VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Elina Annika Kivioja

URKINTALAKI

Liiketalous ja matkailu

2010

VAASAN AMMATTIKORKEAKOULU

Liiketalouden koulutusohjelma

TIIVISTELMÄ

Tekijä	Elina Kivioja
Opinnäytetyön nimi	Urkintalaki
Vuosi	2010
Kieli	suomi
Sivumäärä	68
Ohjaaja	Tuula Hartman

Tämän opinnäytetyön tavoite on antaa kattava kuva siitä, millä keinoilla työnantaja voi lukea työntekijöidensä sähköpostiviestejä, valvoa Internetin ja intranetin käyttöä työpaikoilla, ja näin estää yrityssalaisuuksiensa oikeudettomat paljastumiset ja tietoverkon väärinkäytökset.

Tietoverkon väärinkäytösten osalta työni perustuu pääasiassa sähköisen viestinnän tietosuojalain säännöksiin ja lain esitöihin. Työnantajan oikeuksien osalta hakea esille ja lukea työntekijöiden sähköpostiviestejä perustuu yksityisyyden suojasta työelämässä annettuun lakiin ja sen esitöihin.

Sähköisen viestinnän tietosuojalain uudistus tunnetaan paremmin nimellä Lex Nokia, ja se on tullut voimaan negatiivisen mediakeskustelun saattelemana kesäkuussa 2009. Sähköisen viestinnän tietosuojalain uudistus katsottiin olevan tarpeellinen, koska nykypäivän tietoyhteiskunnan elintärkeät toiminnot ovat suuresti riippuvaisia viestintäverkoista, -palveluista ja tietojärjestelmistä. Näiden suojaamisessa keskeisessä asemassa on sähköisten tieto- ja viestintäjärjestelmien toiminnan varmistaminen. Lakien muuttamisen tarkoituksena oli tehostaa tietoturvauhkien torjumista ja selvittämistä. Lex Nokialla haluttiin varmistaa yritysten toimintaedellytyksiä kattamalla se lainsäädännöllinen aukko, joka etenkin yrityssalaisuuksien suojassa sähköisessä viestintäympäristössä oli auki.

Asiasanat sähköposti, viestintäverkko, yrityssalaisuus, tunnistamistieto

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Liiketalouden koulutusohjelma

ABSTRACT

Author	Elina Kivioja
Title	Snoop Law
Year	2010
Language	Finnish
Pages	68
Name of Supervisor	Tuula Hartman

The goal of this thesis is to present the means how an employer can read an employee's e-mails, control the use of the Internet at work places and this way prevent unauthorized use of business secrets and control the misuse of information network.

This thesis is based on the electronic communication privacy protection act concerning the misuse of network and unauthorized use of business secrets. What is said about employer's rights on reading employees' e-mail is based on privacy protection act at working places act and its legislative history.

The reform of electronic communication privacy protection act is better known as Lex Nokia. The new legislation came into operation summer 2009 with negative media coverage. Today's vital functions are greatly dependent on information networks and systems, so the reform was considered necessary. It is important to secure the functions of network systems by protecting the electronic environment. The purpose of the reform is to intensify the prevention of data security threats and their solution. Lex Nokia covers the pre-exististent legislative flaw and helps enterprises to prevent and solve unauthorized use of business secrets and control the misuse of information network.

Keywords e-mail, network, business secret, identification data

SISÄLLYS

1 JOHDANTO

Opinnäytetyöni käsittelee niitä keinoja, millä työnantaja voi valvoa työntekijän sähköposti- ja verkkoliikennettä sähköisen viestinnän tietosuojalain sallimien oikeuksien rajoissa selvittääkseen verkon luvattomat käytöt ja oikeudettomat yrityssalaisuuksien paljastamiset. Työni käsittelee myös työnantajan oikeuksia hakea esille ja lukea työntekijöiden sähköpostiviestejä yksityisyyden suojasta työelämässä annetun lain rajoissa. Opinnäytetyöni tarkoitus on antaa pääasiassa työnantajalle, mutta myös työntekijän luettavaksi kattava kokonaisuus siitä, missä tilanteissa työnantaja voi lukea työntekijöidensä sähköpostiviestejä, ja valvoa Internetin ja intranetin käyttöä ja näin estää yrityssalaisuuksiensa luvattomat paljastumiset ja tietoverkon väärinkäytökset. Sähköisen viestinnän tietosuojalain lakiuudistus antaa työnantajalle laajemmat oikeudet tunnistamistietojen käsittelylle väärinkäytöstapauksissa. Sähköisen viestinnän tietosuojalain uudistus tunnetaan paremmin nimellä Lex Nokia, ja se on tullut voimaan kesäkuussa 2009. Mediassakin paljon huomiota saanut lakimuutos on ajankohtainen ja keskustelua herättävä aihe, joka on yksi syy miksi päädyin kirjoittamaan opinnäytetyöni aiheesta.

Lex Nokia, tai urkintalaiksikin kutsuttu lakiehdotus sai paljon kielteistä huomiota osakseen syksyllä ja keväällä 2008 - 2009. Se oli yleisen mielipiteen mukaan perustuslain vastainen, koska uudistuksen myötä työantaja saisi jatkossa seurata työntekijän viestintää ja Internetin käyttöä laajemmin. Tämä puolestaan jossain määrin kaventaisi työntekijän yksityisyyden suojaa. Negatiivisen keskustelun taustalla saattoi pohjimmiltaan olla se, että tietoyhteiskunnan edellyttämä lainsäädäntö otti ensiaskeleitaan ja siitä käyty julkinen keskustelu heijasti pelkoa uusien ilmiöiden käsittelyä kohtaan. Sähköisen viestinnän tietosuojalain uudistus katsottiin kuitenkin olevan tarpeellinen, koska yhteiskunnan elintärkeät toiminnot ovat kiinteästi riippuvaisia viestintäverkoista, viestintäpalveluista ja tietojärjestelmistä, ja näiden suojaamisessa keskeisessä asemassa on sähköisten tieto- ja viestintäjärjestelmien toiminnan varmistaminen. Lakien muuttamisen tarkoituksena oli tehostaa tietoturvauhkien torjumista ja selvittämistä. Suomi on myös tuotekehityksen ja korkean teknologian johtavia maita, ja tämän takia myös

lainsäädännön tulisi antaa mahdollisuus yritysten ja työnantajien suojella yrityssalaisuuksiaan mahdollisimman tehokkaasti. Lex Nokialla haluttiin varmistaa yritysten toimintaedellytyksiä kattamalla se lainsäädännöllinen aukko, joka etenkin yrityssalaisuuksien suojassa sähköisessä viestintäympäristössä oli auki. (Helopuro, Perttula & Ristola 2009, 96-97.) (HE 48/2008, 12.)

Tutkimuskysymyksiä työssäni ovat, mitä oikeuksia työnantajalla on seurata työntekijän sähköpostiliikennettä ja viestien sisältöä. Mitä keinoja työnantajalla on tietoverkossa tapahtuvien väärinkäytösten estämiseksi ja selvittämiseksi liiketoiminnassa? Mitä työnantajan tulee lain mukaan vähintään tietää velvollisuuksistaan riittävän tietoturvan ja tietosuojan toteuttamiseksi sähköisestä viestinnästä.

Aloitan opinnäytetyöni kirjoittamalla, mitä yksityisyyden suoja perusoikeutena tarkoittaa ja kuinka se näkyy sähköisten viestien osalta liike-elämässä. Käsittelen työssäni myös yrityssalaisuuksien suojaa, koska pääaiheeni tarkoituksena on yrityssalaisuuksien suojan parantaminen. Kirjoitan myös kuinka ja kuka kyseisten lakien noudattamista valvoo ja mitkä ovat rangaistusseuraamukset sähköisen viestinnän tietosuojalain laiminlyömisestä. Lopuksi otan kantaa onko sähköisen viestinnän tietosuojalain uudistukset vaikuttanut nykypäivän liike-elämään ja työntekijöiden yksityisyyteen.

Olen rajannut aiheeni verkkoliikenteen seuraamisesta yksityisyrityksiin, en käsittele valtion tai kunnan työpaikkojen verkkoliikenteen seurantaa. Lisäksi olen rajannut palvelu- ja viestintäverkossa tapahtuvan liikenteen valvonnan vain yhteisötilaajan tarjoaman sähköposti- ja verkkoliikenteen valvontaan, en puhelin- tai muun liikenteen valvontaan. Tunnistamistietojen käsittelyoikeutta käsittelen vain yhteisötilaajan osalta, en teleyrityksen tai viestintäpalveluntarjoajan osalta. Sähköisen viestinnän tietosuojalain soveltamisesta ei ole oikeuskäytäntöä vielä, koska lakiuudistus yhteisötilaajien tunnistamistietojen käsittelyoikeuksista on suhteellisen uusi, eikä lakia ole ryhdytty soveltamaan toivotussa laajuudessa.

2 YKSITYISELÄMÄN SUOJA JA SANANVAPAUS

Suomen perustuslain 10 pykälän mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu ja henkilötietojen suojasta säädetään tarkemmin lailla. Myös kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton (L731/1999). Säännös kirjesalaisuudesta turvaa jokaiselle oikeuden luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Tämä merkitsee esimerkiksi suojaa kirjeiden tai muiden suljettujen viestien avaamista tai hävittämistä sekä puhelujen kuuntelemista tai nauhoittamista vastaan. Säännös ei suojaa vain viestin lähettäjää, vaan kyseessä on molempien viestinnän osapuolten perusoikeus. Yksityisyyden suojaan kuuluu myös viestinnän luottamuksellisuus, mikä tarkoittaa sitä, että viestin sisällön suojan lisäksi suoja ulottuu myös niihin tunnistamistietoihin, joista voidaan tunnistaa luonnollinen henkilö. Määräykset kirjesalaisuuden suojasta koskevat kaikkia tekniikan kehityksen mukanaan tuomia uusia viestintämuotoja. (HE 162/2003, 3-4.)

Sähköisen viestinnän tietosuojalaki sisältää tarkempia säännöksiä yksityisyyden suojan toteuttamisesta viestintäverkoissa ja luottamuksellisen viestin suojan turvaamisesta sähköisessä viestinnässä. Lailla pyritään varmistamaan, ettei yksityiselämän suojaa, luottamuksellisen viestin suojaa tai muita yksityisyyttä turvaavia perusoikeuksia rajoiteta sähköisessä viestinnässä tai sen toteuttamisessa ilman laissa säädettyä perustetta. (Helopuro, Perttula & Ristola 2009, 269.)

Suomen perustuslain 12 pykälän mukaan jokaisella on myös sananvapaus. Sananvapauteen sisältyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita tietoja kenenkään ennakolta estämättä. Myös viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta. (L731/1999.)

2.1 Yksityisyyden ja luottamuksellisen viestin suoja

Sähköisen viestinnän tietosuojalaki turvaa jokaiselle oikeuden luottamukselliseen viestintään ilman, että ulkopuoliset saavat tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Luottamuksellisuus tarkoittaa sitä, että viestejä ja tunnistamistietoja saa käsitellä vain erikseen laissa säädettyihin tarkoituksiin. Suojaa annetaan kaikille viesteille, jotka viestintäverkoissa liikkuvat, riippumatta vastaanottajien lukumäärästä. Useallekin henkilölle lähetetty sähköposti on luottamuksellinen, koska viestintään osallistumista on kuitenkin rajoitettu. Lain mukaan viesti ei ole kuitenkaan luottamuksellinen, jos se on saatettu yleisesti vastaanotetuksi, esimerkiksi Internetin keskustelupalstoille tai muulle selkeästi julkiselle foorumille. Viestiin liittyvät tunnistamistiedot sen sijaan taas ovat luottamuksellisia. Internet-sivustojen selailusta kertyvät tilaajien ja käyttäjien tunnistamistiedot ovat myös luottamuksellisia, koska sivustoja selailtaessa palvelimelle jää tietoja, joiden avulla nämä viestit voidaan yhdistää vastaanottavaan henkilöön. (Helopuro, Perttula & Ristola 2009, 31-33.)

Luottamuksellisen viestin suoja ulottuu myös tietokoneisiin tallennettuihin viesteihin. Suoja ei kuitenkaan ulotu sellaiseen viestiin, jonka vastaanottaja on jo saanut ja lukenut, esimerkiksi luettu tekstiviesti tai kirje ei nauti luottamuksellisen viestin suojaa koko laajuudessaan. Molemmissa tapauksissa viestin edelleen käyttöä voi rajoittaa muu suojaamisintressi, kuten yksityiselämän salaisuuden paljastamisen kriminalisointi, tai esimerkiksi sähköisen viestinnän tietosuojalain 5.1 §:n mukainen hyväksikäyttökielto. (Helopuro, Perttula & Ristola 2009, 31-33.)

Luottamuksellisen viestin suoja koskee kaikkea kohdeviestintää, riippumatta siitä, onko viestit lähetetty yleisessä verkossa, eli Internetissä vai jossain muussa viestintäverkossa. Kohdeviestinnällä tarkoitetaan viestejä, jotka joku on lähettänyt yhdelle taikka useammalle vastaanottajalle sillä tavoin, ettei viestejä ole tarkoitettu muille kuin vastaanottajille. Tämä tarkoittaa sitä, että myös yritysten ja muiden yhteisöjen sisäisissä viestintäverkoissa lähetetyt sähköpostiviestit ovat luottamuksellisia. (Helopuro, Perttula & Ristola 2009, 3.) (Nyblin 2009, 60-61.)

Perustuslakivaliokunta on katsonut, että viestin tunnistamistietojen käsittely jää luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle. Toisaalta myös tunnistamistietojen salaisuuden suojaan puuttuvan sääntelyn on täytettävä perusoikeuksien rajoittamisen yleiset edellytykset. Perustuslakivaliokunta on lisäksi todennut, että keskeisten yrityssalaisuuksien liiketaloudellinen merkitys saattaa olla yritysten kannalta niin suuri, että tällaiset yritysvarallisuuden arvon ja elinkeinotoiminnan taloudellisten edellytysten turvaamiseen liittyvät seikat ovat hyväksyttäviä ja painavia perusteita tietoverkoissa harjoitettavaan viestintään kohdistuville yksityisyyden suojan rajoituksille. (LiVM 19/2008 vp, 3.)

