto eli EK oli alusta saakka ollut Nokian pompoteltavissa eli ”juok-

supoikana”. Elinkeinoelämän keskusliitto taas on kiistänyt sen, että se olisi painostanut lain valmistelijoita tai muita, jotka ovat olleet osallisina lainsäädäntötyöhön. (Simula 2009 [viitattu 6.10.2009].)

Elinkeinoelämän keskusliiton lakiasianjohtaja Lasse Laatusen lähettämästä sähköpostiviestistä kuitenkin käy selville, että uhkailua on ollut olemassa. Viestin sisältö sanasta sanaan on seuraava: ” Minun kärsivällisyyteni tämän asian suhteen on loppu. Olisi pitänyt olla jo kauan sitten. Olen ollut turhan pitkämielinen. Ei olisi pitänyt. Tulen haastamaan rikollisten suosijat ja viranomaisvallan väärinkäyttäjät tässä prosessissa. En lepää, ennen kuin he joutuvat vastuuseen ja häpeään. Tiedän heidät.” Viestin hän on lähettänyt akavalaiselle johtajalle, akavalaiselle vaikuttajalle ja EK johtajalle. EK on siis uhkaillut ainakin Akavan johtajistoon kuuluvia henkilöitä, ja se on ollut liikkeellä Nokian puolesta, joko omasta aloitteestaan tai Nokian painostuksen alaisena. Suomen Kuvalehti on saanut tietoja, joiden mukaan työnantajat olisivat painostaneet Akavaa koko lainmuutosprosessin ajan. Liikenne- ja viestintäministeriön valmistelutyöryhmä sai valmiiksi kesällä 2007 lakiesityksen, jonka Akava hyväksyi. (Simula 2009 [viitattu 6.10.2009].)

3.4.3 Oikeusoppineiden mielipiteet

Helsingin Sanomat tiedusteli kahdeksalta perustuslakivaliokunnan käyttämältä oikeusoppineelta, mitä mieltä he ovat Lex Nokiasta. Yleisesti ottaen oikeustieteen asiantuntijat pitävät hallituksen laatimaa esitystä perustuslain vastaisena. Perustuslakivaliokunta on jo aiemmin päättänyt, että uusi sähköisen viestinnän tietosuojalaki ei olisi perustuslain vastainen eli se voitaisiin säätää tavallisen lain säätämisjärjestyksessä. (Sajari 2008 [viitattu 6.10.2009].)

Helsingin yliopiston valtiosääntöoikeuden professorin Tuomas Ojasen mukaan talouselämän vaikutusvalta ja mahtipontisuus veivät ykkössijan ja kansalaisten perusoikeudet jäivät toiseksi. Lappeenrannan teknillisen yliopiston informaatio- ja teknologiaoikeuden professori Jukka Kemppinen on sitä mieltä, että laki olisi pitänyt käsitellä perustuslain säätämisjärjestyksessä. Hänen mielestään laki ei ole riittävän selkeä, mikä

tarkoittaa, että se jättää työnantajalle liian paljon liikkumavaraa. Hän myös toteaa, että laatiessaan lakiehdotusta perustuslakivaliokunta ei ole ottanut asiantuntijoiden lausuntoja huomioon. (Sajari 2008 [viitattu 6.10.2009].)

Useat oikeusoppineet epäilevät, että yrityssalaisuuksien vuotamista ei pystytä kokonaan estämään tunnistamistietojen tarkkailulla. Joensuun yliopiston julkisoikeuden professori Teuvo Pohjolainen on sitä mieltä, että sähköisen viestinnän tietosuojalain esityksessä puututaan keskeisiin perusoikeuksiin ja yksilönoikeuksiin sellaisella perusteella, jota hän ei voi hyväksyä. Yleisen oikeustieteen professori Kaarlo Tuori kieltäytyi sanomasta omaa mielipidettään. (Sajari 2008 [viitattu 6.10.2009].)

Haastatteluista voin huomata, että lainoppineet ovat lähes yhtä mieltä siitä, että uusi sähköisen viestinnän tietosuojalaki puuttuisi ihmisten perusoikeuksiin. Miksi kansalaisten perusoikeudet on lailla turvattu, jos lakia pystyy horjuttamaan Lex Nokian tyyppinen asia? Koko sähköisen viestinnän tietosuojalain uudistushan lähti siitä liikkeelle, kun Nokia uhkasi jättää Suomen, jos lakiin ei puututa ja sitä ei uudisteta. Monta vuotta kestänyt lakiuudistusprosessi sai alkunsa siis varsin mitättömästä asiasta. Tosin tässä tulee ottaa huomioon asian toinen puoli. Jos Nokia olisi lähtenyt Suomesta niin kuin se uhkasi, niin tuhannet ihmiset olisivat menettäneet työpaikkansa, jonka seurauksena Suomeen olisi tullut entistä enemmän työttömiä.

3.4.4 Tietosuojavaltuutetun sana

Tietosuojavaltuutettu Reijo Aarnio on antanut oman mielipiteensä asiasta. Hän pitää Lex Nokiaa viestintäsalaisuuden loukkaamisena, mutta ei kuitenkaan tyrmää lakiehdotusta täysin. Hän on samaa mieltä oikeusoppineiden kanssa, että Lex Nokia antaa suuremmat toimivaltuudet yrityksille kuin viranomaisille. Hän näkee asian varjopuolena kuitenkin sen, että laki ei anna valtuuksia automaattisesti, vaan työnantajan tulee tehdä paljon töitä ennen kuin se voi tutkia tunnistamistietoja. Hänen mukaansa Lex Nokian ideana on, että mikäli työnantaja pystyy rakentamaan hyvän tietoturvan, työnantajan ei tarvitse käsitellä tunnistetietoja. Hän myös sanoo, että hallinto pitää rakentaa uudella tavalla: pitää määritellä miten yrityssalaisuuksia voidaan käyttää, ja ketkä saavat tie-

don ja ketkä eivät saa tietoa yrityssalaisuuksista. Aarnio sanoo tämän kaiken olevan sellaista, minkä taitavan yritysjohdon olisi pitänyt tajuta jo aiemmin. Tietosuojalaki rikkoo viestintäsalaisuutta. (Rantanen 2009 [viitattu 6.10.2009].)

3.4.5 Pääministerin mielipide

Elinkeinoelämän keskusliitossa (EK) ollaan sitä mieltä, että tietosuojavaltuutetut eivät saisi tehdä tarkastuksia yhtiöissä, joissa työntekijöiden sähköpostiliikennettä tarkkaillaan sähköisen viestinnän tietosuojalain nojalla. Elinkeinoelämän keskusliiton mukaan valvonta voitaisiin hoitaa siten, että laissa määritellään millä ehdoilla tunnistetietojen selvittämistä voidaan tehdä. (HS-STT 2009 [viitattu 6.10.2009].)

Pääministeri Matti Vanhanen keskustapuolueesta ei ymmärrä ajatusta, minkä takia tietosuojavaltuutettu ei saisi valvoa sähköisen viestinnän tietosuojalain noudattamista eri yrityksissä. Vanhasen mukaan lakien noudattamista pitää voida valvoa, vaikka valvontaa ei ole laissa erikseen mainittu. Viranomaisten kyky valvoa on osa oikeusturvaa, sanoo Vanhanen Savon Sanomien haastattelussa. (HS-STT 2009 [viitattu 6.10.2009].)

3.4.6 Valtiosääntöoikeuden professorin mielipide

Veli-Pekka Viljanen sanoo, että sähköpostien tunnistamistietojen selvittämisellä puututaan luottamuksellisen viestinnän suojaan, jonka perustuslaki takaa. Hän toteaa, että luottamukselliseen viestintään puuttumista on jo viestin seuraaminen, vaikka viestiä ei avata ja lueta. Perustuslakivaliokunta on asettanut käytännön, jonka mukaan viestien tunnistamistiedot eivät kuulu luottamuksellisen viestin ydinosastolle. Tästä ei voi kuitenkaan päätellä, että viestien tunnistamistiedot eivät saisi kyseisen säännöksen antamaa turvaa. (Alinen 2009, 46-47.)

Hänen mukaansa uusi sähköisen viestinnän tietosuojalain ehdotus on perustuslain 10§:n kannalta ongelmallinen. Viljasen mukaan sääntelyä pitäisi rajata ja täsmentää sekä oikeusturvajärjestelyjä parantaa, jotta sitä voitaisiin käsitellä tavallisena lakina.

Eduskunnan perustuslakivaliokunnan tulkinta ja säätämiskannanotto aiheuttavat kritiikkiä yksityiselämän ja luottamuksellisen viestinnän suojan näkökulmasta. (Alinen b 2009, 46-47.)

Veli-Pekka Viljanen sanoo, että hänen mielestään lakia ei saisi muuttaa sen perusteella, että yritykset ovat valvoneet sähköpostiliikennettä lainvastaisesti. On kuitenkin ymmärrettävää, että yritykset haluavat suojella yrityssalaisuuksiaan, mutta voiko lain muuttaminen olla ainoa keino? Keinoja arvioitaessa keinot pitäisi suhteuttaa yhteiskunnallisiin intresseihin ja yksilön perusoikeuksiin. Viljanen on sitä mieltä, että lakimuutos ei olisi tarpeeksi tehokas keino yrityssalaisuuksien vuotamisen estämiseksi eikä paljastamiseksi, joten se ei täytä perusoikeusrajoituksille edellytettyä suhteellisuusvaatimusta. Lainmuutos antaisi lukuisille joukoille mahdollisuuden valvoa tietoliikennettä väärinkäytön varalta. Viljanen sanoo luvattoman käytön olevan käsitteenä laaja, epämääräinen ja luvattomaan käyttöön kohdistuvat lakiehdotukset on liian väljästi kirjoitettu. Hän sanoo, että käsittelyoikeus tulisi rajata väärinkäytöstapauksiin. (Alinen b 2009, 46-47.)

Tietosuojavaltuutettu valvoisi tunnistamistietojen käsittelyä. Tietosuojavaltuutettujen varaan laskettava valvonta ei kuitenkaan ole riittävää oikeusturvan takaamiseksi. Viljanen lisää vielä, että tunnistamistietojen selvitysvelvollisuuden pitäisi liittyä yksittäisiin tunnistamistietojen käsittelytilanteisiin. Tunnistamistietojen käsittelyn aloittamisesta ja käsittelykynnyksen ylittymisestä päättää yhteisötilaaja eli yksityinen toimija eikä tietosuojavaltuutettu. (Alinen b 2009, 46-47.)

3.4.7 Keskusrikospoliisin mielipide

Keskusrikospoliisin apulaispäällikkö Tero Kurenmaa lausuu mielipiteensä keskusrikospoliisin, ei koko poliisin puolesta. Hänen mukaansa laki sekoittaisi yksityisten ihmisten ja esitutkintaviranomaisten roolit. Uuden lain myötä yksityiset saisivat oikeuksia, jotka ovat olleet poliisillekin erittäin valvottuja. Yksityisten valtuudet olisivat laajemmat kuin poliisin. Hänen mielestään ihmetystä herättää myös se, että lainuudistuksen myötä viestintävirastolla ja tietosuojavaltuutetulla olisi oikeus luovuttaa tunniste-

tietoja ulkomaisille viranomaisille, mutta vastaavasti Suomen poliisit jäisivät ilman tietoja. (Ilta-Sanomat 2009 [viitattu 6.10.2009].)

Se, että yksityisten oikeudet ovat laajemmat kuin poliisin, herättää ihmetystä. Poliisi huolehtii yhteiskunnan järjestyksen ylläpitämisestä, ja olisi kohtuullista että poliisilla on laajemmat oikeudet kuin kansalaisilla. Jos kansalaisille annetaan liian laajoja oikeuksia, yhteiskunta voi jossain vaiheessa ajautua kaaokseen.

3.4.8 Käyttöönotto yliopistoissa

Teknillinen korkeakoulu (TKK) ja Tampereen teknillinen yliopisto (TTY) aikovat todennäköisesti ottaa käyttöön niin sanotun Lex Nokian. Yksittäisiä käyttäjiä seurataan sellaisissa tapauksissa, joissa käyttäjää voidaan epäillä verkon käyttösääntöjen rikkomisesta. Turun, Jyväskylän ja Oulun yliopistoissa Lex Nokiaa ei oteta käyttöön. Tampereen ja Helsingin yliopisto harkitsee sen käyttöönottoa. Turun yliopiston tietoturvapäällikön Mats Kommosen mukaan kontrolli ei ole hyvä asia. Ja se, että opiskelijoiden tekemisiä alettaisiin seurata, ei sovellu yliopiston imagoon. Liikennettä, joka on luvatonta, voidaan karsia erilaisten tiedonsiirtorajoitusten avulla, mutta TKK JA TTY eivät halua asettaa rajoituksia, vaan ne haluavat pitää täyden kaistan auki luvalliselle liikenteelle. (Hujanen 2009 [viitattu 6.10.2009].)

Opiskelijan näkökulmasta voin sanoa, että olisi erittäin kummallista, jos opiskelijoiden tekemisiä aletaan seurata. Yliopistossa ja ammattikorkeakoulussa opiskelu on hyvin vapaata, osittain itsenäistä kotona opiskelua, ja opiskelijoilla ei ole kaikissa kursseissa läsnäolopakkoa. Olen samaa mieltä, että opiskelijoiden tekemisten seuranta ei kuulu imagoon.

3.4.9 Tietosuojalaki teleyrityksen näkökulmasta

Teleyrityksen velvollisuutena on pitää verkko toimintakykyisenä, torjua hyökkäyksiä ja estää vahinkoja. Jotta tietoturvauhkia voidaan torjua, teleyrityksellä tulee olla käytössä tarpeelliset ja riittävät keinot. Kyseisiä keinoja käytetään ja niitä pitää käyttää

harkitsevasti sekä kunnioittaa tilaajien yksityisyydensuojaa. Tekemällä yhteistyötä ja painottamalla tietoturvan tärkeyttä voidaan saavuttaa paljon. Lainsäätäjän tehtäviin kuuluu huolehtia, että keinojen käyttämisessä ei ole tulkinnanvaraa. Tunnistamistietojen käsittelyn pitää olla sallittua operaattorille, jotta tele- ja viestintäverkon tietoturvasta voidaan huolehtia. Lisäksi teleyritykset toimivat tietoverkkojen tietoturvan ”esitaistelijoina”. Kehitystä ei saa rajoittaa rajoituksilla, jotka saattaisivat estää mahdollisuuden puuttua havaittuihin tietoturvauhkiin. (Dunderfelt 2009, 38.)

3.4.10 Kysymyksiä ja vastauksia

Mitä uutta laissa on?

Uutuutena voidaan pitää yrityssalaisuuksien suojelua ja käyttöehtojen valvonnan sallimista. Laissa myös määritellään tarkemmin, miten tunnistetietoja saa käyttää ja kuinka valvonnasta tulisi tiedottaa asiaan osallisille henkilöille. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Millä tavalla uudella lailla estetään yrityssalaisuuksien varastamista ja muita tietovuotoja?

Uuden lain myötä yritykset saavat mahdollisuuden kerätä näyttöä mahdollisen viranomaisten suorittaman esitutkinnan käynnistämiseksi. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Miksi nykyisen lain asettamat valtuudet eivät riitä?

Työnantajat eivät voi käsitellä hallussaan olevia tunnistetietoja selvittääkseen kuka on vuotanut yrityssalaisuuksia. Jotta poliisi voisi saada todisteita, poliisin pitää hakea tuomioistuimesta televalvontalupa ja pystyä yksilöimään tapahtuma. Yritykset eivät voi nykyisen sähköisen viestinnän tietosuojalain mukaan yksilöidä tapahtumaa, eivätkä poliisitkaan voi toimittaa tuomioistuimelle yksilöintiä. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Mitkä asiat yhteisötilaajan on tehtävä ennen kuin se voi alkaa seurata sähköpostin ja IP-liikenteen tunnistetietoja?

Yhteisötilaajien on laitettava tietoturva kuntoon. Tämän jälkeen yhteisötilaajan on määriteltävä, miten viestintäverkkoa ja palvelua saa käyttää. Verkon käyttäjille on myös annettava kirjallisessa muodossa olevat ohjeet ja ne henkilöt on nimettävä, jotka saavat käsitellä tunnistamistietoja. Lisäksi tietosuojavaltuutetulle on ilmoitettava, että tunnistamistietojenkäsittely on alkanut ja tietosuojavaltuutetulle on lähetettävä vuosittainen raportti käsitellyistä tunnistamistiedoista. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Millä tavoin valvonnasta pitää tiedottaa työntekijöille?

Jos yritys kuuluu yhteistoimintalainsäädännön piiriin, niin asia on käsiteltävä yhteistoimintamenettelyssä. Jos yritys ei kuulu yhteistoimintalainsäädännön piiriin, työntekijöitä on kuultava ja tiedotettava heille menettelyistä ja käytännöistä. Mitä tulee muihin yhteisötilaajiin, niin heidän on kerrottava valvonnasta esimerkiksi käyttöehtojen yhteydessä. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Voidaanko muistitikkujen ja cd-levyjen polttaminen kieltää työpaikalla? Entä voiko työnantaja kieltää Facebookin käyttämisen työpaikalla?

Jos yrityksellä on merkittäviä viestintäsalaisuuksia viestintäverkossa, yritys voi kieltää muistitikkujen ja cd-levyjen polttamisen nykyisen lain nojalla. Facebookin käyttäminen voidaan kieltää työpaikalla ja samoin myös ulkopuolisen sähköpostipalvelun käyttö. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Voiko työnantaja avata sähköpostiviestejä ja tekstiviestejä?

Sähköposteja työnantaja ei voi avata vanhan eikä uuden lain perusteella. Tekstiviestejä ei voi myöskään avata. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Minkä takia yliopistot, kirjastot ja taloyhtiöt ovat mukana tässä laissa?

Kun edellä mainituissa tahoissa käytetään viestintäpalveluja, niille kertyy samanlaisia tietoja kuin teleyrityksille. Yliopistojen, kirjastojen ja taloyhtiöiden viestintäverkon väärinkäyttö on mahdollista. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Viestintäverkkoa voidaan käyttää väärin. Mitä tällä tarkoitetaan?

Yhteisötilaajat määrittelevät millä tavoin sen viestintäverkkoa käytetään. Jos joku käyttäjä toimii viestintäverkossa vastoin sääntöjä eli tukkii esimerkiksi toisten käyttäjien viestintämahdollisuudet, voidaan puhua haitasta. Mikäli taloyhtiöllä on oma viestintäverkko ja verkkovastaava, olisi verkkovastaavalla uuden lain pohjalta oikeus selvittää mistä ylikuormitus johtuu ja kuka sen aiheuttaa. Taloyhtiön asukkaat saavat itse päättää, haluavatko he, että tällainen järjestelmä otetaan käyttöön. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Mitä tarkoitetaan merkittävällä haitalla verkon käyttötilanteessa?

Merkittävänä haittana voidaan pitää lisääntyneitä kustannuksia tai lisääntynyttä tiedonsiirtokapasiteetin käyttöä, tietoturvauhkaa tai muuta sen kaltaista syytä, joka vaarantaa tai vaikeuttaa verkon käyttämistä. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Jos taloyhtiössä on nettivastaava, voiko hän harrastaa sisältövalvontaa eli sitä millaisilla sivuilla asukkaat surffailevat?

Vastaus on yksiselitteinen, ei voi. Esimerkiksi, jos asukas vierailee aikuisviihdesivuilla, se ei aiheuta taloyhtiölle laissa tarkoitettua merkittävää haittaa, koska kyseinen haitta kohdistuu oman viestintäverkon toimivuuteen. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Millaisia tietoja kirjastonhoitaja saa katsoa kirjastossa yleiseltä päätteeltä, jolla nettiä käyttävä asiakas on lähettänyt viestin?

Tällä lailla ei luoda oikeutta viestien katsomiseen. Tietoturvasta vastaava henkilö voi katsoa, että kielletyltä koneelta ei mennä kielletylle sivustolle. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

Minkä takia uusi laki antaa yrityksille laajemmat oikeudet kuin poliisille tietojen käsittelemiseksi?

Yritykset ja yhteisötilaajat hallinnoivat viestintäjärjestelmiään samalla tavoin kuin esimerkiksi kiinteistöä ja huonetiloja. Näihin eivät ulkopuoliset ihmiset pääse käsiksi,

ei edes poliisi ilman yhteisötilaajan suostumusta tai tuomioistuimen päätöstä. (Helsingin Sanomat 2009 [viitattu 6.10.2009].)

3.5 Käyttöönotto yrityksissä

Runsaasti mielipiteitä herättänyt sähköisen viestinnän uusi tietosuojalaki on ollut voimassa jo useita kuukausia, mutta yhtään ilmoitusta tietosuojavaltuutetulle ei ole tullut lain käyttöön ottamisesta. Eli toisin sanoen yksikään yritys ei ole vielä ottanut lakia käyttöön. (Tirkkonen 2009 [viitattu 14.10.2009].) Elinkeinoelämän keskusliiton asiantuntija Mikko Nyyssölä puolustelee asiaa sillä, että laki tuli voimaan kesällä ja tässä välissä ovat olleet kesälomat, joten uutta lakia ei ole vielä ehditty sisäistää yrityksissä. Electronic Frontier Finlandin varapuheenjohtaja Ville Oksanen taas perustelee asiaa sillä, että laista tuli liian vaikea. Hänen mielestään lain valmisteluun olisi pitänyt käyttää enemmän aikaa. (Tirkkonen 2009 [viitattu 14.10.2009].)

Itse ajattelen asian niin, että kukaan ei voi varmuudella sanoa, onko jokin yritys ottanut lain käyttöön. Yrityksessä on voitu ottaa laki käyttöön, mutta ilmoitusta tietosuojavaltuutetulle ei vain ole tehty, mikä taas on lain vastaista. Lisäksi kukaan ei voi varmuudella tietää, miten moni yrityksistä on suunnitellut ottavansa lain käyttöön.

Lain voimaantulosta on kulunut jo yli seitsemän kuukautta, ja yksikään yritys tai yhteisö ei ainakaan vielä ole soveltanut lakia sähköpostiviestinnän tarkkailussa. Tietosuojavaltuutettu Reijo Aarnio sanoo, että yritykset kokevat lain liian sekavaksi ja monimutkaiseksi. Tämän lisäksi lakia ei osata soveltaa, koska tietoturvan merkitystä johtamiseen liittyvissä asioissa ei oteta riittävästi huomioon. Aarnion mukaan tulee ottaa myös huomioon se, että teknisessä ympäristössä on vaikea määritellä milloin ollaan Lex Nokian soveltamisalan puolella. (Helsingin Sanomat 2010 [viitattu 25.1.2010].)

Aalto-yliopiston tietoverkkotekniikan professori Jukka Mantereen mukaan lain sallima automatisoitu tarkkailu ei ole aukotonta, sillä kaikki tunnistetiedot eivät jää automatiikan haaviin. Hänen mukaansa lailla voi olla ennalta ehkäisevä vaikutus, mutta

ammattimaista yritysvakoilua se ei estä. Mantere toteaa, että ammattilaiset eivät käytä sähköpostia tai jos käyttävät, he osaavat tehdä sen niin, etteivät jää siitä kiinni. (Helsingin Sanomat 2010 [viitattu 25.1.2010].)

Lex Nokian puolustajat ovat taas sitä mieltä, että tunnistamistietojen avulla voidaan jäljittää yrityssalaisuuksien vuotajia rikosilmoituksen tekemiseksi. Tässä on kyse siitä, että vahinko on jo tapahtunut ja yrityssalaisuuksia on välitetty ulkopuolisille ihmisille. Tunnistamistietojen rikosoikeudellisen näyttöarvon voidaan sanoa olevan lähes olematon, on vain tieto siitä, että joku on jollekin jotain lähettänyt. (Helsingin Sanomat 2010 [viitattu 25.1.2010].)

3.6 Valitus Euroopan ihmisoikeustuomioistuimeen

Effi eli kansalaisjärjestö Electronic Frontier Finland on tehnyt valituksen Lex Nokiasta Euroopan ihmisoikeustuomioistuimeen Strasbourgiin. Järjestön varapuheenjohtajan, teknologiaoikeuden tohtorin Ville Oksasen mukaan vielä ei tiedetä miten tuomioistuin reagoi valitukseen. Ihmisoikeustuomioistuin nimittäin käsittelee vain konkreettisia oikeustapauksia, joita Lex Nokiasta ei vielä ole. Oksasen mukaan Lex Nokia on Euroopan ihmisoikeussopimuksen vastainen. (Helsingin Sanomat 2010 [viitattu 25.1.2010].)

4 LAKI YKSITYISYYDEN SUOJASTA TYÖELÄMÄSSÄ

4.1 Laki lyhyesti

Lain tarkoituksena on taata yksityiselämän suoja ja muita yksityisyyden suojaan liittyviä perusoikeuksia työelämässä. Laki asettaa työnantajalle joitakin vaatimuksia tietoturvan ylläpidon ja suunnittelun kannalta. Työntekijällä pitää olla työpaikalla oikeus yksityisyyteen ja luottamuksellisen viestinnän suojaan, vaikka hän käyttäisikin työnantajan työvälineitä, kuten tietokonetta tai tietoliikenneyhteyttä. (Laaksonen et al. 2006, 49.)

Mikäli työntekijöiden yksityisyys työpaikoilla riistetään kokonaan, töihin tuleminen ei ehkä ole mielekästä, ja työnteosta tulee pakonomaista suorittamista. Jos työpaikalla on kireä tunnelma, ja pomo vahtii kaiken aikaa alaistensa tekemisiä, työntekijöiden työhyvinvointi kärsii. Tällöin työntekijöiden vaihtuvuus on suuri, ja työyhteisöstä ei kehity tiivistä joukkoa, joka haluaa toimia yrityksen- ja yhteisen edun parhaaksi.

Työpaikalla työnantaja on oikeutettu keräämään työntekijään liittyviä henkilötietoja, mutta vastaavasti työntekijällä on oikeus kontrolloida tietojen keräämistä jossakin määrin. Tietojärjestelmien avulla voidaan kerätä ja ylläpitää suuria määriä kaikenlaista informaatiota, muun muassa henkilö- tai muita vastaavia tietoja. On tärkeää, että tietoturvallisia tietojärjestelmiä pyritään käyttämään tehokkaasti suunniteltuihin tarkoituksiin niissä puitteissa kuin laki sallii. (Laaksonen et al. 2006, 49.)

Työsopimuslain 3:1§ direktio-oikeuden mukaan työnantaja voi antaa työntekijöille heitä koskevia sitovia määräyksiä ja ohjeita. Nämä määräykset ja ohjeet voivat liittyä työntekijöille osoitettujen työtehtävien suorittamiseen ja esimerkiksi tietoturvatoimenpiteiden noudattamiseen. On otettava huomioon, että työnantaja ei voi antaa ohjeita ja määräyksiä, jotka ovat lain- tai hyvän tavan vastaisia. (Laaksonen et al. 2006, 49.)

4.2 Sähköisen viestin salaisuus työntekijän perusoikeutena

Nykyinen luottamuksellisen viestin salaisuutta koskeva perustuslain 10§:n 2 momentti poikkeaa alkuperäisestä hallituksen 12§:stä tekemästä esityksestä. ”Säännös on kirjoitettu välineneutraaliin muotoon: kaikenlaiset luottamukselliset viestit saavat perusoikeussuojaa siitä riippumatta, millä teknisellä tai muulla välineellä ne on lähetetty (tai aiotaan lähettää).” 1990-luvun loppupuolelta alkaen on katsottu, että sähköposti, puhelut, kirjeet ja muut perinteiset viestintätavat ovat luottamuksellista viestintää. (Nyblin 2009, 55-86.)