2.2 Työntekijän perusoikeudet

Työntekijän lähettämät ja vastaanottamat työasioita koskevat viestit eivät ole lähtökohtaisesti luottamuksellisia suhteessa työnantajaan, mutta useasti työntekijän tietoverkossa tapahtuva viestintä voi työhön selvästi liittyvien viestien ohella sisältää luottamuksellista viestintää. Perustuslain säännökset yksityisyyden suojasta ja sananvapaudesta suojaavat näitä luottamuksellisia yksityisiä viestejä oikeudettomilta puuttumisilta. Oikeus kuuluu jokaiselle, eikä sitä voida rajoittaa esimerkiksi niin sanotun vallanalaisuussuhteen perusteella, työnantajalla ei ole enää oikeutta puuttua työntekijän sähköpostiin ilman laissa säädettyä perustetta. Perustuslain 7 §:n mukaan jokaisella on oikeus henkilökohtaiseen vapauteen ja koskemattomuuteen, joihin ei voi puuttua mielivaltaisesti ja ilman laissa säädettyä perustetta. Tämä koskee myös työntekijöiden yksityiselämän suojaa tekniseltä tarkkailulta. Näissä tilanteissa voi ilmetä perusoikeuksien toteuttamisessa ristiriitatilanteita, jolloin on punnittava rajoitusten luonnetta siten, että ne ovat hyväksyttäviä ja suhteellisia, ja ettei niillä tehdä tyhjäksi perusoikeuksien ydinsisältöä. Laki yksityisyyden suojasta työelämässä turvaa samanaikaisesti sekä työntekijän luottamuksellisten viestien suojan ydinalueen, eli viestien sisällön, että työnantajan toiminnan häiriöttömään jatkumiseen liittyvät välttämättömät edut työntekijän poissa ollessa. (HE 162/2003, 4-5, 54.) (Nyblin 2009, 69-72.)

2.3 Työnantajan perusoikeudet

Perusoikeuskeskustelussa on noussut esille kysymys siitä, kuuluvatko perusoikeudet myös oikeushenkilöille, esimerkiksi osakeyhtiöille, ja voiko näin ollen työnantaja vedota perusoikeuksiin. Perusoikeuksien suoja tulee ulottaa myös oikeushenkilöön silloin, kun oikeushenkilön oikeuksiin kajoaminen johtaa välillisesti luonnollisen henkilön oikeuksiin kajoamisen. Tällöin tulee sovellettavaksi perustuslain 15 §, jonka mukaan jokaisen omaisuus on turvattu, jolloin oikeushenkilöt saavat perustuslaillista suojaa välillisesti. Käytännössä on pohdittava, minkälaisiin toimiin työnantaja on oikeutettu suojellakseen omaisuuttaan. Keskusteltaessa työnantajan perusoikeuksista ja niiden soveltamisesta käytäntöön, on usein vastakkain työntekijän yksityisyyden suoja ja työnantajan omaisuuden suoja. Jos lähdetään siitä, että kysymys on kummankin perusoikeuksista, ristiriitatilanteet on pyrittävä yleensä ratkaisemaan niin, että molempien perusoikeudet toteutuvat mahdollisimman täysimääräisinä. (Nyyssölä 2009, 21-22.)

3 LAKI YKSITYISYYDEN SUOJASTA TYÖELÄMÄSSÄ

Sähköposti on ollut keskeinen työelämän viestintäväline jo 1990-luvun puolivälistä. Tekniikan kehittyessä työelämän viestintä ei välttämättä ole enää sidoksissa työpaikan toimitiloihin tai edes työaikaan, jolloin sähköpostia yleensä luetaan ja lähetetään myös työpaikan ja työajan ulkopuolella. Työnantaja voi periaatteessa edellyttää, että hänen omistamansa laitteet ja työntekijän sähköpostiosoite muotoa etunimi.sukunimi@yritys.fi on tarkoitettu pelkästään työasioiden hoitoon, ja että niitä ei käytetä yksityiseen viestintään. Tästä huolimatta työnantaja ei ole oikeutettu lukemaan työntekijän luottamuksellisia viestejä, koska käytännössä työntekijä ei yleensä ohjaa kaikkia yksityisiä viestejään yksityiseen sähköpostiosoitteeseen, eikä sitä voida vaatiakaan. Myös työntekijälle voidaan lähettää työnantajan kiellosta huolimatta yksityisluonteisia viestejä, joita työnantaja ei ole oikeutettu lukemaan. Työntekijän luottamuksellisen viestinnän piiriin kuuluvat työntekijän muuhun kuin työtehtävien hoitoon liittyvät viestit, myös sellaiset työtehtäviin liittyvät viestit, jotka ovat tarkoitettu vain työntekijälle itselleen. Tästä johtuen rajanveto tulee tehdä aina siitä, mitkä sähköiset viestit kuuluvat työnantajalle ja mitkä viestit ovat työntekijän yksityisiä viestejä. Asiaan on ensimmäisen kerran kiinnitetty huomiota oikeudellisesti jo 1990-luvun lopulla ja 2004 voimaan tulleeseen lakiin yksityisyyden suojasta työelämässä (759/2004) on otettu säännökset työntekijän sähköpostin esille hakemiseen ja avaamiseen, jotta yksityisen viestin suoja toteutuisi mahdollisimman hyvin työelämässä. (HE 162/2003, 55-57.) (Nyblin 2009, 1-3.)

Yksityisyyden suojasta työelämässä annetun lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia oikeuksia työelämässä. Soveltamisalan piirissä ovat kaikki työsuhteet siitä riippumatta, perustuvatko ne työsopimuslakiin, merimieslakiin, kotitaloustyöntekijän työsuhteesta annettuun lakiin vai ovatko ne oppisopimussuhteita. Säännösten tavoitteena on, että työntekijän luottamuksellisten sähköpostiviestien salaisuus ei vaarantuisi, ja että työnantajalle kuuluvat, liiketoiminnan jatkumisen kannalta välttämättömät viestit voitaisiin työntekijän poissa ollessa saada työnantajan

käyttöön. Vaikka laki yksityisyyden suojasta työelämässä antaa työnantajalle mahdollisuuden työntekijän sähköpostiviestien hakemiseen ja avaamiseen ilman työntekijän suostumusta, niin sääntelyn tavoitteena pohjimmiltaan on ohjata siihen, että menetelmä perustuisi työntekijän suostumukseen. Lain (759/2004) 6 luvussa on säännökset niistä edellytyksistä, joiden täyttyessä työnantaja voi hakea esille ja avata hänelle kuuluvat työntekijän sähköpostiviestit, sekä tähän liittyvät menettelyt työntekijän ollessa estynyt hoitamaan työtehtäviään. (HE 48/2008, 1-4.) (Helopuro, Perttula & Ristola 2009, 9.)

3.1 Työnantajan huolehtimisvelvollisuudet

Yksityisyyden suojasta työelämässä annetun lain 18 §:n mukaan työnantajalla on oikeus hakea esille ja avata työntekijän käyttöön osoittamansa sähköpostin viestejä vain, jos työantaja on toteuttanut sanottujen viestien suojaksi laissa määritellyt tarpeelliset toimenpiteet. Lain 18 pykälän 1 momentin mukaan työantajalla on oikeus hakea esille tai avata työnantajan työntekijän käyttöön osoittamaan sähköpostiosoitteeseen lähetettyjä tai työntekijän tällaisesta sähköpostiosoitteesta lähettämiä sähköpostiviestejä ainoastaan silloin, jos hän on suunnitellut ja järjestänyt työntekijälle tämän nimellä lähetettyjen ja tämän lähettämien sähköpostiviestien suojan toteuttamiseksi tarpeelliset toimenpiteet. (L759/2004.) Yksityisyyden suojasta työelämässä annetun lain 18 §:n mukaan työnantaja voi tarjota työntekijöidensä käytettäväksi kolme eri toimintatapamallia, jonka mukaan työnantajan tulee menetellä työntekijän viestin suojan toteuttamiseksi. Kun työnantaja on toteuttanut vähintään yhden säännöksessä kuvatun toimintatapavaihtoehdon työntekijän sähköpostiviestien suojan toteuttamiseksi, voi hän vasta sen jälkeen hakea esille ja avata työntekijän sähköpostiviestejä. Työnantajalla ei ole huolehtimisvelvollisuutta, jos hänellä ei ole tarkoitusta hakea työntekijän nimellä saapuneita tai lähetettyjä sähköpostiviestejä. Säännös on työnantajan vähimmäisvelvoite, eikä estä työntekijää antamasta sähköpostiviestiensä käsittelyoikeutta toiselle työntekijälle huomioon ottaen mahdolliset muut salassapitosäännökset ja työnantajan määräykset. (HE 162/2003, 55-56.) (Nyblin 2009,139-142.)

Ensimmäinen toimintamalli on kuvattu yksityisyyden suojasta työelämässä annetun lain 18 §:n 1 momentin 1 kohdassa, minkä mukaan työnantaja voi tarjota työntekijälle mahdollisuutta siihen, että työntekijä itse voi käytettävän sähköpostijärjestelmän automaattisen vastaustoiminnon avulla lähettää viestin lähettäjälle ilmoituksen poissaolostaan ja sen kestosta sekä tiedon henkilöstä, joka hoitaa poissa olevalle työntekijälle kuuluvia tehtäviä. Työntekijän tulee aina itse huolehtia ennen poissaoloaan siitä, että viestin lähettäjälle lähtee tieto automaattivastauksen muodossa. Mahdollisuus automaattisen poissaolovastauksen käyttämiseen vähentää merkittävästi työnantajan tarvetta mennä työntekijän sähköpostiin poissaolon aikana. Vaikka työntekijä ei asettaisi automaattista poissaoloviestiä, ei siitä koituisi hänelle seuraamuksia, mutta työnantajan katsotaan näin toteuttaneen omalta osaltaan huolehtimisvelvollisuutensa. (HE 162/2003, 56.) (Nyblin 2009,142-143.)

Toinen työnantajan tarjoama toimintamalli on kuvattu lain 18 §:n 1 momentin 2 kohdassa, jonka mukaan työntekijä voi ohjata viestit toiselle työnantajan tähän tehtävään hyväksymälle henkilölle tai toiseen omassa käytössään olevaan työantajan hyväksymään osoitteeseen. (L759/2004.) Tämä järjestely edellyttää aina, että työnantaja hyväksyy niin järjestelyn käytön kuin henkilön ja toisen sähköpostin, mihin viestit uudelleen ohjataan. Tarvittava tietoturvan toteutuminen pystytään näin varmistamaan, kun säännös ei anna työntekijälle yksipuolista päätösoikeutta ohjata sähköpostiviestejä omaan henkilökohtaiseen sähköpostiosoitteeseensa tai henkilölle, joka ei ole työantajan hyväksymä. Tämänkin mahdollisuuden käyttäminen edellyttää aina, että työntekijä itse ennen poissaoloaan päättää käyttää sähköpostiviestien uudelleenohjausta ja asettaa sen. Työnantaja on kuitenkin täyttänyt huolehtimisvelvollisuutensa jo tarjotessaan tällaista vaihtoehtoa. (HE 162/2003, 56.)

Kolmannen toimintamallin mukaan työntekijä voi antaa suostumuksensa siihen, että työntekijän poissa ollessa tämän valitsema työnantajan tehtävään hyväksymä henkilö voi ottaa vastaan työntekijälle lähetetyt viestit sen selvittämiseksi, onko työntekijälle lähetetty sellainen viesti, joka on selvästi tarkoitettu työnantajalle työtehtävien hoitamiseksi ja josta työnantajan on toimintansa tai työtehtävien

asianmukaisen järjestämisen vuoksi välttämätöntä saada tieto. (L759/2004.) 18 §:n 1 momentin 3 kohdan mukaan toinen työntekijä voi ottaa selville työntekijän viestit noudattamatta 19 §:n 1 momentin säännöksiä. Käytännössä poissaoleva työntekijä antaa omat sähköpostitunnuksensa toiselle työntekijälle, joka voi lukea poissaolon aikana tulleet sähköpostiviestit. Suostumuksen antaminen sähköpostin lukemiseen on aina vapaaehtoista ja suostumus voidaan peruuttaa työntekijän toivomuksesta. Suostumusmenettelyltä ei edellytetä muotomääräyksiä, vaikkakin suositeltavaa on tehdä kirjallinen suostumus, jossa määriteltäisiin sen voimassaoloaika ja millaisiin poissaolotilanteisiin sitä saa käyttää. (HE 162/2003, 56.) (Nyblin 2009,149-151.)

Yksityisyyden suojasta työelämässä annetun lain 18 §:n 2 momentin mukaan edellä kuvattujen toimintatapamallien tarjoaminen työntekijöiden käytettäväksi on edellytys sille, että työnantaja voi käyttää 19 ja 20 §:ssä tarkoitettuja oikeuksiaan hakea esille ja avata työnantajalle kuuluvat viestit. (L759/2004.) Työnantajan huolehtimisvelvollisuuksia koskevien säännösten tarkoituksena on ohjata työntekijöitä ja työnantajaa luomaan kullekin työpaikalle sen toimintaan ja työntekijöiden työtehtäviin parhaiten sopivat menettelytavat. Seuraavassa kerrottujen pykälien 19 ja 20 sähköpostiviestien hakemisen ja avaamisen menettelysäännöistä voidaan kuitenkin jossain määrin poiketa työntekijän suostumuksella. (HE 162/2003, 54-55.)