Perustuslain 10§:n 2 momentin luottamuksellisen viestinnän suoja tarkoittaa sitä, ettei kukaan muu kuin viestin lähettäjä ja vastaanottaja saa ottaa selvää, mitä viesti sisältää tai muutenkaan puuttua viestin sisältöön tai sitä koskeviin tunnistamistietoihin. Mitä ulkopuolisiin henkilöihin tulee, niin he eivät saa puuttua viestin perille menemiseen eivätkä tallentaa tai käsitellä viestiä, jos laissa ei ole säädetty sellaiseen oikeutta. (Nyblin 2009, 55-86.)

Sähköisen viestinnän tietosuojalain 4§:n mukaan sähköinen viesti ja siihen liittyvät tunnistamistiedot kuuluvat luottamuksellisen viestin piiriin, jos sähköisen viestinnän tietosuojalaissa tai muussa laissa ei toisin säädetä. Rikoslaissa on rangaistukset sellaisia tapauksia varten, jossa luottamuksellisen viestin salaisuutta on loukattu. (Nyblin 2009, 55-86.)

Lailla voidaan säätää myös rajoituksista luottamuksellisen viestin salaisuuteen. Tätä sääntelee perustuslain 10§:n 3 momentti. Rajoituksia voidaan säätää, jos kyseessä on yksilön tai yhteiskunnan turvallisuus, kotirauhaa vaarantava rikosten tutkinta, oikeudenkäynti, turvallisuustarkastus tai vapaudenmenetys. Viestinnän luottamuksellisuutta voidaan rajoittaa vain eduskunnan säätämällä lailla ja lakivarauksessa. On myös otettava huomioon, että näissä tapauksissa rajoitusten tulee olla välttämättömiä. Viestintäsalaisuuden suojan ydinasiana voidaan pitää sitä, että tarkoitus on turvata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta. Tunnistamistietojen suoja ei kuulu luottamuksellisen viestin suojan ydinalueelle. (Nyblin 2009, 55-86.)

Tunnistamistietojen suojaa on mahdollista kuitenkin rajoittaa yksityisten välisissä suhteissa tavallisella lailla, mikäli perusoikeuksien yleiset rajoitusedellytykset vain täyttyvät. Luottamuksellisen viestin salaisuus on loukkaamaton ja tämä oikeus kuuluu jokaiselle eikä sitä myöskään voida rajoittaa ilman laissa säädettyä perustetta. Tämä säädetään myös perustuslain 10§:ssä. (Nyblin 2009, 55-86.)

Jokaisella on oikeus viestintäsalaisuuteen työpaikalla. Tämä ei tosin merkitse sitä, että kaikki työpaikalle tulevat tai sieltä lähtevät viestit olisivat luottamuksellisen viestin piirin suojassa. Työasioita koskevat viestit, joita työntekijä lähettää ja vastaanottaa, eivät ole lähtökohtaisesti luottamuksellisia suhteessa työnantajaan. Työntekijän lähettämät ja vastaanottamat yksityisasioita koskevat viestit ovat luottamuksellisia ja edes työantajalle ei kuulu niiden sisältö. (Nyblin 2009, 55-86.)

Työssäkäynti on osa jokapäiväistä elämää, ja on itsestään selvää, että eteen tulee tilanteita, jolloin yksityisasioita joutuu hoitamaan työpäivän aikana. Olisi kohtuutonta, jos työnantajalla olisi oikeus puuttua yksityisasioita koskeviin viesteihin. Työnteon lisäksi kaikilla on oma henkilökohtainen elämä, jota pitäisi kunnioittaa ja vaalia, koska henkilökohtaiset ongelmat heijastuvat aika nopeasti myös työntekoon.

Sähköisen viestinnän tietosuojalain säännökset antavat työnantajalle joitakin oikeuksia tehdä toimenpiteitä, jotka kohdistuvat viestintään liittyvien tunnistamistietojen suojaan ja jotka saattavat estää työntekijöille lähetettyjen viestin perille menon. Joissakin tapauksissa työntekijöiden luottamuksellisen viestin sisällön suoja saattaa vaarantua. Työnantaja saa käsitellä viestintäjärjestelmissään kulkevia viestejä ja niihin liittyviä tunnistamistietoja uuden sähköisen viestinnän tietosuojalain antamassa laajuudessa. Työnantaja saa käsitellä viestejä, vaikka joku yksittäinen työntekijä ei haluaisikaan sallia käsittelyä. Työnantaja saa esimerkiksi pysäyttää roskapostin saapumisen tai rajoittaa sitä ilman työntekijän suostumusta. (Nyblin 2009, 55-86.)

Työnantajat eivät voi edellyttää että työntekijät antaisivat suostumusta käytäntöihin, joista ei ole lain tasoisia säännöksiä. Lainsäädännön mukaan työnantajalla ei ole oikeutta sähköposteja tarkkailemalla valvoa, mitä työntekijät tekevät. Poikkeuksen edellä

mainittuun tekee se, että uudessa sähköisen viestinnän tietosuojalaissa 13a-13k§ on säännöksiä, jotka koskevat tunnistamistietojen käsittelyä yrityssalaisuuksien suojaamiseksi. (Nyblin 2009, 55-86.)

4.3 Työnantajan oikeudet ja velvollisuudet

4.3.1 Yleistä

Se, tulevatko työnantajan oikeudet ja velvollisuudet arvioitaviksi yhteisötilaajaa vai rekisterinpitäjää koskevan sääntelyn nojalla, riippuu toimenpiteistä ja tapauskohtaisista olosuhteista. On otettava huomioon myös se, mitä työnantajan oikeuksista ja velvollisuuksista on erikseen säädetty. Työntekijöiden osalta tulee huomioida se, mitä säädetään käyttäjän, rekisteröidyn ja työntekijän oikeuksista. Yhteisötilaajana voidaan pitää elinkeinonharjoittajaa, osakeyhtiötä, osuuskuntaa yhdistystä, oppilaitosta tai valtion virastoa. Rekisterinpitäjäksi määritellään sellainen yhteisö, laitos tai säätiö, joka käyttää henkilörekisteriä ja myös määrää sen käyttöä. (Nyblin 2009, 87-90.)

Työntekijän luottamukselliset viestit pitää erottaa työnantajalle selvästi kuuluvista viesteistä. Laissa määritellään tarkkarajaisesti ja täsmällisesti millaiset ovat viestien esille hakemisen ja avaamisen edellytykset. Voimaan tullut laki antaa työnantajalle mahdollisuuden saada selville hänen toimintaansa kuuluvat viestit. Kyse on sellaisista tilanteista, joissa suostumukseen perustuvat menettelyt eivät syystä tai toisesta ole käytettävissä ja tiedonsaanti on kuitenkin välttämätöntä työnantajan toiminnan jatkumisen turvaamiseksi. (Helopuro, Perttula & Ristola 2009, 49.)

Laki yksityisyyden suojasta työelämässä määrittelee työnantajan huolehtimisvelvollisuuden, joka on pykälässä 18§. Sen mukaan työnantajalle kuuluu oikeus hakea esille tai avata työnantajan työntekijän käyttöön osoittamaan sähköpostiosoitteeseen lähetettyjä tai työntekijän tällaisesta sähköpostiosoitteesta lähettämiä sähköpostiviestejä. Mikäli työnantaja on suunnitellut ja järjestänyt työntekijälle tämän nimellä lähetettyjen ja tämän lähettämien sähköpostiviestien suojan toteuttamiseksi tarpeelliset toimenpiteet ja tässä tarkoituksessa erityisesti huolehtinut siitä, että: (Helopuro et al. 2009, 51).

1) Työntekijä voi sähköpostiin kuuluvan automaattisen vastaustoiminnon avulla lähettää viestin lähettäjälle ilmoituksen poissaolosta ja sen kestosta sekä tiedon henkilöstä, joka hoitaa poissaolevan työntekijän tehtäviä.
2) Työntekijä voi ohjata viestit toiselle henkilölle, jonka työnantaja on tehtävään hyväksynyt, tai viestit voidaan ohjata työntekijän omassa käytössä olevaan osoitteeseen, jonka työnantaja on hyväksynyt.
3) Työntekijä voi suostua siihen, että hänen poissa ollessaan toinen työnantajan hyväksymä henkilö voi ottaa vastaan työntekijälle suunnatut viestit. Näin pystytään välittömästi selvittämään onko työntekijälle lähetetty sellainen viesti, joka on tarkoitettu työnantajalle työtehtävien hoitamista varten, ja josta työnantajan on toiminnan tai työtehtävien asianmukaisen järjestämisen takia välttämätöntä saada tieto. (Helopuro et al. 2009, 51.)

Säännöksessä on kyse edellytyksistä, joiden tulee täyttyä ennen kuin työnantaja voi alkaa selvittää työntekijän nimellä tulleiden viestien otsikoita tai niiden sisältöä. Työnantajalla ei ole säännöksen mukaan oikeutta lähteä selvittämään työntekijän henkilökohtaiseen sähköpostiin tulevia tai sieltä lähteviä viestien sisältöjä. Säännöstä pidetään työnantajan vähimmäisvelvoitteena, eikä se estä työntekijää antamasta sähköpostien käsittelyoikeutta toiselle työntekijälle, kuten esimerkiksi sihteerille. (Helopuro et al. 2009, 51-52.)

Säännöksen keskeisenä sisältönä pidetään, että työnantajan tulee suunnitella ja toteuttaa työntekijän sähköpostiviestinnän suojaamiseksi tarvittavat toimenpiteet. Työnantajan tulee myös huolehtia siitä, että työntekijällä on poissa ollessaan mahdollisuus kytkeä automaattivastaus poissaolosta päälle, ohjata viestit toiseen osoitteeseen, jonka työnantaja on hyväksynyt ja suostua siihen, että joku muu henkilö vastaanottaa hänelle suunnatut viestit. (Helopuro et al. 2009, 52.)

Mitä sitten tarkoitetaan viestin estämisellä tai rajoittamisella? Työnantaja pyrkii ohjaamaan sitä, millaisia viestejä sähköpostijärjestelmästä lähtee tai sinne saapuu. Lisäksi työnantaja pystyy vaikuttamaan siihen, minkälaisista osoitteista viestejä voidaan vastaanottaa ja millaisiin osoitteisiin viestejä voidaan ylipäätänsä lähettää. Jotta roskaposteilta ja haittaohjelmilta voidaan välttyä, työnantaja voi estää niiden vastaanottami-

sen ilman työntekijän suostumusta. Roskapostin suodattamiseen on useita tapoja. Roskaposti voidaan pysäyttää ja poistaa palvelimelta ennen kuin työntekijät edes ehtivät vastaanottamaan niitä. Joissain määrin roskapostin voidaan antaa tallentua palvelimelle, työasemalle ja päätelaitteelle. Roskapostiksi luokitellut viestit voidaan myös jättää palvelimelle esimerkiksi kahden viikon ajaksi, mutta tämä edellyttää erillistä ohjelmistoa ja suurempaa levytilaa. Kun määräaika on kulunut umpeen, viestit poistetaan palvelimelta automaattisesti. (Nyblin 2009, 95-97.)

Sähköpostitse tapahtuva mainonta on lisääntynyt huimasti viime vuosien aikana. Yritykset saavat toisten yritysten ja yrityksen työntekijöiden sähköpostiosoitteita tavalla tai toisella, vaikka ne olisivat salassa pidettäviä. Sähköposti on helppo tapa lähestyä toista ihmistä. Roskapostin määrä on kuitenkin valtava, ja se saattaa tukkia koko sähköpostin. On erittäin järkevää, että roskapostia suodatetaan jo ennenkuin työntekijät edes ehtivät vastaanottaa sitä. Roskapostin mukana saattaa myös levitä viruksia, jotka tuhoavat tietokoneen tiedostoja.

Työnantajalla on oikeus ja velvollisuus poistaa virukset ja muut haittaohjelmat saapuvista viesteistä ilman, että työntekijä on antanut suostumustaan. Saapuvan viestiliikenteen rajoittamiseen saattaa kuulua myös se, että työnantaja estää tietyntyyppisten liitetiedostojen saapumisen sisäverkkoon. Lähtevien viestien osalta työnantajalla on oikeus estää ja rajoittaa tällaisten viestien välittäminen. (Nyblin 2009, 97.)

Sähköisen viestinnän tietosuojalain 6§:n nojalla käyttäjät voivat suojata viestinsä ja tunnistamistietonsa haluamallaan tavalla, jollei laissa toisin säädetä. Suojaus ei saa häiritä verkko- ja viestintäpalvelun toteuttamista ja käyttämistä. Työnantajalla on oikeus kieltää sähköpostiviestien lähettäminen esimerkiksi kilpailevien yritysten sähköpostiosoitteisiin. Tällä pyritään varmistamaan se että luottamuksellista tietoa ei vahingossakaan siirry väärille tahoille. Työnantaja voi myös määrätä, että salassa pidettäväksi tarkoitettua työasioita koskevaa aineistoa ei saa lähettää sähköisesti. Mikäli kyseinen aineisto halutaan lähettää sähköisesti, on ainakin käytettävä asianmukaista salausmenetelmää. (Nyblin 2009, 97-99.)

Työnantajan huolehtimisvelvollisuus ei ole ehdoton. Mikäli työnantaja katsoo, että hänellä ei ole tarvetta hakea esille työntekijöiden lähettämiä tai vastaanottamia sähköpostiviestejä, hänen ei tarvitse täyttää huolehtimisvelvollisuutta. Jos myöhemmin käy ilmi, että työntekijän sähköpostiviesteihin kohdistuvalla tiedonhankinnalle olisi tarvetta, työnantaja ei voi hakea esille viestejä, mikäli hän ei saa työntekijältä tähän erikseen suostumusta. Työelämän tietosuojalain 19 ja 20:ssä säädetään yllä mainituista oikeuksista ja näiden oikeuksien käyttäminen on sallittua, mikäli työnantaja on täyttänyt huolehtimisvelvollisuutensa. (Nyblin 2009, 99-100.)