3.2 Työantajalle kuuluvien sähköisten viestien esille hakeminen

Työnantajalla saattaa tulla oikeus hakea esille tai avata työntekijän sähköpostiviestejä lain 19 §:ssä säädetyissä tilanteissa, eli silloin kun työntekijä on tilapäisesti estynyt suorittamasta työtehtäviään, tai kun työntekijä on kuollut tai muuten pysyväisluonteisesti estynyt suorittamasta työtehtäviään. Näissä kahdessa tilanteessa työantaja voi rajoitetuin oikeuksin hakea esille otsikkotietojen avulla työntekijän sähköpostiosoitteeseen saapuneet tai siitä lähetetyt viestit, joista työnantajan on välttämätöntä saada tieto toimintaansa liittyvien neuvottelujen loppuun saattamiseksi, asiakkaiden palvelemiseksi tai muutoin toimintojensa turvaamiseksi. (L759/2004.)

Työnantajan on harkittava perusteellisesti sähköisten viestien esille hakemisen välttämättömyyttä. Tarpeelliseksi viestien esille hakemiseen voivat tehdä erilaiset määräaikaan sidotut tehtävät, tai esimerkiksi tilausten ja laskutusten sekä reklamointien vastaanotto, vahvistukset, seuranta ja näitä koskevat liikeneuvottelut ja muut tehtävät, joista tiedon saaminen on välttämätöntä liiketoimintojen turvaamiseksi. Jos työntekijä on tehnyt 18 §:n 1 momentissa ehdotetut toimenpiteet ennen poissaoloaan, välttämättömyyskriteerin toteutumisen arvioinnissa on otettava huomioon se, että viestin lähettäjä saa tiedon sekä asiaa hoitavan henkilön poissaolosta, että asiaa sillä hetkellä hoitavasta henkilöstä, minkä vuoksi esimerkiksi työnantajan riskit menettää tilauksia vähenevät. Työnantaja voi käyttää oikeuttaan vain tietojärjestelmän pääkäyttäjän valtuuksia käyttävän henkilön avulla. Pääkäyttäjällä on aina sähköpostijärjestelmän ylläpitohenkilönä oikeus päästä laillisesti järjestelmään, tosin hänen oikeutensa riippuvat paljon myös käytössä olevasta järjestelmästä. Pääkäyttäjät ovat myös aina tunnistettavissa. Järjestelmä voi olla myös ulkopuolelta ostettu, jolloin pääkäyttäjän valtuuksia voi käyttää palvelun tuottaja tai tämän palveluksessa oleva henkilö. Kysymyksessä ei tarvitse olla tietojärjestelmän pääkäyttäjäksi nimetty henkilö, sillä työntekijän sähköpostin lukemisen valtuudet on voitu delegoida tai antaa ne useammalle rajoitetumpana. (HE 162/2003, 57.) (Nyblin 2009, 160-162.)

Viestin lähettäjän tunnistamistiedoista tai sähköpostiviestin otsikon perusteella tulee pystyä arvioimaan kuuluuko viesti pykälän mukaisesti työnantajalle. Usein nämä tiedot ilmaisevat hyvin mihin viestin sisältö liittyy ja onko kyseessä yksityisluonteinen viesti vai ei. Samoin työnantajalla on vastaava oikeus selvittää viestin otsikkotietojen ja vastaanottajan perusteella onko työntekijä lähettänyt sellaisia sähköpostiviestejä joista työnantajan on tarpeellista tietää liiketoimintansa jatkumisen kannalta. Työnantajan oikeus hakea viestejä esille rajoittuu myös ajallisesti. Työantajan tulee ensiksi ottaa selville onko työntekijän poissa ollessa lähetetty hänelle viestejä, tai onko työntekijä välittömästi ennen poissaoloaan lähettänyt tai vastaanottanut työnantajan tietoon kuuluvia sähköpostiviestejä. Laissa tai sen esitöissä ei ole otettu kantaa siihen, kuinka pitkä aika tarkasti voi olla kyseessä, että työnantajalla on oikeus hakea viestejä esille.

Voidaan kuitenkin tulkita, että välittömästi tarkoittaa lyhyehköä aikaa ennen poissaoloa, mutta huomioitava on myös työnantajan kulloinkin tarvitseman välttämättömän tiedon käsittelyaikatauluun liittyvät näkökohdat. (HE 162/2003, 57.) (Nyblin 2009, 160-162.)

3.2.1 Viestien esille hakeminen työntekijän tilapäisesti poissa ollessa

Yksityisyyden suojasta työelämässä annetun lain 19 §:n 1 momentin mukaan työantajalla on oikeus tietojärjestelmän pääkäyttäjän valtuuksia käyttävän henkilön avulla ottaa viestin lähettäjää, vastaanottajaa tai viestin otsikkoa koskevien tietojen perusteella selville, onko työntekijälle lähetetty tämän poissa ollessa tai onko työntekijä välittömästi ennen poissaoloaan lähettänyt tai vastaanottanut työnantajalle kuuluvia viestejä, joista työnantajan on toimintaansa liittyvien neuvottelujen loppuun saattamiseksi, asiakkaiden palvelemiseksi tai toimintojensa turvaamiseksi muutoin välttämätöntä saada tieto, jos seuraavat 19 §:n 1 momentin 1-4 kohdassa säädetyt edellytykset toteutuvat. (L759/2004.)

Ensimmäinen edellytys sille että työnantaja voi hakea esille hänelle kuuluvia työntekijän sähköposteja on, että työntekijä hoitaa tehtäviä itsenäisesti työnantajan lukuun eikä työnantajan käytössä ole järjestelmää, jonka avulla työntekijän hoitamat asiat ja niiden käsittelyvaiheet kirjataan tai saadaan muutoin selville. (L759/2004.) 19 §:n 1 momentissa edellytetty välttämättömyyskriteeri ei toteudu, jos työnantaja voi muutoin saada viestiin liittyvästä asiasta selvän. Työn itsenäisyys merkitsee sitä, että viestiin liittyvää asiaa eivät hoida samanaikaisesti muut henkilöt, joilla voi olla asiaan liittyvät tiedot ilman, että työnantajan on välttämätöntä hakea esille poissaolevan työntekijän sähköpostista viestejä. (HE 162/2003, 58.)

Toisen edellytyksen mukaan työntekijän tehtävien ja vireillä olevien asioiden vuoksi on oltava ilmeistä, että työantajalle kuuluvia viestejä on lähetetty tai vastaanotettu. Kolmantena edellytyksenä on työntekijän tilapäinen estyminen suorittamasta työtehtäviään eikä työnantajalle kuuluvia viestejä siitä huolimatta, että työnantaja on huolehtinut 18 §:ssä tarkoitetuista velvollisuuksistaan, voida saada työnantajan käyttöön. (L759/2004.) Työntekijän tilapäistä estyneisyyttä ei

ole tarkemmin määritelty laissa, mutta lyhyt, vain muutaman tunnin työstä poissaolo ei tee viestin selvittämistä usein välttämättömäksi, toisaalta taas käytännön työelämässä voi hyvinkin tulla tilanteita, jolloin vaaditaan työnantajan nopeaa reagoimista viesteihin. (HE 162/2003, 58.) (Nyblin 2009, 163-165.)

Neljännen edellytyksen mukaan työnantajalla on oikeus hakea esille työntekijän viestit myös jos työntekijän suostumusta ei voida saada kohtuullisessa ajassa ja asian selvittäminen ei kestä viivytystä. (L759/2004.) Tämä tarkoittaa sitä, että työnantajan on tarjottava työntekijälle konkreettisin toimenpitein mahdollisuus antaa suostumuksensa sähköpostiviestiensä hakemiseen. Työnantaja voi esimerkiksi yrittää tavoittaa työntekijää puhelimitse ja pyytää häneltä suostumus hakea esille sähköpostiviestit. Näin työntekijä saa myös tiedon siitä, että hänen sähköpostinsa avaamista harkitaan. Jos työntekijän suostumusta ei saada kohtuullisessa ajassa ja asian selvittäminen ei kestä viivytystä, niin työnantaja saa kuitenkin hakea viestit esille ilman työntekijän suostumusta. (HE 162/2003, 58.) .) (Nyblin 2009, 165-166.)

Edellä mainitut asiat sääntelevät työnantajan oikeuksia hakea esille työntekijän sähköpostiviestejä hänen ollessa tilapäisesti poissa. Työelämässä tulee kuitenkin myös tilanteita jolloin työntekijä kuolee tai on muuten estynyt hoitamaan työtehtäviään pysyväisluonteisesti. Pysyväisluonteisuutta on arvioitava jokaisen yksittäistapauksen kohdalla erikseen, mutta esimerkiksi työsuhteen päättyessä työntekijän poissaolo on pysyväisluonteista. Tällöin työnantajan toiminnan turvaamisen kannalta 19 pykälän 2 momentti antaa työnantajalle 1 momenttia laajemmat oikeudet hakea esille viestejä. Tosin työntekijälle, jonka työsuhde on purettu tai irtisanottu, on työnantajan tarjottava työntekijälle mahdollisuus itse poistaa henkilökohtaiset viestinsä, jotta hänen luottamuksellisen viestin suoja toteutuisi. (HE 162/2003, 58-59.)

3.2.2 Viestien esille hakeminen työntekijän pysyväisluonteisesti poissaollessa

Yksityisyyden suojasta työelämässä annetun lain 19 §:n 2 momentin mukaan jos työntekijä on kuollut taikka jos hän on pysyväisluonteisesti estynyt suorittamasta työtehtäviään eikä hänen suostumustaan voida saada, on työnantajalla oikeus

ottaa viestin lähettäjää tai vastaanottajaa, taikka viestin otsikkoa koskevien tietojen perusteella selville työnantajalle kuuluvat viestit jollei työntekijän hoitamien asioiden selville saaminen ja työnantajan toiminnan turvaaminen ole muilla keinoilla mahdollista. Säännöksessä todetaan myös, että ennen kuin työnantaja voi hakea viestit esille, on 19 §:n 1 momentin 1 ja 2 kohdassa säädettyjen erityisten edellytyksien viestien hakemiseen täytyttävä. Ensimmäinen edellytys on, että työntekijän on hoidettava tehtäviä itsenäisesti työnantajan lukuun, eikä työnantajan käytössä ole järjestelmää, jonka avulla työntekijän hoitamat asiat ja niiden käsittelyvaiheet kirjataan tai saadaan muutoin selville. Toinen edellytys on, että työntekijän tehtävien ja vireillä olevien asioiden vuoksi on ilmeistä, että työnantajille kuuluvia viestejä on lähetetty tai vastaanotettu. (L759/2004.)

Yksityisyyden suojasta työelämässä annetun lain 19 §:n 3 momentin mukaan jos viestin esille hakeminen ei johda viestin avaamiseen, siitä on laadittava siihen osallistuneiden henkilöiden allekirjoittama selvitys, josta ilmenee, miksi viestiä on haettu, hakemisen ajankohta ja sen suorittajat. Selvitys on ilman aiheetonta viivytystä toimitettava työntekijälle, jollei 2 momentista muuta johdu. Viestin lähettäjä- tai vastaanottajatietoja taikka otsikkotietoja ei saa käsitellä laajemmin kuin on välttämätöntä viestin esille hakemisen tarkoituksen vuoksi, eivätkä tietoja käsittelevät henkilöt saa ilmaista näitä tietoja sivulliselle työsuhteen aikana eikä sen päättymisen jälkeen. (L759/2004.) Selvityksen voi toimittaa työntekijälle esimerkiksi sähköpostilla, tai sen voi jättää työntekijän työpöydälle odottamaan hänen paluutaan. Selvitystä ei tarvitse toimittaa jos työntekijä on pysyväisluonteisesti estynyt hoitamasta työtehtäviään. Säännöksen tarkoitus on lisätä avoimuutta työpaikalla. (HE 162/2003, 59.)

3.3 Työnantajalle kuuluvien sähköisten viestien avaaminen

Yksityisyyden suojasta työelämässä annetun lain 20 §:n mukaan työnantaja saa myös avata työnantajalle kuuluvat viestit, jos on ilmeistä, että viestin otsikkotiedon, lähettäjän tai vastaanottajan perusteella viesti on tarkoitettu työnantajalle ja tiedon saaminen siitä on välttämätöntä liiketoiminnan jatkumisen kannalta, eikä viestin lähettäjään tai vastaanottajaan saada yhteyttä viestin sisällön

selvittämiseksi, eikä viestiä voida toimittaa toiseen osoitteeseen. Viestien avaamisen on tapahduttava tietojärjestelmän pääkäyttäjän valtuuksia käyttävän henkilön avulla toisen henkilön läsnä ollessa. Viestin esille hakemisesta ja avaamisesta on laadittava siihen osallistuneiden henkilöiden allekirjoittama selvitys. Siitä on käytävä ilmi, mikä viesti on avattu, miksi viesti on avattu, avaamisen ajankohta, avaamisen suorittajat sekä kenelle avatun viestin sisällöstä on annettu tieto. Selvitys on ilman aiheetonta viivytystä toimitettava työntekijälle, jollei työntekijä ole kuollut tai muuten pysyväisluonteisesti estynyt suorittamasta työtehtäviään. Avattu viesti on säilytettävä, eikä sen sisältöä ja lähettäjätietoja saa käsitellä laajemmin kuin on tarpeen viestin avaamisen tarkoituksen vuoksi, eivätkä tietoa käsittelevät henkilöt saa ilmaista viestin sisältöä sivulliselle työsuhteen aikana, eikä sen päättymisen jälkeen. (L759/2004.)

Työntekijän nimellä lähetetyn sähköpostiviestin voi siis avata, vain jos on aivan ilmeistä, että viesti kuuluu työnantajalle. Tällöin työnantajalle kuuluvien sähköisten viestien esille hakemisen edellytykset ovat täytyttävä pykälän 19 mukaan ja säännöksen mukaiset menettelyt on oltava käyty läpi. Kuitenkaan pelkästään sähköpostiviestin kuuluminen työnantajalle ei riitä antamaan oikeutta avaamaan viestiä. Kyseisen viestin sisältö pitää myös olla työnantajalle välttämätön tieto toimintaansa liittyvien neuvottelujen loppuunsaattamiseksi, asiakkaiden palvelemiseksi ja toimintojensa turvaamiseksi. Vielä tässä vaiheessa, jos se on mahdollista, pitää pyrkiä saamaan viestin lähettäjään tai vastaanottajaan yhteys, jotta viestin sisältö saataisiin tietoon muutoin kun avaamalla. Esimerkiksi kun työnantaja on saanut tiedot viestin lähettäjästä, voi työnantaja pyytää lähettäjää lähettämään viestin uudelleen työnantajan antamaan toiseen osoitteeseen, josta se on luettavissa. (HE 162/2003, 54-55.) (Helopuro, Perttula & Ristola 2009, 59-60.)