Mikä sitten voidaan lukea sähköisten viestien ja tunnistamistietojen käsittelyksi? Niihin sisältyy viestien ja tunnistamistietojen keräys sekä tallennus. Kyseiset tiedot kertyvät ja tallentuvat automaattisesti. Sähköisen viestinnän tietosuojalain sallimat tunnistamistietojen käsittelytoimenpiteet saattavat johtaa siihen, että tietojen käsittelijä saa tunnistamistietojen sisällön selville. Tätä toimenpidettä kutsutaan tunnistamistietoihin kohdistuvaksi tiedonhankinnaksi. Tunnistamistietojen käsittelyssä tulee kuitenkin pyrkiä siihen, että tunnistamistietojen sisältö ei tule käsittelijän tietoon. (Nyblin 2009, 103-104.)

Tunnistamistietojen ja viestien sisällön ilmaisemisella tarkoitetaan sitä, että toinen henkilö tulee viestien sisällöstä tai tunnistamistiedoista tietoiseksi. Tiedot voidaan kertoa toiselle suullisesti tai luovuttamalla sähköinen tai sitä vastaava tallenne. Henkilö, joka on yhteisötilaajan palveluksessa ja se, joka on toiminut yhteisötilaajan lukuun, on vaitiolovelvollinen. (Nyblin 2009, 105-106.)

Viestien ja tunnistamistietojen käsittelyksi luokitellaan se, että tietoja käytetään. Lain mukaan luottamuksellisia viestejä saa käsitellä vain viestin lähettäjän tai sen suostumuksella, kenelle viesti on tarkoitettu tai jos laissa niin säädetään. Tämä merkitsee sitä, että tietojen käyttäminen on kiellettyä, jos laissa ei ole säädetty siihen olevan oikeutta tai viestinnän osapuoli ei ole antanut tietojen käyttämiseen omaa suostumustaan. Viestien ja tunnistamistietojen käsittelyksi luokitellaan myös tietojen luovutus toiselle. Tässä tulee ottaa huomioon, että tietoja voidaan luovuttaa vain silloin, kun siihen on laissa säädetty peruste. Sähköisen viestinnän tietosuojalain 8 §:n 3 momen-

tissa säädetään, että tunnistamistietoja saa luovuttaa vain niille henkilöille, joilla on oikeus käsitellä tietoja kyseisessä tilanteessa. Näissäkin tilanteissa tietoja saa luovuttaa vain, mikäli luovuttaminen on tarpeellista tietojen käsittelyn tarkoituksen kannalta. (Nyblin 2009, 106-107.)

Sähköisen viestinnän tietosuojalain mukaan yhteisötilaajalla on oikeus käsitellä luottamuksellisia viestejä ja niihin liittyviä tunnistamistietoja. Henkilötietoihin liittyvät käsittelyoikeudet kuuluvat taas rekisterinpitäjälle ja rekisterinpitäjän oikeuksista säädetään henkilötietolaissa. (Nyblin, 112-114.) Sähköisen viestinnän tietosuojalain 5 luvussa säädetään tietoturvaa koskevista velvoitteista, jotka koskevat yhteisötilaajaa. Lain mukaan yhteisötilaaja on velvollinen huolehtimaan käyttäjien tunnistamistietojen käsittelyn tietoturvasta. Rangaistukseen voidaan tuomita sellainen, joka tahallaan laiminlyö velvollisuutta huolehtia tunnistamistietojen käsittelyn tietoturvasta tai sellainen, joka tahallaan laiminlyö ennakkoilmoituksen laatimisen tai antamisen käyttäjälle, työntekijöiden edustajalle tai tietosuojavaltuutetulle. Lisäksi työnantaja on velvollinen korvaamaan työntekijälle sen vahingon, joka on aiheutunut tietoturvan laiminlyönnistä. Mahdollisen vahingon korvaaminen määräytyy vahingonkorvauslain mukaan. (Nyblin 2009, 116-119.)

4.3.2 Työntekijän tilapäinen poissaolo

Työnantajan tulee etukäteen täyttää työelämän tietosuojalaissa määritellyt huolehtimisvelvollisuudet. Mikäli hän täyttää nämä, hän voi hakea esille ja avata työntekijän lähettämiä tai hänelle saapuneita sähköpostiviestejä. Työelämän tietosuojalain säännökset 18-20§ koskevat sellaisia viestejä, jotka työntekijälle on lähetetty hänen työsähköpostiosoitteeseensa. Lisäksi säännös ulottuu koskemaan viestejä, jotka työntekijä on tästä osoitteesta lähettänyt. Lain 20§:n nojalla työantaja saa avata vain sellaisia viestejä, joissa on työasioihin liittyvää tietoa ja jotka ovat työnantajalle kuuluvia. Työnantaja ei saa tietosuojalain nojalla yrittää hankkia tietoa viestistä, joka on tallennettu työntekijän yksityiseen sähköpostilaatikkoon. (Nyblin 2009, 155-158.)

Työelämän tietosuojalain mukaan työntekijän sähköposteja voidaan kaivaa esille silloin, kun työntekijä on tilapäisesti esteellinen suorittamaan työtehtäviään. Soveltamisalan ulkopuolelle jäävät tapaukset, joissa työntekijä on esteellinen lukemaan sähköposteja työmatkan tai muun vastaavan työtä koskevan syyn takia. Toisaalta työntekijän sähköposteja olisi oikeus hakea esille kaikissa tapauksissa, joissa työntekijä ei pysty hoitamaan sähköpostiviesteihin liittyviä asioita. (Nyblin 2009, 159.)

Jotta viestejä voidaan selvittää, on otettava huomioon ajallinen edellytys, omistajuusedellytys ja välttämättömyysedellytys. Ajallinen edellytys ulottuu koskemaan työntekijän lähettämiä ja hänelle lähetettyjä viestejä. Työnantajalla on oikeus hankkia tietoa viesteistä, jotka työntekijälle on lähetetty hänen poissaolonsa aikana tai välittömästi ennen poissaoloa tai jotka työntekijä on itse lähettänyt välittömästi ennen poissaoloa. Omistajuusedellytys tarkoittaa sitä, että viestien tulee kuulua työnantajalle, joten edellytyksenä on, että viesti koskee työasioita. Edellytyksenä on myös, että viestien sisältö ei ole tarkoitettu vain viestinnän osapuolten tietoon. Välttämättömyysedellytyksellä tarkoitetaan sitä, että miten merkittävä tarve työnantajalla on saada tieto viestistä sinä aikana kuin työntekijä on poissa. Merkittäväksi tarpeeksi voidaan lukea työnantajan toimintaan liittyvien neuvottelujen loppuun saattaminen ja asiakkaiden palveleminen sekä työantajan toimintojen turvaaminen muutoin. (Nyblin 2009, 160-162.)

Työelämän tietosuojalaissa on säädetty neljä edellytystä, joiden kaikkien tulee täyttyä, ennen kuin viesti voidaan hakea esille. Edellytykset ovat seuraavat:

1. Työntekijä työskentelee itsenäisesti työnantajan lukuun eikä työnantajan käytössä ole järjestelmää, jonka avulla työntekijän tekemät asiat ja asioiden käsittelyvaiheet kirjataan tai saadaan selville toista kautta
2. Työntekijän tehtävien ja vireillä olevien asioiden takia pidetään selvänä, että työnantajalle kuuluvia viestejä on lähetetty tai vastaanotettu
3. Työntekijä on tilapäisesti estynyt suorittamasta työtehtäviään eikä työnantajalle kuuluvia viestejä voida luovuttaa työnantajan käyttöön, vaikka työnantaja on huolehtinut huolellisuusvelvoitteesta

4. Työntekijän suostumusta ei saada kohtuullisessa ajassa ja asian selvittäminen ei siedä viivytystä. (Nyblin 2009, 163.)

Ketkä sitten saavat avata työntekijän sähköposteja? Työntekijän lisäksi sähköposteja saavat avata sellaiset henkilöt, joilla on tietojärjestelmän pääkäyttäjän valtuudet. Sähköpostiviestien esille hakemiseen pitää yleensä osallistua vähintään kaksi henkilöä, työantaja tai tämän edustaja ja sellainen henkilö, jolla on tarvittavat tekniset valtuudet viestien esille saattamiseen järjestelmästä. Työnantajalla, tämän edustajalla tai tietojärjestelmän päävaltuuksia käyttävällä henkilöllä ei ole oikeutta hakea viestejä esille yksin. Poikkeuksena on tapaus, jossa pääkäyttäjän valtuudet ovat samalla henkilöllä, jolla työorganisaatiossa on valtuus tehdä päätöksiä asiasta, millä tavalla poissaolevan työntekijän työtehtävien hoitoon liittyvistä asioista huolehditaan. (Nyblin 2009, 170-174.)

Työnantajalla on oikeus työelämän tietosuojalain 19§:n mukaan ottaa viestin lähettäjää, vastaanottajaa tai viestin otsikkoa koskevien tietojen perusteella selville, onko työntekijälle lähetetty tai onko työntekijä lähettänyt työnantajalle kuuluvia sähköpostiviestejä. Työntekijän sähköpostiviestintää koskevat tunnistamistiedot otetaan tietyltä ajanjaksolta tarkasteltaviksi ja vasta tämän jälkeen työnantajan on mahdollista arvioida, onko jokin tai jotkin viesteistä työnantajalle kuuluvia. Arvioitaessa sitä onko viesti työnantajalle kuuluva vai ei, työnantajan tulee kiinnittää huomiota kahteen seikkaan: ensinnäkin kuka on viestin toinen osapuoli ja millaisia tietoja on merkitty viestin otsikkokenttään. Näiden tietojen perusteella työnantajan tulisi muodostaa mielikuva siitä, onko viesti työ- vai yksityisasia. (Nyblin 2009, 175-178.)

Työelämän tietosuojalain 20§:ssä on säädetty, että ennen kuin työnantaja ryhtyy avaamaan työntekijän sähköpostilaatikossa tallennettuna olevaa viestiä, työnantajan on saatava yhteys viestin lähettäjään tai vastaanottajaan, jotta viestin sisältö voidaan saada selville. Työnantaja saa avata viestin vain siinä tapauksessa, että viestin lähettäjään tai vastaanottajaan ei ole saatu yhtyettä. Mikäli työntekijää ei ole tavoitettu tai häneltä on saatu suostumus vain tunnistamistietojen esille hakemiseen tai mikäli hän ei ole antanut minkäänlaista suostumusta, työnantajan pitää pyrkiä saamaan yhteys

viestinnän toiseen osapuoleen. Toinen osapuoli voi näin ollen lähettää viestin työnantajalle uudelleen toiseen osoitteeseen tai kertoa mitä viesti sisältää. (Nyblin 2009, 178-182.)

Jos viestejä vain haetaan, mutta niitä ei avata, viestien esille hakemisesta on laadittava siihen osallistuneiden allekirjoittama selvitys, johon tulee kirjata miksi viestiä on haettu, hakemisen ajankohta ja suorittajat. Selvitys tulee toimittaa työntekijälle tiedoksi ilman aiheetonta viivytystä. Kun työntekijän sähköpostiviestien esille hakeminen on johtanut viestien avaamiseen, on siitä laadittava selvitys. Selvityksestä tulee ilmetä, miksi viesti on avattu, avaamisen ajankohta, avaamisen suorittajat sekä kenelle avatun viestin sisällöstä on annettu tieto. Myös tämä selvitys on ilman aiheetonta viivytystä annettava työntekijälle tiedoksi. (Nyblin 2009, 182-184.)

Sähköpostiviestien tunnistamistietoja saa käsitellä vain siinä määrin kuin se on välttämätöntä työnantajalle kuuluvien viestien erottelemiseksi muista viesteistä. Avattujen viestien sisältöä ei saa käsitellä laajemmin kuin on tarpeen välttämättömien työtehtävien hoitamisen kannalta. Mikäli työnantaja on erehdyksissään avannut yksityisen viestin, sitä koskevien tietojen käsittely on välittömästi lopetettava. (Nyblin 2009, 184-185.)

Työelämän tietosuojalain 18§:ssä on säädetty mahdollisuudesta, jonka mukaan työntekijä voi ohjata hänelle tarkoitetut viestit poissaolonsa ajaksi toiselle työnantajan hyväksymälle henkilölle. Työntekijä voi antaa myös suostumuksensa siihen, että poissaolon aikana toinen henkilö ottaa vastaan hänelle tarkoitetut viestit selvittääkseen ovatko jotkin viestit sellaisia, jotka on tarkoitettu työnantajalle työtehtävien hoitamiseksi ja joista työnantajan pitää saada tieto. Valtuutetun lukemisoikeus kohdistuu vain sellaisiin viesteihin, jotka ovat työnantajalle kuuluvia, ja joista työnantajan on välttämätöntä saada tieto jo ennen kuin työntekijä palaa töihin. (Nyblin 2009, 188-191.)

Valtuutetulla työntekijällä on oikeus laatia avatusta sähköpostista selonteko, johon tulee avaamiseen osallistuneiden henkilöiden allekirjoitus, selitys miksi viesti on avattu, avaamisen ajankohta, avaamisen suorittajat ja kenelle avatun viestin sisällöstä on

annettu tieto. Tämä selvitys on toimitettava työntekijälle tiedoksi. Lisäksi viesti on säilytettävä eikä viestin sisältöä ja lähettäjätietoja saa käsitellä laajemmin kuin on tarpeen viestin avaamisen tarkoituksen kannalta. Tietoja käsittelevät henkilöt eivät saa ilmaista viestien sisältöä sivulliselle työsuhteen aikana eikä myös sen päättymisenkään jälkeen. (Nyblin 2009, 188-191.)

4.3.3 Työntekijän kuolema tai vakava sairastuminen

Työelämän tietosuojalain 19§:n 2 momentti sanoo, jos työntekijä on kuollut tai on muuten pysyväluonteisesti estynyt suorittamaan työtehtäviään eikä hänen suostumustaan voida saada, niin työnantajalla on oikeus ottaa viestin lähettäjää, vastaanottajaa tai viestin otsikkoa koskevien tietojen perusteella selville viestit, jotka kuuluvat työnantajalle. Työelämän tietosuojalaissa säädetään yhdeksi viestin avaamisen edellytykseksi se, että työntekijän suostumusta viestin avaamiseen ei saada. Sellaisessa tapauksessa, jossa työntekijä on kuollut, on selvää että suostumusta ei voida enää hankkia. Viestejä voidaan hakea esille myös, mikäli työntekijän hoitamien asioiden selville saaminen ja työnantajan toiminnan turvaaminen ei ole muilla keinoilla mahdollista. Mikäli kuolleen tai sairastuneen työntekijän viestejä on haettu esille, mutta niitä ei ole avattu, on niistä laadittava selvitys. Selvitys tulee toimittaa työntekijälle, jos työntekijä on sellaisessa tilassa, että hän pystyy vastaanottamaan selvityksen. (Nyblin 2009, 193-201.)

Tapauksissa, joissa työntekijä on kuollut tai sairastunut vakavasti, työnantajan on poistettava työntekijän henkilökohtainen postilaatikko. Sähköpostitilin lakkauttaminen aiheuttaa sen, että saapuneet viestit eivät enää tallennu työantajan tarjoamalle sähköpostipalvelimelle. Viestien lähettäjät saavat ilmoituksen, että sähköpostitiliä ei ole enää olemassa. Ennen kuin sähköpostilaatikon sisältö voidaan tuhota, työnantajan tulee varmistua siitä, että kaikki työasioita koskevat viestit, joista työnantajan tulee saada työelämän tietosuojalain mukaan tieto, voidaan ottaa työnantajan käyttöön. (Nyblin 2009, 201-203.)

Jos työntekijä on kuollut, nousee esille kysymys siitä pitäisikö sähköpostilaatikossa olevat yksityiset viestit luovuttaa jollekulle. Työnantajalla ei ole oikeutta luovuttaa yksityisiä viestejä työntekijän omaisille, ja tällöin voidaan puhua viestintäsalaisuudesta. Käytännössä saattaa esiintyä tapauksia, joissa kuolinpesän osakkaat esittävät perustellun pyynnön saada selvittää työntekijän yksityisen viestin sisältöä. Joissakin tapauksissa kuolinpesän osakkaat saattavat olettaa, että työntekijän sähköposteista löytyy pesänselvityksen kannalta olennaista tietoa. Useimmissa tapauksissa asiakirjan sisältö voi olla selvitettävissä viestin toiselta osapuolelta. Joskus toisen viestin osapuolen henkilöllisyys ei kuitenkaan ole tiedossa. Mahdollisena voidaan pitää myös sitä, että toinen osapuoli ei halua antaa tietoja asiakirjasta. (Nyblin 2009, 201-203.)

4.3.4 Työntekijän työsuhteen päättyminen

Työntekijän työsuhde voi päättyä irtisanomisen tai työsuhteen purkamisen myötä, määräaikaisen työsopimuksen päätyttyä tai työntekijän eläkkeelle siirtymisen johdosta. Kun työntekijä on jäämässä eläkkeelle tai määräaikainen työsopimus on lähenemässä loppuaan, työnteon lopettamisen ajankohta on tiedossa hyvissä ajoin. Edellä mainituissa tapauksissa ei synny tilanteita, joissa sähköpostiviestejä pitäisi jälkeenpäin selvitellä. Mikäli työsuhde päättyy irtisanomisen takia, tarvittavat asiat ehditään yleensä hoitaa kuntoon irtisanomisajan kuluessa. Ongelmia saattaa sähköpostiviestien osalta koitua, jos työsuhde puretaan välittömin vaikutuksin tai työsopimus irtisanotaan ilman työn tekemisen velvoitetta irtisanomisaikana. Työelämän tietosuojalain 18§:n säännöksen mukaan työnantaja saa hakea esille työntekijän sähköpostiviestejä vain siinä tapauksessa, että työnantaja on täyttänyt huolehtimisvelvollisuutensa. (Nyblin 2009, 207-210.)

Mikäli työntekijän työsuhteen päättymisen ajankohta on hyvissä ajoin sekä työntekijän että työnantajan tiedossa, ongelmia työnantajalle kuuluvien ja työntekijän yksityisten viestien erottelussa ei pitäisi olla. Työntekijä järjestää sähköpostiaan koskevat asiat siten, että työnantaja saa tiedon viesteistä, jotka koskevat työasioita. Tyypillisesti ongelmia aiheutuu tilanteissa, joissa työsuhteen päättyminen tulee täysin yllätyksenä jommallekummalle osapuolelle. Toisinaan sähköpostilaatikon lakkauttaminen saattaa

viivästyä ja tällöin ollaan tilanteessa, että sähköpostilaatikkoon kertyy viestejä ja viestien lähettäjät eivät saa ilmoitusta siitä, että työntekijä ei ole enää tavoitettavissa. (Nyblin 2009, 210-211.)

Työelämän tietosuojalain mukaan työnantajalle ei ole säädetty velvollisuutta siirtää entisen työntekijän yksityisiä sähköpostiviestejä työntekijän uuteen sähköpostiosoitteeseen. Lain 19§:n 2 momentin mukaan työnantajalla on oikeus hakea esille entisen työntekijän sähköpostiviestejä vain siinä tarkoituksessa, että sieltä löytyisi työasioita koskevia viestejä. Viestejä avattaessa työnantaja on velvollinen noudattamaan varovaisuutta, koska avaamisoikeus koskee vain viestejä, jotka kuuluvat selvästi työnantajalle. Mikäli työntekijä ilmoittaa tarvitsevansa sähköpostilaatikostaan joitakin viestejä, työntekijän tulee valtuutta aikaisempi työtoveri käymään läpi hänen sähköpostilaatikkoaan ja erottelemaan sieltä pyydetyt viestit. Edellä mainittu menettely vaatii työnantajan hyväksynnän. Lisäksi on saatava työnantajan suostumus siitä, onko valtuutettu henkilö sopiva etsimään sähköpostiviestejä. Huomattavasti yksinkertaisempaa olisi, jos entinen työntekijä voisi itse saapua erottelemaan viestinsä. Tällaista mahdollisuutta voidaan käyttää vain silloin, jos työnantajalla ei ole sähköpostilaatikossa olevien viestien suhteen salassapitovelvollisuuksia kolmansiin henkilöihin nähden. (Nyblin 2009, 217-218.)

5 HENKILÖTIETOLAKI

5.1 Lain tarkoitus

Henkilötietolakia (523/1999) tulee soveltaa henkilötietojen käsittelyyn ja sitä pidetään yleislakina, mutta henkilötietojen suojasta säädetään myös muissa laeissa. Henkilötietolaki on myös tärkeä laki tietoturvan kannalta, ja sen peruskäsitteitä on otettu tietoturvaa käsitteleviin erityislakeihin kuten sähköisen viestinnän tietosuojalakiin. Henkilötietolakia sovelletaan lähes jokaisessa yrityksessä, jossa käsitellään yksittäisen ihmisen henkilötietoja. Henkilötiedoksi voidaan laskea mikä tahansa tieto, nimi, osoite tai vaikka DNA, mikäli henkilö pystytään sen tiedon perusteella yksilöimään. (Laaksonen et al. 2006, 31-32.)

Henkilötieto-käsitteellä ja sähköisen viestinnän tunnistamistieto-käsitteellä on yhteneväisyyksiä. Henkilötieto voi koskea vain luonnollisia henkilöitä eli ihmisiä, kun taas tunnistamistieto voi koskea lisäksi oikeushenkilöitä, joihin luokitellaan yritykset, säätiöt ja yhdistykset. (Laaksonen et al. 2006, 31-32.)

5.2 Henkilötietojen käsittely

Henkilötietojen käsittelyllä voidaan tarkoittaa useita asioita kuten henkilötietojen keräämistä, tallentamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista ja toimenpiteitä, jotka kohdistuvat henkilötietoihin. Ennen varsinaista henkilötietojen käsittelyä on määriteltävä käsittelyn tarkoitus, koska käsittelyyn liittyy tietoturvavelvoitteita. Henkilötietojen käsittelyyn liittyy suunnitteluvelvollisuus, joka velvoittaa rekisterinpitäjän laatimaan selosteen, jossa määritellään käsittelyn tarkoitus, toteutustapa, henkilötietojen hankkimistapa, luovuttaminen ja tietoturvan toteuttaminen. Suunnitteluvelvollisuus toteuttaa laissa määriteltyä hyvää tietojen käsittely- ja tiedonhallintatapaa. Suunnitteluvaiheessa määritellään myös tietoturvavaatimukset nykyisten ja tulevien tarpeiden mukaan. On otettava huomioon, kuka yrityksessä saa henkilötietojen käsittelyoikeuden ja kuka tällaista oikeutta todellisuudessa tarvitsee. (Laaksonen et al. 2006, 35-36.)

Yritysten osalta lähtökohtana voidaan pitää sitä, että työnantajalla on oikeus kerätä työntekijöiden henkilötietoja, mikäli ne ovat tarpeellisia työnantajan ja työntekijän välisen työsuhteen kannalta. Työntekijän suostumusta henkilötietojen käsittelylle ei vaadita, mutta vaatimuksena on, että työnantaja käsittelee työsuhteen kannalta tarpeellisia henkilötietoja, jotka voivat liittyä osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan tarjoamiin etuuksiin. Työnantaja ei saa kerätä tarpeettomia henkilötietoja edes työntekijän suostumuksella. Työnantaja ei voi myöskään kerätä mitä tahansa ja missä laajuudessa tahansa olevaa työntekijää koskevaa henkilötietoa, vaan henkilötiedoilla tulee olla liityntä työnantajan toimintaan. (Laaksonen et al. 2006, 37.)

Henkilötietojen käsittelyyn liittyy myös huolellisuusvelvoite. Sillä tarkoitetaan sitä, että rekisterinpitäjän tulee käsitellä henkilötietoja laillisesti, huolellisuutta ja hyvää tietojenkäsittelytapaa noudattaen. Lisäksi rekisterinpitäjän tulee toimia niin, ettei yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia rajoiteta ilman laissa määrättyä perustetta. Rekisterinpitäjän on myös huolehdittava virheettömyysvaatimuksesta, joka tarkoittaa sitä, että virheellisiä, epätäydellisiä tai vanhentuneita henkilötietoja ei käsitellä. Virheettömyysvaatimus asettaa velvoitteita myös tietoturvanäkökulmasta, sillä tietoturvan kolmeen peruselementtiin kuuluvat luottamuksellisuus, eheys ja käytettävyys. (Laaksonen et al. 2006, 38-40.)

Huolellisuusvelvoite on erittäin tärkeä huomioon otettava seikka henkilötietojen käsittelyssä. Henkilöön liittyvät tiedot voivat olla osittain hyvinkin arkaluonteista tietoa, jos on kyse esimerkiksi sairaudesta. Puhelinnumero ja sähköpostiosoite ovat myös henkilökohtaisia, ja jotkut ihmiset haluavat pitää ne salassa, koska lehti- ja suoramarkkinamyyjät ovat tänä päivänä aktiivisesti yhteydessä kansalaisiin.

5.3 Henkilötietolain tietoturvaperiaatteet ja tietoturvan tasovaatimus

Henkilörekisteri on suojattava niin, että laittomat yritykset päästä rekisteriin käsiksi aiheuttavat ilman viiveitä hälytyksen rekisterinpitäjälle. Monissa yrityksissä tämä ei

kuitenkaan toteudu, mikä tarkoittaa, että käytössä ei ole riittävän kattavia menetelmiä. Laki asettaa lähtökohdaksi, että riittävän tietoturvatason määrittää rekisterinpitäjä itse. Tietoturvantaso riippuu siitä, minkä laatuisia henkilötiedot ovat. Henkilötietojen käyttövaltuuksia tulee myös määritellä, ja yleensä ne määritellään rooliperusteisesti eli työntekijöiden työtehtävien perusteella. Tekniset tietoturvatoimenpiteet tulee ottaa huomioon. Teknisillä tietoturvatoimenpiteillä tarkoitetaan tietojärjestelmän suojausta salasanalla ja asianmukaisella palomuurijärjestelmällä. Laki asettaa siis minimivaatimuksen tietoturvalle, siten että järjestelmiin ei pääse kuka tahansa käsiksi. Mikä on sitten riittävä tietoturvan taso? Riittävä tietoturvan taso ei ole staattinen vaan se on sidoksissa riskien ja tallennettavan materiaalin luonteeseen. (Laaksonen et al. 2006, 42-44.)

Henkilörekistereistä tulee laatia rekisteriselosteet. Henkilötietolaki sisältää erillisen vahingonkorvaussäännöksen. Tämän lain mukaan rekisterinpitäjä on velvollinen korvaamaan taloudellisen ja muun vahingon, joka aiheutuu rekisteröidylle tai muulle henkilölle henkilötietojen huolimattomasta käsittelystä. Henkilö voidaan tuomita rangaistukseen, jos hän tahallaan tai törkeästä huolimattomuudesta jättää henkilötietojen käsittelyn tarkoitukset määrittelemättä tai laiminlyö sen mitä rekisteriselosteen laatimisesta on säädetty laissa. (Nyblin 2009, 117-118.)

6 HAASTATTELU

Haastattelin Turun kaupungin It-suunnittelupäällikköä Jouni Satopäätä. Turun kaupunki jakautuu 20 hallintokuntaan ja jokaisella hallintokunnalla on oma tietoturvavastaava. Satopää kertoo hankkivansa lisäosaamista kouluttamalla itseään joka vuosi seminaarien ja koulutustilaisuuksien merkeissä. Kouluttajista hän mainitsee ainakin Telewaren, joka antaa tietoliikenne- ja tietoturvakoulutusta.