Jos työntekijä on tilapäisesti estynyt suorittamasta työtehtäviään, työntekijä on voinut antaa suostumuksensa muuhun menettelyyn sähköpostiviestiensä lukemiseksi. Jos työnantaja on hyväksynyt työntekijän ehdottaman muun menettelytavan, ei työnantajan tarvitse noudattaa 20 §:ssä säädettyä velvollisuutta. Työntekijä voi esimerkiksi antaa suostumuksensa sille, että toinen työnantajan

tähän tehtävään hyväksymä henkilö, tavallisimmin toinen työntekijä, tai pienemmissä yrityksissä sen johtaja, voi tarkistaa työntekijälle tulleen sähköpostin työntekijän antamien käyttäjätunnus ja salasanojen avulla sekä avata ja lukea työnantajalle kuuluvat viestit. Viestinnän luottamuksellisuus ei vaikuta viestinnän osapuolten välisiin suhteisiin laajemmin. Muu menettely mahdollistaa muun muassa sen, että toinen työntekijä voi lukea suostumuksen antaneen työntekijän viestejä ja hoitaa niin sovittaessa ja toimivaltansa rajoissa myös sähköpostiviesteissä tarkoitettuja työtehtäviä noudattamatta tässä luvussa tarkoitettuja menettelytapoja. Jos työntekijä ei noudata työnantajan tarjoamia menettelytapoja, työnantaja voisi siinä tapauksessa käyttää 19 ja 20 §:ssä tarkoitettuja oikeuksiaan. Jos työntekijä menettelee työnantajan tarjoamien vaihtoehtojen mukaisesti, supistaa se taas työnantajan oikeutta käyttää oikeuksiaan hakea ja avata työntekijän sähköpostiviestit. (HE 162/2003, 54-55.) (Helopuro, Perttula & Ristola 2009, 59-60.)

4 SÄHKÖISEN VIESTINNÄN TIETOSUOJALAIN KÄSITTEET

Sähköisen viestinnän tietosuojalain sääntely kohdistuu uuteen ja monimuotoiseen teknis-sosiaaliseen toimintaympäristöön, jossa samankaltaisia toimintoja toteutetaan hyvin erilaisin teknisin välinein ja sovelluksin. Nämä välineet ja sovellukset kehittyvät poikkeuksellisen nopeasti, joten valtaosa sähköisen viestinnän tietosuojalaissa käytetyistä käsitteistä ja lähestymistavoista tulee suoraan toisista laista. Esimerkiksi vuonna 2004 kumotusta yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta annetusta laista, viestintämarkkinalaista, henkilötietolaista ja tietoyhteiskunnan palvelujen tarjoamisesta annetusta laista. Sähköisen viestinnän tietosuojalain 2 pykälässä on selitetty ne käsitteet, jotka tulee ymmärtää tulkittaessa lakia. Seuraavassa otan esille vain tämän työn kannalta keskeisimmät käsitteet. (Helopuro, Perttula & Ristola 2009, 13.)

1) *viestillä* tarkoitetaan viestintäverkossa osapuolten välillä tai vapaasti valikoituville vastaanottajille välitettävää puhelua, sähköpostiviestiä, tekstiviestiä, puheviestiä ja muuta vastaavaa sanomaa. (L516/2004.) Osapuolilla tarkoitetaan yksittäistä tiettyä henkilöä, esimerkiksi työntekijää ja asiakasta, kun taas vapaasti valikoitu vastaanottaja voi periaatteessa olla kuka tahansa. Sähköisen viestinnän tietosuojalain viestin määritelmä sisältää laissa sananvapauden käyttämisestä joukkoviestinnässä tarkoitetun verkkoviestin, eli mielipiteen tai muun viestin, kuten televisio-ohjelmia ja radio-ohjelmia sekä kaikkia Internetin yleisölle avoimia sivuja tai tiedostoja. Viestin määritelmä on tärkeä koko sähköisen viestinnän tietosuojalain kannalta ja erityisesti arvioitaessa viestin sisältöön kajoamisen edellytyksiä ja toteuttamistapoja. Viestin käsite rakentuu lyhyesti sanottuna sanomasta ja sen teknisestä kuljetusalustasta. Teknisiä kuljetusalustoja ovat sähköisten tiedostojen lisäksi kirjepaperi ja kirjekuori, minkä avulla viesti saadaan vastaanottajalle. (Helopuro, Perttula & Ristola 2009, 14-15.)

2) *viestintäverkolla* tarkoitetaan toisiinsa liitetyistä johtimista ja laitteista muodostuvaa fyysistä järjestelmää, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella

tavalla. Määritelmä kattaa yleiset viestintäverkot ja muut viestintäverkot. Yleisiä viestintäverkkoja ovat esimerkiksi matkaviestinverkot, kiinteät puhelinverkot, joukkoviestintäverkot ja Internet, joita tarjotaan etukäteen rajaamattomalle käyttäjäpiirille. Muita viestintäverkoja ovat esimerkiksi asunto-osakeyhtiöiden, yritysten ja julkisyhteisöjen sekä yksityisten henkilöiden viestintäverkot, niin sanotut intranetit, jotka on kytketty yleisiin viestintäverkkoihin. (L516/2004.) (Helopuro, Perttula & Ristola 2009, 16.)

3) *teleyrityksellä* tarkoitetaan viestintämarkkinalain (393/2003) 2 §:n 17 kohdan mukaista verkkoyritystä tai 19 kohdan mukaista palveluyritystä. (L516/2004.) Teleyrityksiä ovat esimerkiksi TeliaSonera Oyj ja Elisa Oyj. Teleyritykset tarjoavat verkko- ja viestintäpalveluja yleisissä viestintäverkoissa etukäteen rajoittamattomalle joukolle. (Helopuro, Perttula & Ristola 2009, 17.)

4) *verkkopalvelu ja viestintäpalvelu.* Verkkopalvelulla tarkoitetaan teleyrityksen toteuttamaa viestintäverkon tarjoamista käytettäväksi viestien siirtoon, jakeluun tai tarjolla pitoon etukäteen rajoittamattomalle käyttäjäpiirille. (L516/2004.) Verkkopalveluun kuuluu tyypillisesti verkon hallinta, ylläpito ja kehittäminen. Verkkopalvelun tarjoaja huolehtii viestintäverkkojen yhtyeenliittämisestä toisten verkkojen kanssa, esimerkiksi matkaviestinverkkojen osalta se solmii kansainväliset verkkovierailusopimukset, joiden mukaan hinnoitellaan ulkomaanpuhelut, tekstiviestit ja datasiirrot. Viestintäpalvelulla tarkoitetaan sellaista teleyrityksen toteuttamaa viestien siirtämistä, jakelemista tai tarjolla pitämistä viestintäverkossa, jota tarjotaan etukäteen rajoittamattomalle käyttäjäpiirille. (L516/2004.) Viestintäpalvelun tarjoaja huolehtii tyypillisesti matkaviestinliittymän antamisesta käyttäjälle, liittymän avaamisesta ja sulkemisesta. Määritelmä vastaa sisällöllisesti viestintämarkkinalain viestintäpalvelun määritelmää. Käytännössä verkkopalveluun sisältyy automaattisesti viestintäpalvelu, eli kun asiakas tilaa Internetliittymän, saa hän oikeuden käyttää verkkoa, eli verkkopalvelun ja siihen kuuluvat datasiirrot, eli viestintäpalvelut. (Helopuro, Perttula & Ristola 2009, 17.)

5) tietoyhteiskunnan palveluja ovat yhteisötilaajan omaan viestintäverkkoon liitetyt palvelut, ja palvelut joita käytetään yhteisötilaajan viestintäverkon kautta ja

joiden käytön yhteisötilaaja maksaa. Tietoyhteiskunnan palvelut toimitetaan ilman, että osapuolet ovat yhtä aikaa läsnä, sähköisesti, palvelun vastaanottajan henkilökohtaisesta pyynnöstä tapahtuvana tiedonsiirtona ja tavallisesti vastiketta vastaan. (HE 48/2008, 20.)

5) *lisäarvopalvelulla* tarkoitetaan palvelua, joka perustuu tunnistamistietojen tai paikkatietojen käsittelyyn muuta tarkoitusta kuin verkkopalvelun tai viestintäpalvelun toteuttamista varten. (L516/2004.) Lisäarvopalvelut voivat olla esimerkiksi käyttäjän päätelaitteen sijaintiin perustuvaa mainontaa ja reittineuvontaa sekä liikennetiedotuksia, säätiedotuksia taikka matkailutietoa. Määritelmän mukaisia lisäarvopalveluita eivät ole esimerkiksi verkkopankkipalvelut, hallinnon sähköiset asiointipalvelut tai muut vastaavat palvelut, joissa palvelun sisältö ei pääosin perustu tunnistamistietojen tai paikkatietojen käsittelyyn. Nämä palvelut ovat tietoyhteiskunnan palveluja. (Helopuro, Perttula & Ristola 2009, 18.)

6) *tunnistamistiedolla* tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. (L516/2004.) Tunnistamistietoihin voi kuulua tietoja, jotka viittaavat viestinnän reititykseen, kestoon, ajankohtaan tai siirrettävän tiedon määrään, käytettyyn protokollaan, lähettäjän tai vastaanottajan päätelaitteen sijaintiin tietyn tukiaseman alueella, lähettävään tai vastaanottavaan verkkoon ja yhteyden alkuun, loppuun tai kestoon. Tiedot voivat myös koskea muotoa, jossa viesti välitetään verkossa. (HE 48/2008, 3.) Tilaaja, johon tunnistamistieto voidaan yhdistää, voi olla luonnollinen- tai oikeushenkilö. Tunnistamistiedon käsitteellä tarkoitetaan viestintäverkoissa käsiteltävien tietojen lisäksi viestintäverkoissa olevia tietoja, joita käsitellään tiettyihin tarkoituksiin eli viestien siirtämiseen, jakeluun ja tarjolla pitämiseen. Tunnistamistiedon käsitteen rajaus tarkoituksenmukaisella tavalla on tärkeää, koska liian tarkkarajainen rajaus saattaisi mahdollistaa sääntelyn vaivattoman kiertämisen ja aiheuttaa sen, että lakia jouduttaisiin teknologian kehityksen myötä muuttamaan hyvinkin pian. Erilaisten käyttötarkoitusten monimuotoisuudesta johtuen on mahdotonta määritellä konkreettisin esimerkein ja kattavasti tunnistamistiedon käsitteen

yhteydessä täsmällisiä rajapintoja palveluihin, verkkoihin ja päätelaitteisiin. Sääntelyssä on välttämätöntä pyrkiä teknologianeutraaliuteen, eikä esimerkiksi yksittäisellä teknisellä toteuttamistavalla voi olla olennaista merkitystä tunnistamistietojen määritelmän kannalta. Käytännössä tunnistamistiedosta käy ilmi, kuka puhuu puhelimessa kenenkin kanssa, ketkä lähettelevät toisilleen sähköposti- ja tekstiviestejä, ja millä Internet-sivustolla kukin surffaa. (Helopuro, Perttula & Ristola 2009, 18-19.)

7) *tilaajalla* tarkoitetaan oikeushenkilöä tai luonnollista henkilöä, joka on tehnyt sopimuksen viestintäpalvelun tai lisäarvopalvelun toimittamisesta. (L516/2004.) Olennaista määritelmän kannalta on, että tilaajan ja palvelun tarjoajan välillä on sopimussuhde, mikä voi edellyttää säännöllistä tai kertaluonteista maksua tarjotusta palvelusta. Se voi myös olla vastikkeeton. (Helopuro, Perttula & Ristola 2009, 20.)

8) *Yhteisötilaajalla* tarkoitetaan viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä tai yhteisöä, joka käsittelee viestintäverkossaan käyttäjien luottamuksellisia viestejä, tunnistamistietoja tai paikkatietoja. (L516/2004.) Yhteisötilaajan käsite kattaa elinkeinonharjoittajat, osuuskunnat, osakeyhtiöt, yhdistykset, yliopistot ja valtion virastot. Lain soveltamisessa yhteisötilaajan koolla ei ole merkitystä, vaan on katsottu, että kaikki yhteisötilaajat ovat oikeutettuja samanlaiseen kohteluun ja velvoitettu samanlaisilla velvollisuuksilla. Yhteisötilaaja on teleyrityksen tapaan sivullinen suhteessa viestinnän osapuoliin. Yhteisötilaaja tilaa viestintäpalvelun tai lisäarvopalvelun käyttäjiensä, esimerkiksi työntekijöidensä, käytettäväksi. Tätä tarkoitusta varten yhteisötilaaja hallinnoi samalla järjestelmää, jossa käsitellään käyttäjien luottamuksellisia tunnistamistietoja ja paikkatietoja erilaisin palvelimin ja päätelaittein. Silloin kun elinkeinonharjoittaja on viestinnän osapuolena, ei sovelleta yhteisötilaajaa koskevaa sääntelyä, vaan viestinnän osapuolen oikeuksia ja velvollisuuksia koskevaa sääntelyä, koska kyseisten roolien käsittelysäännöt poikkeavat olennaisesti toisistaan. (Helopuro, Perttula & Ristola 2009, 21-22, 99-100.) (LiVM 19/2008 vp, 4.)