Jounin työtehtäviin kuuluu koko kaupungin tietoturvan hallinnointi. Lisäksi tehtäviin kuuluu tietoturvallisuuden hallintajärjestelmän jatkuva kehittäminen vaadittujen standardien mukaiseksi. Tietoturvallisuus on ala, joka kehittyy jatkuvasti ja sen myötä myös henkilökunta on pidettävä ajan tasalla tietoturvallisuuteen liittyvissä asioissa. Jouni on ennen it-suunnittelupäällikön virkaa työskennellyt kahdessa muussa työtehtävässä Turun kaupungin palveluksessa. Työt hän on aloittanut Turun kaupungilla 1987.

Ihmisiä ei valisteta tarpeeksi tietoturvaan liittyvissä asioissa ja hän pyrkiikin kartoittamaan Turun kaupungin työntekijöiden tietoturvatietoisuutta. Koulutustilaisuuksia järjestetään siten, että aina yksi hallintokunta koulutetaan kerralla. Hallintokuntien varalle on laadittu koulutussuunnitelmat, ja aika ajoin heille järjestetään tietoisku tapahtumia. Turun kaupunki työllistää noin 13 000 työntekijää.

Miten hän kokee eri hallintokuntien henkilöiden suhtautumisen tietoturvaan. Kokevatko ihmiset tietoturvan asioiden mahdollistajana vai työn tekemisen hankaloittavana asiana? Työntekijät kokevat teknisen tietoturvan hankaloittavan työntekoa. Nykypäivänä on paljon eri järjestelmiä ja ohjelmia, joita henkilökunnan tulisi osata käyttää, ja ohjelmia käytettäessä on otettava huomioon mahdolliset tietoturvariskit. Toinen ongelman koituu siitä, että salasanat ovat usein hukassa. Kaupungilla on tällä hetkellä menossa käyttövaltuusprojekti, joka tarkoittaa sitä, että työntekijälle annetaan hänen työroolinsa mukaan käyttöoikeuksia eri järjestelmiin. Satopään mukaan myöhemmin saattaa tulla kokeilun alle verkkopankkitunnuksilla kirjautuminen järjestelmään. Täl-

lainen pankkitunnuksilla kirjautuminen on kuitenkin sähköpostin osalta ongelmallinen.

Mikä on tärkein huomioon otettava seikka, kun puhutaan tietoturvasta ja miten tietoturvatietoisuutta voitaisiin parantaa työntekijöiden keskuudessa? Satopään mukaan käyttäjä on heikoin lenkki. Työnantajat olettavat, että työntekijät osaavat käyttää ohjelmia ja tietokonetta oikein, mutta näin ei kuitenkaan aina ole. Terveydenhuollon puolella on tietoturvaorganisaatio olemassa. Sosiaali- ja terveystoimen puolella käytetään sovellusta, johon voidaan kirjata kaikki läheltä piti-tilanteet. Läheltä piti-tilanteiden avulla pystytään seuraamaan, missä tietojärjestelmän osa-alueissa on havaittavissa koulutuksen puutetta. Tietoturvatietoisuutta voidaan parantaa järjestämällä käyttäjäryhmille koulutusta. Suunnitelmallisella kehittämisellä ja palautteen antamisella on suuri merkitys. Turun kaupungilla on käytössä vaarat ja-haitat ohjelma, joka toteutetaan kaksi kertaa vuodessa. Kyseiseen ohjelmaan ei kuitenkaan oteta mukaan yksittäisiä vaaratilanteita.

Tiedustelin Satopään mielipidettä Lex Nokiasta. Hänen mukaansa Lex Nokia on aivan tarpeeton. Työnantajalla on mahdollisuus kieltää yksityinen viestintä työpaikalla, mutta työnantaja ei pysty seuraamaan, käyttävätkö työntekijät sähköpostia yksityiseen viestintään. Jos Turun kaupungin työntekijän sähköpostiviestin avaamiseen on tarvetta, viestin avaamiseen tarvitaan neljä henkilöä: työnantajan edustaja, työntekijän edustaja (luottamushenkilö) sekä kaksi ”likaisen työn tekijää”. Tapauksesta on laadittava pöytäkirja, joka lähetetään tiedoksi työnantajalle. Lisäksi työntekijälle on ilmoitettava tehdyistä toimista. Satopään mukaan uusi sähköisen viestinnän tietosuojalaki ei estä työntekijöitä vuotamasta yrityssalaisuuksia. Työntekijät voivat ottaa tärkeitä tietoja esimerkiksi muistitikulle, jolloin niitä ei ole havaittavissa enää sähköpostissa.

Haastattelun päätteeksi Jouni kertoi vielä hieman siitä ajasta, jolloin hän oli valmistumassa yliopistolta eli vuonna 1986. Yliopistolla ei kuulemma tuohon aikaa puhuttu vielä tietoturvasta. Tietojärjestelmät eivät kommunikoineet silloin keskenään. Viruksia oli jo silloin. Virukset tulivat levykkeiden mukana ja myöhemmin viruksia alkoi tulla web-selaimen kautta. Noin vuonna 1995-1996 Internet löi itsensä läpi. Internetse-

lain muutti maailman täydellisesti. 1990-luvun alkupuolella otettiin virustorjunta käyttöön. (J.Satopää, henkilökohtainen tiedonanto 22.12.2009.)

7 POHDINTA

Opinnäytetyötä kirjoittaessani olen itsekin väistämättä joutunut pohtimaan kysymystä, onko Lex Nokia tarpeeton vai tarpeellinen. Aloittaessani kirjoittaa opinnäytetyötä en tiennyt Lex Nokiasta juuri mitään. Aihe tuntui lähinnä sekavalta ja monimutkaiselta. Joka päivä sain kuitenkin lukea lehdistä uutta tietoa Lex Nokiasta ja uuden lain valmistelusta. Mielestäni Lex Nokiaa on paisuteltu aivan liian paljon eri medioiden keskuudessa. Ymmärrän toki, että uusi lainmuutos aiheuttaa paljon keskustelua ja mielipiteiden vaihtoa. Mitä enemmän lakia pengotaan, sen enemmän uuden lainmuutoksen varjopuolia tulee esille.

Aiheesta oli helppo tehdä opinnäytetyö, koska kirjallisuutta, lehtiä ja internetjulkaisuja oli saatavilla erittäin paljon. Toisinaan tuntui, että tietoa tulee kaiken aikaa lisää ja työni sivumäärä vain lisääntyy. Työssäni olen käyttänyt pääosin vuonna 2009 kirjoitettua kirjallisuutta ja artikkeleja. Kirjojen tiedot ovat ajan tasalla, mikä on erittäin hyvä asia, jos opinnäytetyötäni käytetään esimerkiksi soveltuvin osin opetuksessa. Työn luonteesta johtuen empiirinen osa jäi melko suppeaksi, mutta pohdintaosiossa yritän tuoda omia mielipiteitä esille.

Uusi laki on sekava, ja ennen kuin tunnistamistietoja voidaan edes alkaa käsitellä, yritysten tulee täyttää monia velvoitteita. Yritysten tulee täyttää huolehtimis-, suunnittelu- ja yhteistoimintavelvoitteet sekä tehdä ennakkoilmoitus tietosuojavaltuutetulle. Mikäli työntekijän sähköpostiliikenteeseen on syytä puuttua, niin työntekijälle pitää ilmoittaa asiasta etukäteen. Tämän lisäksi työnantajan pitää raportoida tietosuojavaltuutetulle toimista, joita on tehty. Uusi laki asettaa siis yrityksille melkoisia vaatimuksia, jos nämä aikovat tarkkailla työntekijöiden sähköpostiliikennettä. Työmäärä yrityksissä lisääntyisi, mikä saattaa tarkoittaa sitä, että yritykseen on palkattava henkilö tai henkilöitä hoitamaan sähköpostiliikenteen tarkkailuun liittyviä tehtäviä. Tämä taas tarkoittaa sitä, että palkkakustannuksiin menee yhä enemmän rahaa. Yritysten tulisi punnita tässä tilanteessa, onko sähköpostiliikenteen tarkkailu ollenkaan kannattavaa vai käytetäänkö yrityksessä johtoportaan voimavarat mieluummin johonkin muuhun.

Koska viestin sisältöön ei saa puuttua, pelkkien tunnistetietojen perusteella pitäisi pystyä päättelemään, sisältääkö sähköpostiviesti yrityssalaisuuksia vai ei. Tämä on mielestäni hyvin hankalaa, koska sähköpostiviestien otsikot eivät välttämättä kerro, mitä sähköpostiviesti tosiasiassa pitää sisällään. Aalto-yliopiston tietoverkkotekniikan professori on todennut lausunnossaan, että ammattilaiset rikolliset eivät käytä sähköpostia tai vaikka käyttäisivätkin, niin he osaavat tehdä sen niin, että eivät jää kiinni. Voin yhtyä täysin hänen mielipiteeseensä. En usko, että kaikkia tietovuototapauksia pystyttäisiin estämään ja havaitsemaan pelkän sähköpostiviestinnän tarkkailun perusteella. Tietovuotoasioita kun pystyttäisiin levittämään muullakin tavoin, kuten ottamalla omalta työkoneelta salaisia ja merkittäviä asioita esimerkiksi muistitikulle.

Sähköisen viestinnän tietosuojalain (SVTSL) uhkana on, että yritykset käyttävät lakia annettujen ohjeiden vastaisesti. Yritykset saattavat ottaa lain käyttöön ilman, että ne ovat täyttäneet annetut huolehtimis-, suunnittelu- ja yhteistoimintavelvoitteet. Ja tämän lisäksi työantajat eivät välttämättä tee tietosuojavaltuutetulle ilmoitusta, vaikka olisivatkin ottaneet uuden lain käyttöön. On myös mahdollista, että työnantaja urkkii työntekijän sähköpostiliikennettä ilman perusteltua syytä. Edellä mainittu voi johtaa siihen, että työntekijän luottamus työnantajaa kohtaan saattaa alkaa horjua. Tästä taas voi seurata erimielisyyksiä työpaikalla. Yhtenä keskeisenä lakiuudistuksen varjopuolena voin nähdä sen, että jotkut tahot sanovat lain loukkaavan ihmisten perusoikeuksia, jotka on taattu perustuslaissa.

Uuden lain avulla työntekijöiden ja työnantajien väliset sähköpostiin liittyvät tunnistetietojenkäsittelyasiat ovat selkiintyneet. Laissa työnantajille on määritetty selvät oikeudet, joista työntekijöiden tulisi olla tietoisia. Voin myös todeta uuden sähköisen viestinnän tietosuojalain parantavan tietoturvaa. Tietokoneisiin voidaan lain myötä asentaa automaattisia hakutoimintoja, mikä tarkoittaa sitä, että jos hakutoiminto havaitsee epäilyttäviä tiedostoja tai kansioita koneessa, niin työnantajan tulee puuttua niihin. Tietoturva paranee, mikäli kaikki epäilyttävät tiedostot saadaan poistettua koneelta. Yritysten tulee ennen uuden sähköisen viestinnän tietosuojalain käyttöönottoa varmistua siitä, että tietoturva-asiat ovat yrityksessä kunnossa.

Kuka tai ketkä uudesta laista hyötyvät? On selvää, että työnantajille koituu lakimuutoksesta suurin hyöty. Laki tosin koskee työnantajien lisäksi virastoja, kirjastoja, yliopistoja, kouluja ja jopa taloyhtiöitä. En usko, että muualla kuin yrityksissä on tarpeeksi resursseja ottaa uutta lakimuutosta käyttöön. Työnantajat pystyvät lain myötä paremmin kontrolloimaan työntekijöiden ajankäyttöä töissä, eli työnantaja saa halutessaan tietää millaisin otsikoin varustettuja sähköpostiviestejä työntekijät lähettelevät ja mihin kellonaikoihin. Uudistuksen hyvänä puolena voidaan nähdä myös se, että tietovuotojen määrää pystytään minimoimaan ja poistamaan ne lähes kokonaan. Näin työnantajan ei tarvitse elää pelossa siitä, että yrityksen tietoja vuodetaan ulkopuolisille. Tosin uusi lakiuudistus ei voi taata sitä, että tietoja ei pystytä vuotamaan ulkopuolisille. Virastoissa, kirjastoissa, yliopistoissa ja kouluissa hyödyt ovat lähes samat kuin työnantajille koituvat hyödyt. Taloyhtiöissä uusi sähköisen viestinnän tietosuojalaki voidaan nähdä hyvänä asiana siltä kannalta, että isännöitsijä pystyy tarkkailemaan netissä surffailua, jos on aihetta epäillä, että verkkoa kuormitetaan vierailemalla esimerkiksi laittomilla sivuilla.

Eri tahojen mielipiteiden yhteenvetona voin ikävä kyllä todeta, että uusi sähköisen viestinnän tietosuojalaki ei ole saavuttanut täydellistä hyväksyntää yksityisten ihmisten eikä yritystenkään keskuudessa. On erittäin mielenkiintoista nähdä tulevaisuudessa, tuleeko tietosuojavaltuutetulle yhtäkään ilmoitusta uuden lain käyttöönottamisesta. Jos yksi yritys ottaisi lain käyttöön, muut saattaisivat seurata perässä, mutta kukaan ei uskalla olla ensimmäinen, koska käyttöönottoa puitaisiin julkisuudessa aivan varmasti. Mieleeni tulee kysymys, onko laki valmis vai tullaanko lakia muuttamaan tulevaisuudessa. Laki voitaisiin ottaa uudelleen käsittelyyn, ja huomioida oikeusoppineiden mielipiteet. Tällä tavoin laista saattaisi tulla täydellisempi, ja lain tulkinnanvaraisuudet poistuisivat. Olisi myös tärkeää, että yksikään taho ei kokisi lakia perusoikeuksien vastaisena, ja perusoikeuksia loukkaavana.