9) *käyttäjällä* tarkoitetaan luonnollista henkilöä, joka käyttää viestintäpalvelua tai lisäarvopalvelua olematta välttämättä tämän palvelun tilaaja. (L516/2004.) Olennaista käyttäjän määritelmän kannalta on, että käyttäjä on aina luonnollinen henkilö, kun tilaaja sen sijaan voi olla oikeushenkilö tai luonnollinen henkilö. (Helopuro, Perttula & Ristola 2009, 23.)

10) *tietoturvalla* tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. (L516/2004.) Näitä tietoturvatoimia ovat esimerkiksi tietoliikenteen häirinnän valvonta ja estäminen, laitteille ja järjestelmiin pääsyn valvonta, tietojen ja järjestelmien luvattoman käytön esto, käsittelytapahtumien kirjaaminen, tietoliikenteen alkuperävalvonta ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen ja tietojen sekä järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta, kuten viruksilta ja muilta haittaohjelmilta. Tietoturvan huolehtimisvelvoitteen laiminlyönti voi johtaa rikosoikeudelliseen vastuuseen. Yhteisötilaajan on ylläpidettävä kirjallisia ohjeita siitä, miten tietoturvavaatimukset toteutetaan, oman tietoturvan tasoa seurattava säännöllisesti, varmistettava tietoturvavaatimusten toteuttaminen käytettäessä alihankkijoita ja suojattava laitteet ja tiedostot luvatonta pääsyä ja käyttöä vastaan. Yhteisötilaajan on myös pidettävä rekisteriä kunkin järjestelmän osalta siitä, kenellä on järjestelmän käyttäjätunnuksia, ja mitä oikeuksia milläkin käyttäjätunnuksella on, ja valvotaan tietojen, asiakirjojen, viestintäverkkojen, laitteistojen, palvelujen ja tiedostojen tietoturvaan vaikuttavia tapahtumia niin, että tieturvan kannalta merkittävät tapahtumat havaitaan. Yhteisötilaajan on myös käytettävä sellaisia laitteistoja, tietojärjestelmiä ja ohjelmistoja, joista aiheutuva tietoturvauhka on vähäinen, sekä järjestetään toiminnan kannalta tärkeiden ohjelmistojen varmuuskopiointi ja turvallinen säilytys. Tietoturvatoimenpiteistä lisää sille otsikoidussa luvussa. (Helopuro, Perttula & Ristola 2009, 23-24.)

11) *käsittelyllä* tarkoitetaan keräämistä, tallentamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita vastaavia toimenpiteitä. (L516/2004.) Käsitteeseen sisältyy myös tietojen luovuttaminen, mutta vain niille tahoille joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa. Käsittelyllä ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. (Helopuro, Perttula & Ristola 2009, 25.)

12) *palveluyrityksellä* tarkoitetaan viestintämarkkinalain 2 §:n 19 kohdassa tarkoitettua yritystä. (L516/2004.) Viestintämarkkinalain mukaan palveluyrityksellä tarkoitetaan yritystä, joka siirtää viestejä hallussaan olevassa tai verkkoyritykseltä käyttöönsä samassa viestintäverkossa taikka jakelee tai pitää tarjolla viestejä joukkoviestintäverkossa. (Helopuro, Perttula & Ristola 2009, 25.)

4.1 Luvaton käyttö

Sähköisen viestinnän tietosuojalaissa ei ole määritelty mitä luvattomalla käytöllä tarkoitetaan, mutta katson oleelliseksi selventää käsitettä. Luvaton käyttö ja sen merkittävyys yhteisötilaajalle määrittyvät yhteisötilaajan omasta toiminnasta käsin. Lain kirjoittamisen kannalta on mahdotonta luetella tyhjentävästi ne tilanteet, jolloin yhteisötilaajan viestintäverkkoa käytetään luvattomasti, ja se milloin merkittävyyden kynnys ylittyy kenenkin toiminnassa. Luvaton käyttö yrityksissä tapahtuu yleensä tietoyhteiskunnan palvelun, jonka yhteisötilaaja tavallisesti maksaa, luvattomana käyttönä. Tietoyhteiskunnan palvelulla tarkoitetaan palvelua, joka toimitetaan ilman, että osapuolet ovat yhtä aikaa läsnä, sähköisesti, palvelun vastaanottajan henkilökohtaisesta pyynnöstä tapahtuvana tiedonsiirtona ja tavallisesti vastiketta vastaan. Esimerkkinä maksullisen tietoyhteiskunnan luvattomasta käytöstä voisi olla se, että yrityksen henkilökunnan koon mukaan hinnoiteltua palvelua jaettaisiin luvatta ulkopuolisten käyttöön. Tällöin yritys joutuisi vastaamaan hankkimansa käyttöoikeuden ylittävästä käytöstä. (Helopuro, Perttula & Ristola 2009, 100-101.)

5 LIIKESALAISUUKSIEN SUOJA

Sähköisen viestinnän tietosuojalain uudistuksen keskeisin tavoite oli antaa keinot yhteisötilaajalle selvittää oikeudeton yrityssalaisuuden paljastaminen. Siksi on tärkeää ymmärtää, mitä yrityssalaisuuden käsitteellä sähköisen viestinnän tietosuojalaissa tarkoitetaan. Hallituksen esityksessä 48/2008 todetaan, että yrityssalaisuuden käsitteen tulee vastata rikoslain 30 luvun 11 §:n yrityssalaisuuden määritelmää. Rikoslain pykälän mukaan yrityssalaisuudella tarkoitetaan liike- tai ammattisalaisuutta, taikka muuta vastaavaa elinkeinotoimintaa koskevaa tietoa, jonka elinkeinonharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinonharjoittajalle, joka on uskonut tiedon hänelle. Käsite kattaa sellaisetkin teknologista ja muuta kehittämistyötä koskevat tiedot, joissa ei vielä ole kysymys esimerkiksi patentoitavista tuotteista. (HE 48/2008, 20.) (L39/1889.)

Liikesalaisuuksien suojasta säädetään myös sopimattomasta menettelystä elinkeinotoiminnassa annetun lain (1061/1978) 4 §:ssä. Pykälän mukaan kukaan ei saa oikeudettomasti hankkia tai yrittää hankkia tietoa liikesalaisuudesta eikä käyttää tai ilmaista näin hankkimaansa tietoa. Joka elinkeinonharjoittajan palveluksessa ollessaan on saanut tiedon liikesalaisuudesta, ei saa sitä palvelusaikanaan oikeudettomasti käyttää eikä ilmaista hankkiakseen itselleen tai toiselle etua tai toista vahingoittaakseen. Joka elinkeinonharjoittajan puolesta tehtävää suorittaessaan on saanut tiedon liikesalaisuudesta tai jolle työn tai tehtävän suorittamista varten taikka muuten liiketarkoituksessa on uskottu tekninen esikuva tai tekninen ohje, ei saa sitä oikeudettomasti käyttää eikä ilmaista. Joka on saanut toiselta tiedon liikesalaisuudesta, teknisestä esikuvasta tai teknisestä ohjeesta tietäen, että tämä on hankkinut tai ilmaissut tiedon oikeudettomasti, ei saa sitä käyttää eikä ilmaista. (L1061/1978.)

Liikenne- ja viestintäministeriön lausunnon mukaan on tärkeää erotella toisistaan yrityssalaisuuksien vuotamisen ja luvattoman käytön selvittäminen. Kaikkia yhteisötilaajia ei koske yrityssalaisuuksien vuotamisen selvittämistä koskevat säännökset, koska kaikilla yhteisötilaajilla ei aina ole suojattavia

yrityssalaisuuksia. Toisaalta luvattoman käytön selvittäminen voi olla hyvin pienelle yhteisötilaajalle hyvin merkittävää. Sähköisen viestinnän tietosuojalakia tulkittaessa on päädytty soveltamaan yrityssalaisuuden käsitettä koska siihen liittyy kiinteästi elinkeinonharjoittajan oma salassapitotahto ja koska säännökset vaikuttavat yksityisten osapuolten välillä. (LiVM 19/2008 vp, 5.) (HE 48/2008, 21.)

5.1 Yritysvakoilu, yrityssalaisuuden rikkominen ja -väärinkäyttö

Oikeudettoman yrityssalaisuuden paljastumisen tilanteissa tulevat sovellettavaksi myös rikoslain 30 luvun 4 – 6 §:t yritysvakoilusta, yrityssalaisuuden rikkomisesta ja yrityssalaisuuden väärinkäytöstä. Yritysvakoilusta on säädetty rikoslain 4 §:ssä seuraavasti: Joka oikeudettomasti hankkii tiedon toiselle kuuluvasta yrityssalaisuudesta 1) tunkeutumalla ulkopuolisilta suljettuun paikkaan taikka ulkopuolisilta suojattuun tietojärjestelmään, 2) hankkimalla haltuunsa tai jäljentämällä asiakirjan tai muun tallenteen taikka muulla siihen rinnastettavalla tavalla tai 3) käyttämällä teknistä erikoislaitetta tarkoituksin oikeudettomasti ilmaista tällainen salaisuus tai oikeudettomasti käyttää sitä, on tuomittava, jollei teosta ole muualla laissa säädetty ankarampaa rangaistusta, yritysvakoilusta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Yritys on rangaistava. (L39/1889.)

Yrityssalaisuuden rikkomisesta on säädetty rikoslain 5 §:ssä seuraavasti: Joka hankkiakseen itselleen tai toiselle taloudellista hyötyä tai toista vahingoittaakseen oikeudettomasti ilmaisee toiselle kuuluvan yrityssalaisuuden tai oikeudettomasti käyttää tällaista yrityssalaisuutta, jonka hän on saanut tietoonsa 1) ollessaan toisen palveluksessa, 2) toimiessaan yhteisön tai säätiön hallintoneuvoston tai hallituksen jäsenenä, toimitusjohtajana, tilintarkastajana tai selvitysmiehenä taikka niihin rinnastettavassa tehtävässä, 3) suorittaessaan tehtävää toisen puolesta tai muuten luottamuksellisessa liikesuhteessa tai 4) yrityksen saneerausmenettelyn yhteydessä, on tuomittava, jollei teosta ole muualla laissa säädetty ankarampaa rangaistusta, yrityssalaisuuden rikkomisesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Rikoslain pykälä yrityssalaisuuden rikkomisesta ei koske

tekoa, johon henkilö on ryhtynyt kahden vuoden kuluttua palvelusaikansa päättymisestä. Yritys on rangaistava. (L39/1889.)

Yrityssalaisuuden väärinkäytöstä on säädetty rikoslain 6 §:ssä seuraavasti: Joka oikeudettomasti 1) käyttää rikoslaissa rangaistavaksi säädetyllä teolla tietoon saatua tai ilmaistua toiselle kuuluvaa yrityssalaisuutta elinkeinotoiminnassa taikka 2) hankkiakseen itselleen tai toiselle taloudellista hyötyä ilmaisee tällaisen salaisuuden, on tuomittava yrityssalaisuuden väärinkäytöstä sakkoon tai vankeuteen enintään kahdeksi vuodeksi. (L39/1889.)

5.2 Yrityssalaisuuksien suojaaminen

Yrityksen henkilöstö on suurin uhka elinkeinonharjoittajalle yrityssalaisuuksien paljastumisessa. Työntekijät tarvitsevat salassa pidettäviä tietoja suorittaakseen työtehtäviään ja suurin osa työnantajan yrityssalaisuuksista myös syntyy työntekijöiden työsuoritusten pohjalta. Liiketoiminnan hyvä tulos edellyttää useasti myös tiedon jakamista työyhteisössä enemmän kuin tietoon pääsemisen rajoittamista. Useissa yrityssalaisuuden suojaa koskevissa tuomioistuinkäsittelyissä yrityssalaisuuden vuoto on tapahtunut työsuhteen loppuvaiheessa tai sen päätyttyä, jolloin keskeistä on erottaa toisistaan yrityssalaisuudeksi luokiteltava tieto, sellaisesta tiedosta mistä on työsuhteen kestäessä tullut osa työntekijän omaa ammattitietoa tai taitoa. Aikaisemmin lainsäädäntö on lähtenyt siitä, että salassapitovelvollisuus ja yrityssalaisuuksien oikeudeton hyväksikäyttäminen on rajoittunut vain työsuhteen kestoaikaan. Vuonna 2003 rikoslain 30 luvun 5 pykälään tehty muutos säätää teon rangaistavaksi vielä kahden vuoden ajan työsuhteen päättymisen jälkeen. Perusteena muutokselle on pidetty tarvetta puuttua sellaisiin moitittaviin tekoihin, joilla aikaisemmalle työnantajalle kuuluvia yrityssalaisuuksia suoraan siirretään toisen työnantajan tai työntekijän perustaman uuden yrityksen toimintaan. Rikoslain uudistuksen aikana otettiin kantaa myös siihen, mikä tekijä erottaa yrityssalaisuuden työntekijän omasta ammattitaidosta ja –tiedosta. Tultiin siihen tulkintalopputulokseen, että sähköisesti tallennettu tieto on lähtökohtaisesti työnantajalle kuuluvaa yrityssalaisuutta ja muistin varassa kulkeva tieto työntekijän omaa ammattitaitoa. (Defensor Legis.)

Rikoslain mukaisessa yrityssalaisuuden määritelmän esitöissä on pidetty tärkeänä sitä, että salassa pidettävän tiedon tulee olla tosiasiallisesti suojattu ulkopuolisilta. Tiedon tulee olla suojattu teknisillä ja fyysisillä suojaamistoimenpiteillä, esimerkiksi salassa pidettävät tiedostot tulee säilyttää tietojärjestelmissä salasanojen takana ja salassa pidettävät asiakirjat kassakaapissa tai muulla tavalla estettävä ulkopuolisten pääsy tietoihin. Yritys voi suojata salassa pidettäviä tietojaan myös yrityksissä suoritettavien valvontatoimenpiteiden avulla, esimerkiksi kameravalvonnan ja kulunvalvonnan avulla, tietojärjestelmiin kirjautumisten ja tietojärjestelmissä toteutettujen käsittelytoimenpiteiden valvomisella ja valvomalla millaisia tietokoneohjelmia työntekijöiden käyttöön annetuille työasemille on tallennettu. Työantaja voi suojata yrityssalaisuuksiaan myös työntekijän kanssa tehtävien salassapitosopimusten avulla ja ohjeistamalla henkilöstöä salassa pidettävästä tiedosta. Jos suojattavana on huomattavan arvokas liike- tai ammattisalaisuus, tai muu tähän rinnastettava erittäin merkittävä yksityinen etu, voi työantaja turvallisuusselvityksistä annetun lain (177/2002) mukaan hankkia selvityksen työntekijän luotettavuudesta. Tietoa ei voida luokitella yrityssalaisuudeksi jos edellä mainittuja tietoturvallisuustoimenpiteitä ei ole elinkeinonharjoittajan puolesta asianmukaisesti suunniteltu etukäteen ja toteutettu käytännössä. (HE 66/1988, 92.) (HE 48/2008, 20.)

6 SÄHKÖISEN VIESTINNÄN TIETOSUOJALAKI

Sähköisen viestinnän tietosuojalaki on luotu Euroopan parlamentin ja neuvoston vuonna 2002 antaman sähköisen viestinnän tietosuojadirektiivin (2002/58/EY) pohjalta. Kansallisesti direktiivi pantiin täytäntöön syyskuussa 2004 sähköisen viestinnän tietosuojalailla (516/2004). Sähköisen viestinnän tietosuojalaissa on säädetty sähköisten viestien välittäjien velvollisuuksista, joilla taataan julkisen vallan velvollisuus turvata sananvapaus, viestinnän luottamuksellisuus ja viestintäverkkojen käyttäjien yksityisyys. Lain tarkoitus on myös edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisten viestinnän palvelujen tasapainoista kehittymistä. (L516/2004.) (HE 48/2008, 4,11.)

Vuoden 2004 sähköisen viestinnän tietosuojalain alkuperäiset säännökset olivat tietyiltä osin puutteelliset. Ne eivät antanut yhteisötilaajalle tarvittavia oikeuksia käsitellä tunnistamistietoja tietoverkossa tapahtuvien väärinkäytösten ja yrityssalaisuuksien luvattomien paljastamisien estämiseksi. Myös sähköisen viestinnän tietosuojalain 20 §:n tietoturvasäännös oli puutteellinen, se ei mahdollistanut tarkoituksenmukaista suojautumista ammattimaisesti toteutetulta sähköpostihyökkäysliikenteeltä. Säännösten soveltaminen käytännössä osoittautui myös ongelmalliseksi. Erityisesti lain 13 § tunnistamistietojen käsittelystä oli niin suppea, ettei se taannut yhteisötilaajille riittäviä toimintamahdollisuuksia selvittää ja kerätä väärinkäytöksistä näyttöä itse ja saattaa poliisille esitutkintaan viestintäverkkoihinsa kohdistuneita väärinkäytöksiä. Tästä johtuen Liikenne- ja viestintäministeriö valmisteli esiin tulleiden tarpeiden perusteella Eduskunnalle ehdotuksen lain muuttamisesta vuonna 2009. Lakimuutoksella viestinnän luottamuksellisuuden takaava sääntely ulotettiin koskemaan teleyritysten lisäksi myös yhteisötilaajia eli muita tavallisia yrityksiä, organisaatioita ja yhteisöjä. Tehdyt muutokset turvaavat myös paremmin yritysten toimintaa ja liikesalaisuuksien salassa pysymistä. Lakia haluttiin selkeyttää, ja parantaa erityisesti yhteisötilaajien oikeutta käsitellä tunnistamistietoja. Lain voimaantulon jälkeen muutokset ovat helpottaneet yhteisötilaajien maksullisten verkkopalvelujen ja viestintäverkon luvattoman käytön tai ohjeiden vastaisen käytön selvittämistä. Lakimuutoksella annettiin myös yhteisötilaajalle tietyin

edellytyksin oikeus käsitellä tunnistamistietoja estääkseen ja selvittääkseen yrityssalaisuuksien paljastumista. Ehdotus on parantanut myös teleyritysten, lisäarvopalvelun tarjoajien ja yhteisötilaajien mahdollisuutta huolehtia viestintäverkon ja –palvelujen tietoturvasta. Tunnistamistietojen käsittelyoikeudet eivät kuitenkaan oikeuta yhteisötilaajia saamaan tietoa viestien sisällöstä. (HE 48/2008 kansilehti, 3-5, 11-12.) (Helopuro, Perttula & Ristola 2009, 22.)

Yhteisötilaajien tunnistamistietojen käsittelyoikeuden laajentamisen perusteena voidaan pitää perustuslakivaliokunnan kantaa siitä, että keskeisten yrityssalaisuuksien liiketaloudellinen merkitys saattaa olla niin suuri, että tällaiset yrityssalaisuuden arvon ja elinkeinotoiminnan taloudellisten edellytysten turvaamiseen liittyvät seikat ovat hyväksyttäviä ja painavia perusteita tietoverkoissa harjoitettavaan viestintään kohdistuville rajoituksille. Vaikka sähköisen viestinnän tietosuojalaissa on laajennettu yhteisötilaajien oikeutta käsitellä tunnistamistietoja, perustuslakivaliokunta pitää kuitenkin keskeisenä sitä, että uudistuksilla ei heikennetä työntekijän työsuhdeturvaa. Perusteluissa lain muuttamisesta otettiin kantaa siihen, että myös yhteisötilaajalle kertyy teknisiin ja sähköpostijärjestelmiin käyttäjien luottamuksellisia tunnistamistietoja ja viestejä. Teleyrityksille ja yhteisötilaajille kertyy viestintäpalveluja toteuttaessa ja käyttäessä täysin samanlaisia tietoja, siten yhteisötilaajan mahdollisuudet väärinkäytöksiin ja tarve yhtäläisiin käsittelyoikeuksiin ja velvollisuuksiin eivät poikkea teleyrityksen mahdollisuuksista ja tarpeesta. Yhteisötilaajan toiminnan mahdollistamiseksi sekä yksityisyyden, että luottamuksellisen viestin suojan turvaamiseksi yhteisötilaajalle on ollut välttämätöntä asettaa teleyrityksiä vastaavat tietoturvavelvoitteet sekä tunnistamistietojen ja paikkatietojen käsittelysäännöt. (LiVM 19/2008 vp, 3-7.) (Helopuro, Perttula & Ristola 2009, 21-22, 99-100.)

6.1 Sähköisen viestinnän soveltamisala

Sähköisen viestinnän tietosuojalain pääsäännön mukaan lakia sovelletaan yleisien viestintäverkojen palveluihin, eli kaikkeen viestintää, tiedonsiirtoihin ja muihin palveluihin mitä Internetissä tarjotaan. Internet-sivustojen selailu kuuluu lain soveltamisalaan, koska yleisölle avoimia sivuja selailtaessa palvelimelle tai

viestintäverkon kautta päätelaitteelle jää yleensä tietoja, joiden avulla viestit voidaan yhdistää ne vastaanottavaan luonnolliseen henkilöön tai oikeushenkilöön. Lisäksi lakia sovelletaan suoramarkkinointiin yleisissä viestintäverkoissa sekä tilaajaluettelopalveluihin ja numerotiedotuspalveluihin. Lakia ei sovelleta sisäisiin ja muihin rajoitetuille käyttäjäpiireille tarkoitettuihin viestintäverkkoihin, esimerkiksi yrityksen intranettiin, ellei näitä verkkoja ole liitetty yleiseen viestintäverkkoon. Yleisiin viestintäverkkoihin liitetyissä ja yhteisötilaajien hallinnoimissa sisäverkoissa sovelletaan yksityisyyden ja luottamuksellisen viestin suojaamiseksi vastaavia tietoturvaa koskevia perusvelvoitteita ja käsittelysääntöjä kuin teleyritysten toteuttamaan tunnistamis- sekä paikkatietojen käsittelyyn. Sähköisen viestinnän tietosuojalakia sovelletaan esimerkiksi tilanteissa, joissa sähköpostiviestejä luetaan yrityksen intranetin sähköpostipalvelimelta, josta on yhteys yleisiin viestintäverkkoihin, riippumatta siitä, kulkevatko viestit yleisen viestintäverkon kautta vai ainoastaan sisäisessä viestintäverkossa. Henkilötietojen käsittelyyn sovelletaan henkilötietolain (523/1999) säännöksiä, jollei sähköisen viestinnän tietosuojalaista muuta johdu ja työnantajan ja työntekijän välisessä suhteessa sovelletaan yksityisyyden suojasta työelämässä annettua lakia (477/2001). (L516/2004.) (Helopuro, Perttula & Ristola 2009, 3,10.)

Tietosuojalakia ei sovelleta joukkoviestintäverkossa välitettävään viestiin, jos viestiä ei voida yksittäisessä tapauksessa yhdistää sitä vastaanottavaan tilaajaan tai käyttäjään. Sähköisen viestinnän tietosuojalakia ei myöskään sovelleta viranomaistoimintaan viranomaisverkossa tai muussa yleiseen järjestykseen ja turvallisuuteen, maanpuolustukseen, pelastustehtäviin, väestönsuojeluun tai maaliikenteen, meriliikenteen, raideliikenteen taikka ilmaliikenteen turvallisuuteen liittyvien tarpeiden vuoksi rakennetussa viestintäverkossa. Lakia ei myöskään sovelleta, jos rahanpesun estämisestä tai selvittämisestä annetusta laista (68/1998) muuta johtuu. (L516/2004.)

6.2 Vaitiolovelvollisuus ja hyväksikäyttökielto

Sähköisen viestinnän tietosuojalain 5 §:n mukaan henkilöllä joka on ottanut vastaan tai muutoin saanut tiedon luottamuksellisesta viestistä tai

tunnistamistiedosta, jota ei ole hänelle tarkoitettu on vaitiolovelvollisuus ja hyväksikäyttökielto, ellei viestinnän toinen osapuoli anna viestien ilmaisemiseen tai käyttämiseen suostumustaan. (L516/2004.) Kyse on tilanteista, jolloin luottamuksellinen viesti on lähetetty erehdyksessä sellaiselle henkilölle jolle se ei ole tarkoitettu. Tällöin vastaanottajalle syntyy vaitiolovelvollisuus ja hyväksikäyttökielto viestistä, vaikka hän ei itse olekaan aktiivisesti toimien hankkinut viestiä. Sähköisessä viestinnässä käytettävät tekniikat ja palvelut tekevät helposti mahdolliseksi viestinnän ohjautumisen muulle kuin vastaanottajalle vähäisenkin teknisen vian tai virheen vuoksi. Säännöksen tarkoituksena ei ole estää esimerkiksi sähköpostin jälleenlähettämistä oikealle vastaanottajalle, jos viesti vahingossa tulee väärään osoitteeseen, vaan kyseessä on nimenomaisesti kielto käyttää tällaista viestiä ja tunnistamistietoja hyötymistarkoituksessa. Viestin voi siis lähettää sille henkilölle jolle viesti kuuluu, tai takaisin sen lähettäjälle. (Helopuro, Perttula & Ristola 2009, 37-39.)

7 TUNNISTAMISTIETOJEN KÄSITTELYSÄÄNNÖT

Yhteisötilaajan tunnistamistietojen käsittelyoikeuksia väärinkäytöstapauksissa koskeva lakimuutos, paremmin tunnettuna Lex Nokia tai urkintalaki sai valtavasti kielteistä huomiota osakseen syksyllä ja keväällä 2008-2009. Se oli yleisen mielipiteen mukaan perustuslain vastainen, vaikka perustuslakivaliokunta antoi lakimuutoksesta yksipuolisesti puoltavan lausunnon. Negatiivisen keskustelun taustalla saattoi pohjimmiltaan olla se, että tietoyhteiskunnan edellyttämä lainsäädäntö otti varsinaisia ensiaskeleitaan ja siitä käyty julkinen keskustelu heijasti pelkoa uusien ilmiöiden käsittelyä kohtaan. Perinteisesti yrityksiin on saapunut kirjepostia, mikä saattaa sisältää juuri samat tiedot kuin sähköpostiviestikin. Kirje haetaan julkisista lokeroista, joista on helppo nähdä muiden työntekijöiden tunnistamistietoja, esimerkiksi kenelle kirje on lähetetty, mitä se koskee ja usein myös lähettäjä, eikä tästä asiasta ole milloinkaan väitetty, että se olisi perustuslain vastaista tai loukkaisi yksityisyyttä. Yrityksillä on laajat mahdollisuudet estää paperi- tai muussa fyysisessä muodossa oleviin aineistoihin kohdistuvat väärinkäytökset, esimerkiksi kulunvalvonnalla tai lukitsemalla tilojaan. Vastaavia oikeuksia ei kuitenkaan ole samojen aineistojen osalta, jos ne ovat sähköisessä muodossa. Vuoden 2009 väärinkäytössäännöksellä haluttiin varmistaa yritysten toimintaedellytyksiä kattamalla se lainsäädännöllinen aukko, joka etenkin yrityssalaisuuksien suojassa sähköisessä viestintäympäristössä oli auki. (Helopuro, Perttula & Ristola 2009, 96-97.)

7.1 Yleiset käsittelysäännöt

Sähköisen viestinnän tietosuojalain 3 luvun 8 pykälässä on säädetty tunnistamistietojen yleisistä käsittelysäännöistä, joiden mukaan viestin lähettäjä tai se, jolle viesti on tarkoitettu, voi käsitellä omia viestejään ja niihin liittyviä tunnistamistietoja. Omiin viesteihin kuuluvat sekä lähetetyt, että vastaanotetut viestit. Vastaanotettuja viestejä, ei kuitenkaan saa käsitellä, jos viesti on vahingossa lähetetty väärälle vastaanottajalle, eli viestiä ei ole tarkoitettu hänelle. Tällöin vastaanottajaa koskee vaitiolovelvollisuus viestistä ja viestin hyväksikäyttökielto. Tapauskohtaisesti viestinnän osapuoli voi olla joko

luonnollinen henkilö tai oikeushenkilö. Mitä viestin käsittelyyn tulee, niin sähköisen viestinnän tietosuojalaki ei juuri rajoita viestinnän osapuolten oikeutta hävittää, tallentaa tai muutoin käsitellä viestejään. Muu laki voi sen sijaan tapauskohtaisesti rajata käsittelyä, esimerkiksi kunnialoukkausta koskevat rikoslain säädökset. (L516/2004.) (Helopuro, Perttula & Ristola 2009, 70-72.)