LÄHTEET

Alinen, Henri 2009a. *HEI, meitä VALVOTAAN.* LakimiesUutiset 2/2009, 44-47.

Alinen, Henri 2009b. *Lain hyödyllisyys kyseenalainen.* LakimiesUutiset 2/2009, 46-47.

Dunderfelt, Marja 2009. *Tietosuojalaki teleyrityksen näkökulmasta.* Tietosuoja 1/09 Kolumni, 38.

Helopuro, Sanna, Perttula Juha & Ristola, Juhapekka 2009. *Sähköisen viestinnän tietosuoja.* Helsinki: Talentum.

Järvinen, Petteri 2002. *Tietoturva & yksityisyys*. Jyväskylä: Docendo.

Karppinen, Lauri 2009. *Valvonnan viimeinen keino.* Tietosuoja 2/2009, 7-11.

Laaksonen, Mika, Nevasalo, Terho& Tomula, Karri 2006. *Yrityksen tietoturvakäsikirja.* Helsinki: Edita.

Keskuskauppakamari ja Helsingin seudun kauppakamari. *Yritysten rikosturvallisuus 2008. Riskit ja niiden hallinta.*

Keskusrikospoliisi rikostietopalvelu 22.10.2008. *Yrityksiin kohdistuvan ja niitä hyödyntävän rikollisuuden tilannekuva syksy 2008.* Arkistoviite KRP/RTP 5876/213/08.

Lagus, Antti J. 2009. *Tietoturvan perustaidot kunnossa.* Tietosuoja 1/2009, 24-25.

Nyblin, Klaus 2009. *Työelämän sähköposti.* Helsinki:TALENTUM.

Ruohonen, Mika 2002. *Tietoturva*. Jyväskylä: Docendo.

Saario, Kaisa 2009. *Salainen tieto ajoissa suojaan.* Tietosuoja 3/2008, 8-9.

Satopää, Jouni 22.12.2009 (henkilökohtainen tiedonanto [viitattu 11.1.2010]). Turun kaupunki. Turku.

Keskuskauppakamari ja Helsingin seudun kauppakamari. *Yritysten rikosturvallisuus 2008. Riskit ja niiden hallinta.*

Elektroniset lähteet

Asiaa tietosuojasta 1/2009.*Yhteisötilaajan oikeus käsitellä tunnistamistietoja väärinkäytöstapauksissa.* [online, viitattu 15.2.2010]. Saatavilla www-muodossa: <URL: http://www.tietosuoja.fi/uploads/lf9uwtx86.pdf>.

HE 48/2008. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta [online, viitattu 30.9.2009]. Saatavilla www-muodossa:
<URL:http://217.71.145.20/TRIPviewer/show.asp?tunniste=HE+48/2008&base=erhe&palvelin=www.eduskunta.fi&f=WORD>.

Helsingin Sanomat 2009. *Kysymyksiä ja vastauksia Lex Nokiasta.* Helsingin Sanomat 4.3.2009. [online, viitattu 6.10.2009]. Saatavilla www-muodossa:
<URL:http://www.hs.fi/politiikka/artikkeli/Kysymyksi%C3%A4+ja+vastauksia+Lex+Nokiasta/1135244024320>.

Helsingin Sanomat 2010. *Lex Nokiasta valitettiin Euroopan ihmisoikeustuomioistuimeen.* Helsingin Sanomat 10.1.2010. [online, viitattu 25.1.2010]. Saatavilla www-muodossa:
<URL:http://www.hs.fi/kotimaa/artikkeli/Lex+Nokiasta+valitettiin+Euroopan+ihmisoikeustuomioistuimeen/1135252024094>.

Himanen, Keijo 2009. *Urkintaa vai tietoturvaa.* Helsingin Sanomat 4.5.2008.[online, viitattu 30.9.2009]. Saatavilla www-muodossa:
<URL:http://hs.fi/haku/?kaikkiSanat=urkintaa+vai+tietoturvaa&hae=Hae>.

HS-STT 2009. *Vanhanen sallisi Lex Nokia –tarkastukset yrityksissä.* Helsingin Sanomat 19.5.2009. [online, viitattu 6.10.2009]. Saatavilla www-muodossa:
<URL:http://www.hs.fi/politiikka/artikkeli/Vanhanen+sallisi+Lex+Nokia+tarkastukset+yrityksiss%C3%A4/1135246072507>.

Hujanen, Touko 2009. *Osa yliopistoista aikoo ottaa Lex Nokian käyttöön.* Helsingin Sanomat 19.6. 2009. [online, viitattu 6.10.2009]. Saatavilla www-muodossa:
<URL:http://www.hs.fi/talous/artikkeli/Osa+yliopistoista+aikoo+ottaa+Lex+Nokian+k%C3%A4ytt%C3%B6%C3%B6n/1135247036133>.

Ilta-Sanomat 2009. *Keskusrikospoliisi tyrmää Lex Nokian.* Ilta-Sanomat 21.2.2009. [online, viitattu 6.10.2009]. Saatavilla www-muodossa:
<URL:http://www.iltasanomat.fi/uutiset/kotimaa/uutinen.asp?id=1643218>.

Liikenne- ja viestintäministeriö. *Kysymyksiä ja vastauksia, sähköisen viestinnän tietosuojalaki.* Liikenne- ja viestintäministeriö. [online, viitattu 6.10.2009]. Saatavilla www-muodossa: <URL:http://www.lvm.fi/web/fi/245>.

Rantanen, Miska 2009. *Reijo Aarnio: Tietosuojalaki rikkoo viestintäsalaisuutta*. Helsingin Sanomat 21.2.2009. [online, viitattu 6.10.2009]. Saatavilla www-muodossa:

<URL:http://www.hs.fi/politiikka/artikkeli/Reijo+Aarnio+Tietosuojalaki+rikkooviestint%C3%A4salaisuutta/HS20090221SI1YO02pzl>.

Sajari, Petri 2008. *Oikeusoppineet: Lex Nokia rikkoo perustuslakia.* Helsingin Sanomat 20.11.2008. [online, viitattu 6.10.2009]. Saatavilla www-muodossa: <URL:http://www.hs.fi/talous/artikkeli/Oikeusoppineet+Lex+Nokia+rikkoo+perustuslakia/1135241246344>.

Sajari, Petri 2009. *Kännykkäyhtiön painostus sai aikaan Lex Nokian.* Helsingin Sanomat 1.2.2009. [online, viitattu 15.9.2009]. Saatavilla www-muodossa: <URL:http://www.hs.fi/talous/artikkeli/K%C3%A4nnykk%C3%A4yhti%C3%B6n+painostus+sai+aikaan+Lex+Nokian/1135243187834>.

Simula, Matti 2009. *Lex Nokia: SK löysi todisteet painostuksesta.* Suomen Kuvalehti 23.2.2009. [online, viitattu 6.10.2009]. Saatavilla www-muodossa: <URL:http://suomenkuvalehti.fi/jutut/kotimaa/lex-nokia-sk-loysi-todisteet-painostuksesta>.

Suomen perustuslaki 11.6.1999/731.[online, viitattu 30.9.2009]. Saatavilla www-muodossa: <URL:http://www.finlex.fi/fi/laki/ajantasa/1999/19990731?search[type]=pika&search[pika]=PERUSTUSLAKI>.

Sähköisen viestinnän tietosuojalaki 16.6.2004/516 [online, viitattu 15.9.2009 ja 23.9.2009]. Saatavilla myös www-muodossa: <URL:http://www.finlex.fi/fi/laki/ajantasa/2004/20040516>.

Tietosuojavaltuutettu 2009. *Yhteisötilaajan oikeus käsitellä tunnistamistietoja väärinkäytöstapauksissa.* Asiaa tietosuojasta 1/2009. [online, viitattu 15.2.2009]. Saatavilla www-muodossa: <URL:http://www.tietosuoja.fi/46871.htm>.

Tirkkonen, Kirsi 2009. *Yritykset väistelevät Lex Nokiaa.* YLE uutiset 14.10.2009. [online, viitattu 14.10.2009]. Saatavilla www-muodossa: <URL:http://yle.fi/uutiset/talous_ja_politiikka/2009/10/yritykset_vaistelevat_lex_nokiaa_1077329.html>.

Welp, Klaus 2009. *Lakia vahvempi Nokia.* Helsingin Sanomat 1.2.2009. [online, viitattu 30.9.2009]. Saatavilla www-muodossa: <URL:http://www.hs.fi/politiikka/artikkeli/Lakia+vahvempi+Nokia/1135244022164>

YLE uutiset 2009. *Lex Nokia hyväksyttiin eduskunnassa.* YLE.fi 4.3.2009. [online, viitattu 6.10.2009]. Saatavilla www-muodossa: <URL:http://yle.fi/uutiset/talous_ja_politiikka/2009/03/lex_nokia_hyvaksyttiin_eduskunnassa_588957.html>.

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

9 §

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 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.

Ehdotus

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.

Voimassa oleva laki

12 §

Käsittely teknistä kehittämistä varten

Teleyritys ja lisäarvopalvelun tarjoaja voi käsitellä tunnistamistietoja palvelujen 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.

Ehdotus

12§

Käsittely teknistä kehittämistä varten

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

Yhteisötilaaja voi käsitellä tunnistamis-tietoja 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.

Voimassa oleva laki

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.***

Ehdotus

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, yhteenlaskettuun kokoon, tyyppiin, määrään, yhteystapaan tai kohdeosoitteisiin.

***Yhteisötilaaja saa käsitellä tunnistamistietoja manuaalisesti, jo*s 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 (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 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 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

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.

Ehdotus

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 ja selvittämiseksi.***

Voimassa oleva laki

20 §

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.

Edellä 1 momentissa tarkoitettuihin toimiin saa ryhtyä vain, jos toimet ovat välttämättömiä verkkopalvelujen tai viestintäpalvelujen taikka viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi.

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 epäillä, että viestiä käytetään rikoslain 38 luvun 5 §:ssä säädettyyn tietoliikenteen häirintään.

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.

Viestintävirasto voi antaa tarkempia määräyksiä tietoturvaloukkausten tässä pykälässä tarkoitetusta teknisestä torjumisesta ja tietoturvaan kohdistuvien häiriöiden poistamisesta.

Ehdotus

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 ohjelmakäskyn 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.

Voimassa oleva laki

32 §

Tietosuojavaltuutetun tehtävät

Tietosuojavaltuutetun tehtävänä on valvoa:

1) edellä 4 luvussa tarkoitettua paikkatietojen käsittelyä;

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

3) edellä 7 lukuun sisältyvien suoramarkkinointia koskevien säännösten noudattamista; sekä

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

Ehdotus

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 tiedon-saantioikeuksia 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

33 §

Ohjaus- ja valvontaviranomaisten **tiedonsaantioikeus.**

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 merkittävi-

en tietoturvaloukkausten ja -uhkien selvittämiseksi ja jos Viestintäviraston tai tietosuojavaltuutetun arvion mukaan on syytä epäillä, että jokin seuraavista tunnusmerkistöistä täyttyy:

Ehdotus

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*****:**

Voimassa oleva laki

34 §

Valvontaviranomaisten vaitiolovelvollisuus **ja tietojen luovuttaminen**

Viestintäviraston ja tietosuojavaltuutetun 33 §:n 3 momentin nojalla saamat tiedot luottamuksellisista viesteistä, tunnistamistiedoista ja paikkatiedoista 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.

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 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.

Muilta osin valvontaviranomaisen tietojen salassapidosta ***on voimassa, mitä*** viranomaisen toiminnan julkisuudesta annetussa laissa (621/1999) säädetään.

(*34 §:n 2 momentti*)

(*34 §:n 3 momentti*)

(*34 §:n 2 momentti*)

Ehdotus

34 §

Valvontaviranomaisten vaitiolovelvollisuus

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.

(*34 a §:n 1 momentti*)

(*34 a §:n 2 momentti*)

(*34 a §:n 3 momentti*)

Muilta osin valvontaviranomaisten tietojen salassapidosta ***säädetään*** viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) säädetään.

34 a §

Valvontaviranomaisten tietojen luovuttaminen

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.

Viestintävirastolla on 34 §:n 1 momentissa tarkoitetun salassapitosäännöksen tai muun tietojen luovuttamista koskevan rajoituksen estämättä oikeus luovuttaa tietoturva-loukkauksia 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 viranomai-

selle 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.

Voimassa oleva laki

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 oikeuksista, *tai*

8) harjoittaa suoramarkkinointia 7 luvussa säädetyn vastaisesti,

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

Rangaistusta ei tuomita, jos rikkomus on vähäinen.

Ehdotus

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 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.

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

1 luku

Yleiset säännökset

Soveltamisala

Henkilötietojen käsittelyyn sovelletaan henkilötietolakia (523/1999) ja sähköisen viestinnän tietosuojalakia (516/2004), jollei tässä laissa toisin säädetä.

Ehdotus

1 luku

Yleiset säännökset

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.

Voimassa oleva laki

7 luku

Erinäisiä säännöksiä

21 §

Yhteistoiminta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä

Työntekijöihin kohdistuvan kameravalvonnan, 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.

Ehdotus

7 luku

Erinäisiä säännöksiä

21 §

Yhteistoiminta teknisin menetelmin toteutetun valvonnan ja tietoverkon käytön järjestämisessä

Työntekijöihin kohdistuvan kameravalvonnan, 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.