Yleisesti luottamuksellisia viestejä ja tunnistamistietoja saa käsitellä lisäksi jos siihen saa suostumuksen viestin lähettäjältä tai siltä, kenelle viesti on tarkoitettu. Suostumuksen tulisi olla tarpeeksi yksilöity, eikä kovinkaan yleisluonteinen, esimerkiksi ”kaikki viestit tästä lähtien”. Muihin tarkoituksiin tunnistamistietoja ei saa käsitellä, ellei siihen anneta erityistä oikeutta jossakin toisessa laissa. (L516/2004.) (Helopuro, Perttula & Ristola 2009, 48.)

Perustuslakivaliokunta on painottanut, että yhteisötilaajan oikeus käsitellä tunnistamistietoja on sähköisen viestinnän tietosuojalain 8 §:n 3 momentin vaatimusten vuoksi sallittua ainoastaan sen tarkoituksen vaatimassa laajuudessa, eikä käsittelyllä voida rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Toisin sanoen väärinkäytökset on ensisijaisesti pyrittävä selvittämään muiden kuin luottamuksellista viestintää koskevien tunnistamistietojen avulla. Käsittelyn laajuudella tarkoitetaan käsittelyn rajausta varsinaisen käyttötarkoituksen osalta myös ajallisesti. Käsittely on siten sallittua esimerkiksi ainoastaan siinä laajuudessa, että yhteisötilaaja pystyy riittävällä tavalla yksilöimään poliisille osoitettavan rikosilmoituksen tai tutkintapyynnön. Tunnistamistietoja ei myöskään saa luovuttaa muille tahoille, kuin niille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa. Käsittelyn jälkeen viestit ja tunnistamistiedot on hävitettävä tai tehtävä sellaisiksi ettei niitä voi yhdistää tilaajaan tai käyttäjään. Näin tulkittuna ja sovellettuna sääntely ei valiokunnan mielestä tältä osin muodostu ongelmalliseksi oikeasuhtaisuudesta johtuvien vaatimusten kannalta. (LiVM 19/2008 vp, 4.) (L516/2004.) (Helopuro, Perttula & Ristola 2009, 73-74,102.)

7.2 Yhteisötilaajan käsittelyoikeus väärinkäytöstapauksissa

Väärinkäytösten ja oikeudettomien yrityssalaisuuksien paljastumisia on ensisijaisesti pyrittävä selvittämään muiden kuin luottamuksellista viestintää koskevien tunnistamistietojen avulla. Näiden selvittämisessä ovat käytettävissä tietohallinnolliset keinot, kuten käyttäjälokien tarkastaminen, pääsyä rajoittaviin järjestelmiin kirjautuvien tietojen tarkastaminen sekä järjestelmien teknisessä ylläpidossa kerätyt tiedot. Tiedoista selviää, kuka on tallentanut mitäkin tietoja, missä muodossa, koska ja mille tallenteelle. Sähköisen viestinnän tietosuojalaki ei aseta rajoituksia edellä mainittujen tietojen käsittelylle. Lakimuutos antaa yhteisötilaajalla oikeudet käsitellä tunnistamistietoja maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvattoman tai ohjeen vastaisen käytön taikka yrityssalaisuuksien paljastamisen ehkäisemiseksi ja selvittämiseksi siten kuin sähköisen viestinnän tietosuojalain 13 b – k §:ssä säädetään. Lakiuudistuksen myötä tulee silti muistaa, että tunnistamistietojen käsittelyyn on oikeutettua ryhtyä vain viimesijaisena keinona. (HE 48/2008, 19-20.) (Helopuro, Perttula & Ristola 2009, 103.) (L516/2004.)

Jotta yhteisötilaaja voisi käsitellä tunnistamistietoja väärinkäytöstapauksissa, on sähköisen viestinnän tietosuojalain 13 a §:n mukaan tunnistamistietojen käsittelyoikeuden yleiset ja erityiset edellytykset täytyttävä. Erityisiä edellytyksiä tunnistamistietojen käsittelylle ovat muun muassa asianmukaisesti toteutetut tietoturvatoimenpiteet. Myös sähköisen viestinnän tietosuojalain välttämättömyysedellytyksen vuoksi yhteisötilaaja ei voi seurata tavanomaisiin viesteihin liittyviä tunnistamistietoja. Välttämättömyysedellytyksellä tarkoitetaan sitä, että väärinkäytökset on ensisijaisesti pyrittävä selvittämään muiden kuin luottamuksellista viestintää koskevien tunnistamistietojen avulla. Jos tunnistamistietojen käsittely on välttämätöntä väärinkäytöksen selvittämiseksi, on käsiteltäväksi tulevien tunnistamistietojen piiri rajattava aina tapauskohtaisesti käytettävissä olevien muiden tietojen perusteella. Esimerkiksi työantaja asemassa oleva yhteisötilaaja ei voi seurata viestintäverkon tai viestintäpalvelun käyttöä työajan seuraamiseksi, tai selvittääkseen onko käyttäjä ollut yhteydessä henkilöstön edustajaan, työsuojeluviranomaisiin tai työterveyshuoltoon. Säännös

ei oikeuta käsittelemään tunnistamistietoja ajallisesti yhtään laajemmin kuin käsillä olevan tapauksen selvittämisen kannalta on välttämätöntä. (HE 48/2008, 20.) (Helopuro, Perttula & Ristola 2009, 102.)

Sähköisen viestinnän tietosuojalain 13 a §:n 2 momentin mukaan viestintäverkon tai viestintäpalvelun luvatonta käyttöä voi olla laitteen, ohjelman, tai palvelun asentaminen yhteisötilaajan viestintäverkkoon, sivulliselle oikeudettomasti pääsyn avaaminen yhteisötilaajan viestintäverkkoon tai viestintäpalveluun, taikka muu näihin rinnastuva viestintäverkon tai viestintäpalvelun käyttö, jos se on yhteisötilaajan käytöstä laadittujen asianmukaisten ohjeiden vastaista. Muulla luvattomalla käytöllä tarkoitetaan esimerkiksi yrityksen henkilökunnan käyttöön tarkoitetun maksullisen palvelun jakamista luvatta ulkopuoliseen käyttöön, jolloin yritys joutuisi vastaamaan hankkimansa käyttöoikeuden ylittävästä käytöstä. (L516/2004.) (HE 48/2008, 20.)

Sähköisen viestinnän tietosuojalain säännökset yhteisötilaajan oikeudesta käsitellä tunnistamistietoja eivät koske kiinteän tai matkapuhelinverkon puhelinpalvelujen tunnistamistietoja. Eli yhteisötilaaja ei saa säännöksen mukaan käsitellä työntekijöidensä puheluihin, tekstiviesteihin, sähköpostiviesteihin, puheviesteihin tai muihin vastaaviin sanomiin liittyviä tietoja. (L516/2004.) (HE 48/2008, 21.)

Sähköisen viestinnän tietosuojalain 8 §:n 3 momentin mukaan tunnistamistiedot on käsittelyn jälkeen hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään. Sähköisen viestinnän tietosuojalain 13 k pykälä kuitenkin oikeuttaa yhteisötilaajan asianomistajana luovuttamaan tunnistamistietojen käsittelystä saadut tiedot poliisille rikosilmoituksen tai tutkintapyynnön yhteydessä lain 8 §:n 3 momentin sitä estämättä. (L156/2004.) Säännös on tarpeellinen, jotta yhteisötilaaja voi saattaa rikoksena selvitettäväksi sellaiset tapaukset, joissa voi olla kysymys rangaistavaksi säädetystä teosta, kuten luvattomasta käytöstä tai yrityssalaisuuteen kohdistuvasta rikoksesta. (Helopuro, Perttula & Ristola 2009, 134-135.)

8 YHTEISÖTILAAJAN HUOLEHTIMISVELVOLLISUUDET

Yhteisötilaajan huolehtimisvelvollisuus tarkoittaa niitä toimia, jotka yhteisötilaajan on tullut hoitaa ennen kuin se voi ryhtyä käsittelemään tunnistamistietoja. Yhteisötilaajan ensisijaisena keinona estää väärinkäytökset viestintäverkossaan ja -palvelussaan on huolehtia ennakoivista toimenpiteestä, eli huolehtia asianmukaisesta tietoturvasta ja verkkojen ja palvelujen käyttäjien ohjeistuksesta ja niiden noudattamisen automaattisesti tapahtuvasta seurannasta. Yhteisötilaajan tulee erityisesti huolehtia siitä, ettei viestintäverkkoon tai –palveluihin ole pääsyä sellaisilla henkilöillä, joille niitä ei ole tarkoitettu. Sähköisen viestinnän tietosuojalain 13 b § sääntelee yhteisötilaajan huolehtimisvelvollisuudesta ennen tunnistamistietojen käsittelyn aloittamista viestintäverkon ja -palvelujen luvattoman tai ohjeen vastaisen käytön ehkäisemiseksi ja selvittämiseksi. Pykälä sääntelee myös ne ennakoivat toimenpiteet, jotka yhteisötilaajan tulee tehdä ennen kuin se ryhtyy käsittelemään tunnistamistietoja yrityssalaisuuksien paljastamisen ehkäisemiseksi. (HE 48/2008, 21.)

8.1 Ennaltaehkäisevät toimenpiteet

Sähköisen viestinnän tietosuojalain 13 b §:n mukaan yhteisötilaajan on pitänyt tehdä seuraavat toimenpiteet ennen tunnistamistietojen käsittelyyn ryhtymistä:

Yhteisötilaajan on ensin laitettava tietoturvansa kuntoon, eli rajoitettava viestintäverkkonsa ja viestintäpalvelunsa käyttöä ja rajoitettava niihin pääsyä asiankuulumattomilta henkilöiltä. Yrityssalaisuuksien suojaamisessa yhteisötilaajan on samoin tosiasiallisesti suojattava yrityssalaisuudet sellaisilta ulkopuolisilta tahoilta, joilla ei ole tarvetta käsitellä näitä tietoja, esimerkiksi käyttäjätunnuksin ja salasanoin. Yhteisötilaajan tulee myös ryhtyä muihin asianmukaisiin tietoturvallisuustoimenpiteisiin viestintäverkkonsa ja viestintäpalvelunsa käytön ja yrityssalaisuuksien suojaamiseksi ja varmistettava tietoturvan riittävä taso. Yrityksessä on myös hyvä olla määriteltynä ne valikoidut henkilöt ja tahot, joilla on pääsy yrityssalaisuuksiin. Jos verkkoa tai palveluita käytetään kuitenkin luvatta asianmukaisesta käyttäjähallinnosta ja muista

tietoturvatoimista huolimatta, on yhteisötilaajalla oikeus ryhtyä tunnistamistietojen käsittelyyn asian selvittämiseksi. (L516/2004.) (HE 48/2008, 21-22.)

Toiseksi yhteisötilaajan on määriteltävä minkälaisia viestejä sen viestintäverkon kautta saa välittää ja hakea, sekä miten sen viestintäverkkoa ja viestintäpalvelua saa muutoin käyttää ja minkälaisiin kohdeosoitteisiin viestintää ei saa harjoittaa. Viestintäverkon ja viestintäpalvelun käyttäjällä tulee olla tieto siitä, miten yhteisötilaajan verkkoa saa käyttää, jotta tunnistamistietoja saa ryhtyä käyttämään. Kun verkon käyttäjä noudattaa edellä mainittuja vaatimuksia, voi hän välttyä omien viestiensä tunnistamistietojen tulemisesta yhteisötilaajan tietoon. Yhteisötilaajan on jo ennakoivissa toimenpiteissä otettava huomioon, että luvattoman käytön selvittäminen ei ole mahdollista, ellei merkittävyys-kynnys ylity. Tämä tarkoittaa sitä, että tavanomainen viesti voidaan kyllä periaatteessa ohjeilla kieltää, mutta käytännössä viestintää ei voida tarkkailla. Tällä tavoin esimerkiksi tavallinen Internet-surffailu ja tavanomainen viestien lähettäminen ei voi tulla tarkkailun kohteeksi. (L516/2004.) (HE 48/2008, 21.) (Helopuro, Perttula & Ristola 2009, 104-105.)

Yhteisötilaajan on ennen tunnistamistietojen käsittelyn aloittamista yrityssalaisuuksien paljastamisen ehkäisemiseksi myös määriteltävä, miten yrityssalaisuuksia saa viestintäverkossa siirtää, luovuttaa tai muutoin käsitellä ja minkälaisiin kohdeosoitteisiin yrityssalaisuuksia käsittelemään oikeutetut henkilöt eivät ole oikeutettuja lähettämään viestejä. Suojattavan tiedon kanssa tekemisissä olevien henkilöiden, on oltava selvillä siitä, mitä tietoja pidetään organisaatiossa yrityssalaisuuksina. Yhteisötilaajan erityisten tietojen suojaamistoimenpiteet, rajoitettu pääsy ja käsittelysäännöt tiedon käyttäjille määrittelevät osaltaan, mitä yhteisötilaaja pitää keskeisinä yrityssalaisuuksinaan. Ohjeessa on myös määriteltävä, mikäli yhteisötilaaja haluaa kieltää liikennöinnin kokonaan tietyn tyyppisiin kohdeosoitteisiin. (L516/2004.) (HE 48/2008, 22.) (LiVM 19/2008 vp, 5.)