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

19 §

Muuhun lainsäädäntöön perustuvien suunnitelmien, periaatteiden ja käytäntöjen käsittely

Yhteistoimintaneuvotteluissa tulee käsitellä:

4) sähköpostin ja tietoverkon käytön periaatteet;

Ehdotus

19 §

Muuhun lainsäädäntöön perustuvien suunnitelmien, periaatteiden ja käytäntöjen käsittely

Yhteistoimintaneuvotteluissa tulee käsitellä:

4) sähköpostin ja tietoverkon käytön periaatteet sekä työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely;

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

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 sekä sähköpostin ja tietoverkon käyttö; (13.8.2004/762)

Ehdotus

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 sekä sähköpostin ja tietoverkon käyttö sekä virkamiehen ja työntekijän sähköpostin ja muuta sähköistä viestintää koskevien tietojen käsittely;

Tyhjennä lomake

ENNAKKOILMOITUS TUNNISTAMIS-TIETOJEN KÄSITTELYN ALOITTAMISESTA

Peruste: Sähköisen viestinnän tietosuojalaki 13 i §

* katso ennakkoilmoituksen täyttöohje

1 Ilmoituksen tekijänä oleva yhteisötilaaja	Yhteisötilaajan nimi	Y-tunnus
2 Yhteisötilaajan yhteystiedot	Osoite	Puhelin
3 Yhteisötilaajan puolesta ilmoitusasiaa käsittelevä yhteyshenkilö	Nimi ja asema	
4 Yhteyshenkilön yhteystiedot	Osoite	
	Puhelin	Sähköpostiosoite
5a Ilmoitusperuste: luvaton käyttö	☐ Maksullisen tietoyhteiskuntapalvelun luvaton käyttö ☐ Viestintäverkon tai viestintäpalvelun luvaton käyttö Yhteisötilaajan viestintäverkon käyttäjien lukumäärä *	
5b Ilmoitusperuste: yrityssalaisuuksien paljastamisen ehkäiseminen	☐ Yrityssalaisuuksien paljastamisen ehkäiseminen Yrityssalaisuuksien käsittelyyn oikeutettujen lukumäärä henkilöä*	
6 Nimetyt henkilöt, joiden tehtäviin tunnistetietojen käsittely kuuluu tai määrittely tehtävistä (13 c § 1 mom)*	☐ Litteellä	
7 Miten huolehtimisvelvollisuus on toteutettu (13 b §)*	☐ Litteellä	
8 Miten yhteistoimintavelvoitteen noudattaminen sekä tiedottaminen käyttäjille on toteutettu (13 c § 2 ja 3 mom)*	☐ Litteellä	
9 Tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt (13 i § 1 mom 1 kohta) *	☐ Litteellä	
10 Huomautus	Ilmoitukseen on liitettävä viestintäverkon tai viestintäpalvelun käyttäjälle väärinkäytösten ehkäisemiseksi annetut **kirjalliset ohjeet**.	
11 Lisätietoja		

Huom! Ennakkoilmoituksen voi lähettää postitse tai sähköpostitse osoitteeseen **valvonta.tietosuoja@om.fi**. Kirjekuoren päälle tulee kirjoittaa viite **VALVONTA**.

Tulosta

ENNAKKOILMOITUKSEN TÄYTTÖOHJEET

5a ja 5b

Ilmoitusperusteena voi olla joko luvaton käyttö tai yrityssalaisuuksien paljastamisen ehkäiseminen tai molemmat yhdessä.

5a Yhteisötilaajan viestintäverkon käyttäjien lukumäärä

Käyttäjät voivat olla esim. yhteisötilaajan henkilökuntaa tai ulkopuolisia henkilöitä, joilla on käyttöoikeus yhteisötilaajan viestintäverkkoon. Asunto-osakeyhtiöiden osalta ilmoitetaan verkkoon liitettyjen huoneistojen määrä ja muiden yhteisötilaajien osalta niiden käyttäjien määrä, jota valvonta koskee. Lukumäärä tulee ilmoittaa mahdollisimman tarkasti ennakkoilmoituksen tekohetken mukaan.

5b Yrityssalaisuuksien käsittelyyn oikeutettujen lukumäärä

Yhteisötilaajan tulee ennen tunnistamistietojen käsittelyn aloittamista rajoittaa pääsyä keskeisiin yrityssalaisuuksiin. Yrityssalaisuuksien käsittelyyn oikeutetuilla henkilöillä tarkoitetaan niitä tiettyjä tehtäviä hoitavia käyttäjiä, joilla on pääsy yrityssalaisuuksiin ja joita valvonta koskee. Lukumäärä tulee ilmoittaa mahdollisimman tarkasti ennakkoilmoituksen tekohetken mukaan.

6 Nimetyt henkilöt, joiden tehtäviin tunnistetietojen käsittely kuuluu tai määrittely tehtävistä

Tunnistamistietoja voivat käsitellä vain yhteisötilaajan viestintäverkon ja viestintäpalvelun ylläpidosta ja tietoturvasta sekä turvallisuudesta huolehtivat henkilöt. Yhteisötilaaja voi vaihtoehtoisesti määritellä ne tehtävät tai esimerkiksi toimintayksiköt, joissa tunnistamistietoja voidaan käsitellä ko. tarkoituksissa. Jos yhteisötilaaja hankkii ko. palvelun ulkopuoliselta taholta, riittävää on, että palveluntarjoajan kyseiset tehtävät tai toiminnot on määritelty.

7 Miten huolehtimisvelvollisuus on toteutettu

Yhteisötilaajan tulee selvittää, millä tavalla se on rajoittanut pääsyä tietoverkkoon tai yrityssalaisuuksiin. Käytännössä pääsyä voi rajoittaa mm. kulunvalvonnalla ja tietohallinnollisin toimenpitein (esim. käyttäjätunnuksin, salasanoin tai muutoin käyttäjäoikeuksia hallinnoimalla).

Yhteisötilaajan tulee huolehtia siitä, että tietoturvallisuuden taso on riittävä. Yhteisötilaajan suorittamia tietoturvatoimenpiteitä voi havainnollistaa esim. tietojärjestelmien ja tietoverkon käyttöä koskevilla säännöillä tai selonteolla noudatetusta tietoturvapolitiikasta.

8 Miten yhteistoimintavelvoitteen noudattaminen sekä tiedottaminen käyttäjille on toteutettu

Ennen kuin työnantaja-asemassa oleva yhteisötilaaja voi alkaa käsitellä tunnistamistietoja, on käsittelyn perusteista, tavoitteista, tarkoituksesta ja vaikutuksista neuvoteltava niiden työntekijöiden edustajien kanssa, joita asia koskee. Yhteistoimintamenettelyssä käsiteltäviin asioihin kuuluvat esim. 1) tunnistamistietojen käsittelyn tarkoitus 2) viestintäverkon käytöstä laaditut ohjeet, 3) tunnistamistietojen käsittelijät tai tehtävät, joihin käsittelyä liittyy, 4) automaattisen haun toimintaperiaatteet, 5) millä perusteella luvattoman käytön katsotaan aiheuttavan työnantajalle merkittävää haittaa ja vahinkoa tai millä perusteella työnantaja katsoo yrityssalaisuuden olevan keskeinen sekä 6) selkat ja perusteet, joiden perusteella automaattinen tai manuaalinen käsittely on mahdollista.

Mikäli yhteisötilaaja ei ole yhteistoimintalainsäädännön piiriin kuuluva työnantaja, on sen kuultava työntekijöitä mainituista seikoista ja tiedotettava niistä. Jos yhteisötilaaja ei ole työnantaja, on sen tiedotettava käyttäjään tunnistamistietojen käsittelyssä noudatettavista menettelyistä ja käytännöistä.

Yhteisötilaaja voi toimittaa liitteenä esim. yhteistoimintamenettelystä laaditun pöytäkirjan, työntekijöiden kuulemisesta laaditun asiakirjan tai laatimansa tiedotteen käyttäjille. Asiakirjasta tulee ilmetä miten ja kenen kanssa asiaa on käsitelty ja mitä on päätetty.

9 Tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt

Ennakkoilmoituksesta on käytävä ilmi tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt. Yhteisötilaaja voi toimittaa esim. asiakirjan, josta ilmenee automaattisessa haussa käytettävien järjestelmien kuvaukset sekä käytössä olevat hakukriteerit tai tunnistamistietojen käsittelijöille (ylläpitäjät, tietoturvasta tai turvallisuudesta vastaavat) antamansa ohjeet sekä koulutussuunnitelman (yleinen kuvaus). Asiakirjasta on käytävä ilmi, miten tunnistamistietojen käsittelyn asianmukaisuudesta on huolehdittu. Jos yhteisötilaaja hankkii tunnistamistietojen käsittelypalvelun ulkopuoliselta taholta, tulee ko. palveluntarjoajan tunnistamistietojen käsittelyssä noudatettavat perusteet ja käytännöt selvittää.

10 Viestintäverkon tai viestintäpalvelun käyttäjälle väärinkäytösten ehkäisemiseksi annetut kirjalliset ohjeet

Tunnistamistietojen käsittelyn aloittaminen edellyttää, että yhteisötilaaja laatii kirjallisen ohjeen, jossa se määrittelee, miten sen viestintäverkkoa ja viestintäpalveluita saa käyttää. Ohjeessa on oltava riittävän tarkka informaatio viestintäverkon käytölle asetetuista rajoituksista. Ohjeesta tulee olla selkeästi ymmärrettävissä, mikä on väärinkäyttöä. Lisäksi ohjeesta tulee ilmetä, miten tietoverkkoa, sähköpostia ja muita sähköisiä viestimiä saa käyttää ja/tai miten yrityssalaisuuksia saa käsitellä tietoverkoissa.

Tyhjennä lomake

SELVITYS MUUTOKSISTA TUNNISTAMIS-TIETOJEN KÄSITTELYSSÄ

Peruste: Sähköisen viestinnän tietosuojalaki 13 i §

1 Ilmoituksen tekijänä oleva yhteisötilaaja	Yhteisötilaajan nimi	Y-tunnus
2 Yhteisötilaajan yhteystiedot	Osoite	Puhelin
3 Yhteisötilaajan puolesta ilmoitusasiaa käsittelevä yhteyshenkilö	Nimi ja asema	
4 Yhteyshenkilön yhteystiedot	Osoite	
	Puhelin	Sähköpostiosoite
5 Selvitys olennaisista muutoksista tunnistamistietojen käsittelyssä	☐ Liitteellä	

Huom! Selvityksen tunnistamistietojen käsittelyssä tapahtuneista muutoksista voi lähettää postitse tai sähköpostitse osoitteeseen **valvonta.tietosuoja@om.fi**. Postitse lähetettäessä kirjekuoren päälle tulee kirjoittaa viite **VALVONTA**.

Tulosta

SELVITYKSEN TÄYTTÖOHJEET

5 Selvitys olennaisista muutoksista tunnistamistietojen käsittelyssä

Yhteisötilaajan on ilmoitettava ennalta tietosuojavaltuutetulle tunnistamistietojen käsittelyn aloittamisesta. Ennakkoilmoituksesta on käytävä ilmi tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt, tehtävät, joissa tunnistamistietoja käsitellään sekä se, miten yhteisötilaaja on järjestänyt käsittelyä edeltävän tiedottamisvelvollisuutensa.

Jos ennakkoilmoituksessa selvitetyissä asioissa tapahtuu olennaisia muutoksia, tulee niistä toimittaa uusi selvitys tietosuojavaltuutetulle. Uusi ilmoitus on tehtävä esimerkiksi silloin, kun

- tunnistamistietoja ryhdytään käsittelemään ennakkoon ilmoitetusta poikkeavalla perusteella,
- kun tunnistamistietojen automaattisen käsittelyn kriteerit muuttuvat,
- käyttäjille annettujen ohjeiden sisältöä muutetaan merkittävästi tai
- tunnistamistietojen käsittelyoikeuksia annetaan kokonaan erityyppisissä tehtävissä toimiville henkilöille, kuin mitä ennakkoilmoituksessa on esitetty.

Tyhjennä lomake

SELVITYS TUNNISTAMISTIETOJEN MANUAALISESTA KÄSITTELYSTÄ

Peruste: Sähköisen viestinnän tietosuojalaki 13 § 2 momentti

1 Ilmoituksen tekijänä oleva yhteisötilaaja	Yhteisötilaajan nimi	Y-tunnus
2 Yhteisötilaajan yhteystiedot	Osoite	Puhelin
3 Yhteisötilaajan puolesta ilmoitusasiaa käsittelevä yhteyshenkilö	Nimi ja asema	
4 Yhteyshenkilön yhteystiedot	Osoite	
	Puhelin	Sähköpostiosoite
5 Tunnistamistietojen käsittely	☐ Tunnistamistietoja ei ole käsitelty manuaalisesti ☐ Maksullisen tietoyhteiskuntapalvelun luvaton käyttö, kertaa ☐ Viestintäverkon tai viestintäpalvelun luvaton käyttö, kertaa ☐ Yrityssalaisuuksien paljastamisen ehkäiseminen, kertaa	
6 Lisätietoja	☐ Liitteellä	

Huom! Selvityksen tunnistamistietojen manuaalisesta käsittelystä voi lähettää postitse tai sähköpostitse osoitteeseen **valvonta.tietosuoja@om.fi**. Postitse lähetettäessä kirjekuoren päälle tulee kirjoittaa viite **VALVONTA**.

Tulosta

VUOSI-ILMOITUKSEN TÄYTTÖOHJEET

5 Tunnistamistietojen käsittely

Sähköisen viestinnän tietosuojalain 13 i §:n 2 momentin mukaan 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.

Ilmoita tekemästäsi tunnistamistietojen manuaalisesta käsittelystä rastittamalla soveltuva kohta tai kohdat ja kirjoittamalla käsittely tapahtumien lukumäärä annettuun tilaan.

Muista, että lukumäärään tulee sisältyä myös parhaillaan meneillään olevat käsittelytapahtumat.

Sähköisen viestinnän tietosuojalain 13 g §:n mukaan yhteisötilaajan on säilytettävä tunnistamistietojen manuaalisesta käsittelystä laatimiaan selvityksiä vähintään kaksi vuotta. Selvityksistä muodostuu henkilötietolain mukainen henkilörekisteri. Ensimmäistä kertaa vuosi-ilmoitusta lähettäessäsi liitä mukaan manuaalisten tunnistamistietojen käsittelyn selvityksistä muodostuvan henkilörekisterin rekisteriseloste.