Sähköisen viestinnän tietosuojalain 13 b §:n 3 momentin mukaan yhteisötilaajan on edellä mainittujen väärinkäytösten ehkäisemiseksi annettava lisäksi kirjalliset

ohjeet viestintäverkon tai viestintäpalvelun käyttäjälle. Kielletyt kohdeosoitteet voidaan määritellä kohtuullisen yleisellä tasolla, mutta kirjallisista ohjeista tulisi olla helposti ymmärrettävissä, mikä on väärinkäyttöä. (L516/2004.) (HE 48/2008, 22.)

8.2 Yhteisötilaajan suunnittelu- ja yhteistoimintavelvoite väärinkäytöstapauksissa

Sähköisen viestinnän tietosuojalain 13 c §:ssä säädetään tarkemmin niistä edellytyksistä, joita yhteisötilaajan tulee täyttää joko suunnittelemalla tai tiedottamalla ennen kuin se voi ottaa uudet käsittelymenettelyt käyttöönsä. 13 c §:n 1 momentin mukaan tunnistamistietojen käsittelyn yhtenä edellytyksenä on, että yhteisötilaajan on ennen 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. (L516/2004.) Käyttäjien oikeusturvan kannalta on tärkeää, että he tietävät ketkä yhteisötilaajan puolesta tunnistamistietoja voivat käsitellä, ja että vain sellaiset henkilöt käsittelevät tunnistamistietoja, joilla on riittävä ammattitaito siihen. Siten esimerkiksi yrityksen johto ei välttämättä ole se taho, joka tunnistamistietoja käsittelee. Jos yhteisötilaaja hankkii kyseisen palvelun ulkopuoliselta taholta, on riittävää, että on määritelty palveluntarjoajan kyseiset tehtävät tai toiminnot. Jos tunnistamistietojen käsittelyyn osallistuu ulkopuolisen yrityksen palvelussa oleva henkilö, tulisi yhteisötilaajan varmistua ennen toimenpiteisiin ryhtymistä siitä, että tunnistamistietojen käsittelyn edellytykset täyttyvät. Tunnistamistietoja käsittelevillä henkilöillä on lisäksi erityinen vaitiolovelvollisuus käsittelemistään tiedoista, ja jos vaitiolovelvollisuutta rikkoo, voi rangaistus olla enimmillään jopa kolme vuotta vankeutta. (HE 48/2008, 22.) (Helopuro, Perttula & Ristola 2009, 108.)

Jos yhteisötilaaja on yhteistoimintalainsäädännön piiriin kuuluva työnantaja, on hänen tiedotettava tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteista ja käytännöistä yhteistoiminnasta yrityksissä annetun lain (334/2007)

tarkoittamassa yhteistoimintamenettelyssä, ja tiedotettava tunnistamistietojen käsittelystä tekemänsä päätökset työntekijöille tai heidän edustajilleen, siten kuin yksityisyyden suojasta työelämässä annetun lain (759/2004) 21 §:ssä säädetään. (L516/2004.)

Yhteistoiminta käsittää henkilöstön kuulemisen ja henkilöstölle tiedottamisen. Tämän takia, ennen kuin työnantaja ottaa käyttöön tunnistamistietojen käsittelyn aloittamisen tuomia menettelyjä tai muutoksia, on niiden perusteista, tavoitteista, tarkoituksesta ja vaikutuksista neuvoteltava niiden työntekijöiden edustajien kanssa joita asia koskee. Yhteistoimintamenettelyn piiriin kuuluvat viestintäverkon luvattomaan käyttöön tai viestintäpalvelun ohjeen vastaiseen käyttöön liittyvät keskeiset kysymykset, kuten viestintäverkon käytöstä laaditut ohjeet, automaattisen haun toimintaperiaatteet ja millä perusteella viestintäverkon luvattoman tai ohjeen vastaisen käytön katsotaan aiheuttavan työnantajalle merkittävää haittaa ja vahinkoa. Yhteisötilaajan tulee vastaavasti selvittää myös ne seikat ja perusteet, joiden perusteella automaattinen tai manuaalinen käsittely on mahdollista yrityssalaisuuksien paljastamisen selvittämiseksi. Toiseksi yhteistoimintamenettelyssä on käsiteltävä ne 1 momentissa tarkoitetut tehtävät, joissa tunnistamistietoja voidaan käsitellä. (Helopuro, Perttula & Ristola 2009, 109-111.) (HE 48/2008, 22-23.)

Työnantajan on myös noudatettava, mitä yksityisyyden suojasta työelämässä annetun lain 21 §:ssä säädetään. Säännöksen mukaan työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan tarkoitus, käyttöönotto ja siinä käytettävät menetelmät sekä sähköpostin ja muun tietoverkon käyttö kuuluvat edellä mainitussa yhteistoimintalainsäädännössä tarkoitettujen yhteistoimintamenettelyjen piiriin. Yhteistoiminta- ja kuulemismenettelyn jälkeen työnantajan on määriteltävä työntekijöihin kohdistuvan teknisin menetelmin toteutetun valvonnan käyttötarkoitus ja siinä käytettävät menetelmät sekä tiedotettava työntekijöille valvonnan tarkoituksesta, käyttöönotosta ja siinä käytettävistä menetelmistä sekä sähköpostin ja tietoverkon käytöstä. Yhteisötilaajiin sovelletaan myös yksityisyyden suojasta työelämässä annetun lain säännöksiä työnantajalle kuuluvien sähköpostiviestien hakemisesta ja

avaamisesta. Ilmoitus tunnistamistietojen käsittelystä voi olla kertaluontoinen ja se voidaan tehdä joko silloin kun käyttöoikeus viestintäverkon tai viestintäpalvelun käyttöön annetaan käyttäjälle tai jos se ei ole mahdollista, niin muulla sopivalla tavalla. Lainsäätäjä on tällä säännöksellä halunnut tuoda esiin sen, että aito vuorovaikutteinen pelisäännöistä sopiminen edistää jokaisen yrityksen työilmapiiriä ja siten myös sen kannattavuutta. (Helopuro, Perttula & Ristola 2009, 109-111.) (HE 48/2008, 22-23.)

Jos yhteisötilaaja on työnantaja joka ei kuulu yhteistoimintalainsäädännön piiriin, on hänen kuultava työntekijöitä sähköisen viestinnän tietosuojalain 13 c §:n 2 momentin 1 kohdassa tarkoitetuista seikoista ja tiedotettava niistä työntekijöille siten kuin yksityisyyden suojasta työelämässä annetun lain 21 §:n 1 ja 2 momentissa säädetään. (L516/2004.)

Yhteisötilaajan huolehtimisvelvollisuuksiin kuuluvat myös niin sanotut jälkikäteiset toimet, mitkä yhteisötilaajan on mietittävä etukäteen valmiiksi. Näitä ovat selvityksen antaminen käyttäjälle, jonka tietoja on manuaalisesti käsitelty sekä vuosittainen raportti manuaalisesta käsittelystä tietosuojavaltuutetulle ja työntekijöiden edustajalle. (Helopuro, Perttula & Ristola 2009, 112.)

9 LUVATTOMAN KÄYTÖN SELVITTÄMINEN

Jos yhteisötilaaja on tehnyt kaikki ennakolliset toimenpiteet, saa hän sähköisen viestinnän tietosuojalain 13 d §:n mukaan käsitellä maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun tunnistamistietoja luvattoman käytön selvittämiseksi. Luvatonta käyttöä tulee ryhtyä selvittämään ensisijaisesti automaattisen hakukoneen avulla, mikä etsii poikkeamia viestintäverkon käytössä. Kun hakukone on löytänyt tietyn tai tietyt poikkeamat, voidaan seuraavaksi luvatonta käyttöä selvittää käsittelemällä tunnistamistietoja manuaalisesti. (L516/2004.)

9.1 Yhteisötilaajan tunnistamistietojen käsittelyoikeus

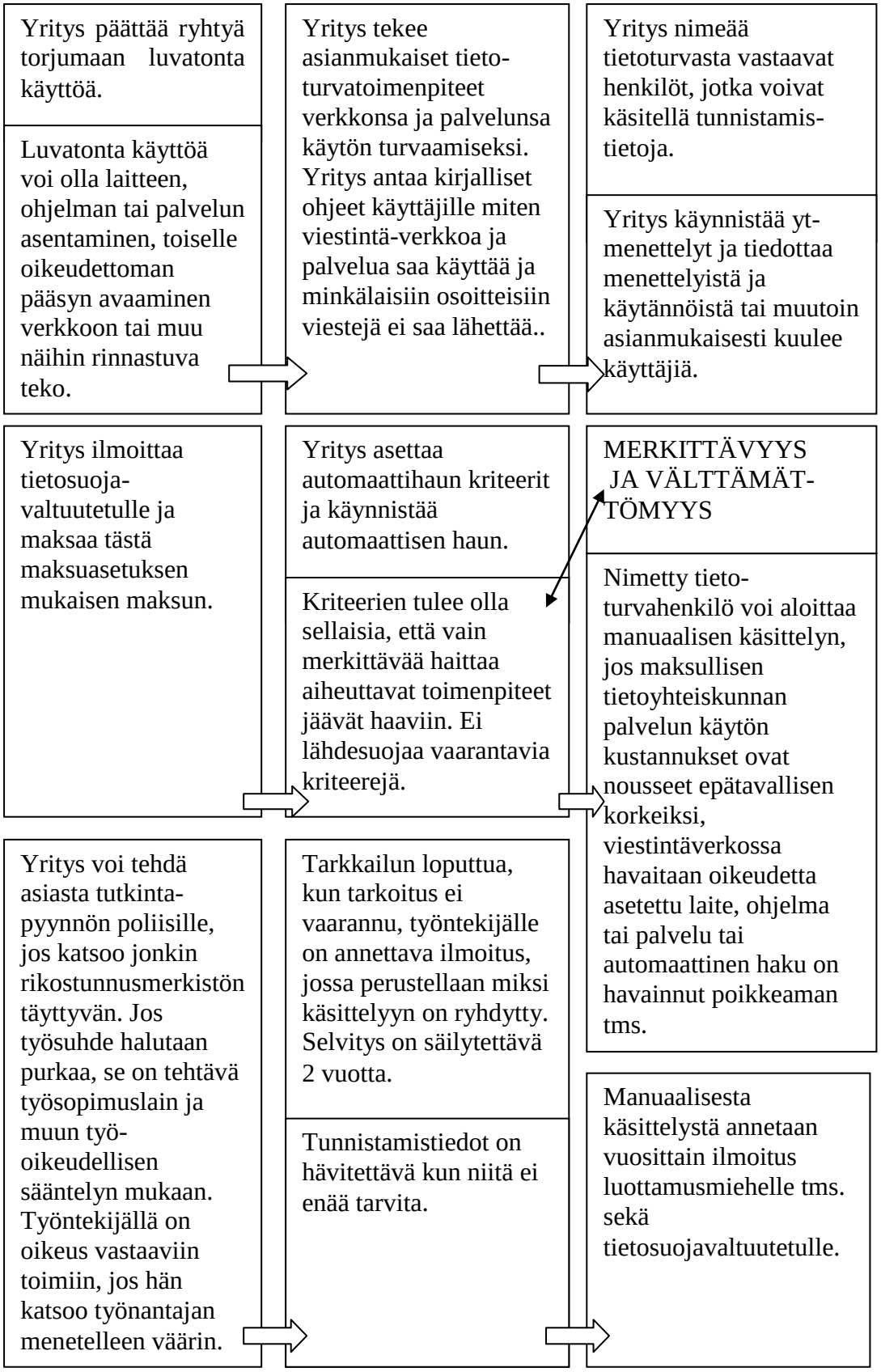
Automaattisessa haussa kone hakee massamuotoisesti viestintäverkosta automaattisesti poikkeamia tietyin ennalta määritellyin kriteerein. Kriteereiksi soveltuvat vain laissa määritellyt perusteet, esimerkiksi viestin epätavallisen suuri koko, viestin tyyppiin perustuva, esimerkiksi viestin tallennusmuoto .doc, viestien määrä, yhteystapa tai kohdeosoite, mihin yhteisötilaaja on rajoittanut tai kieltänyt kokonaan liikennöinnin. Automaattinen haku on täysin tekninen toimenpide, joten siinä ei tule yksittäisen käyttäjän tunnistamistietoja kenenkään luonnollisen henkilön tietoon. Käytännössä luvatonta käyttöä voidaan selvittää muun muassa kapasiteetin käyttömittareilla tai palomuurein, joilla yhteisötilaaja voi estää liikennöinnin omasta verkostaan tiettyihin kohdeosoitteisiin. Luvattoman käytön seuraaminen on kohdistuttava vain yhteisötilaajan kannalta merkittävään toimintaan, ja rajoitusten oltava muutoinkin asiallisia ja perusteltuja. Automaattinen käsittely on tarkoitettu jatkuvaksi toiminnaksi, että se voi tosiasiallisesti seurata luvatonta käyttöä. (Helopuro, Perttula & Ristola 2009, 112-114.) (HE 48/2008, 23-24.)

Sähköisen viestinnän tietosuojalain 13 d §:n 2 momentin mukaan yhteisötilaaja saa käsitellä tunnistamistietoja myös manuaalisesti luvattoman käytön selvittämiseksi, jos hänellä on perusteltu syy epäillä, että viestintäverkkoa, viestintäpalvelua tai maksullista tietoyhteiskunnan palvelua käytetään yhteisötilaajan antamien kirjallisten käyttöohjeiden vastaisesti. Perusteltuja syitä

epäillä luvatonta käyttöä lain mukaan on jos yhteisötilaaja havaitsee automaattisen hakutoiminnon avulla viestinnässä poikkeaman, tai jos maksullisen tietoyhteiskunnan palvelun käytön kustannukset ovat nousseet epätavallisen korkeiksi, tai jos viestintäverkossa havaitaan sinne oikeudetta asennettu laite, ohjelma tai palvelu. Yhteisötilaaja saa käsitellä tunnistamistietoja manuaalisesti myös jos yksittäistapauksesta muusta edellä mainittuihin seikkoihin rinnastuvasta, voidaan päätellä, että viestintäverkkoa, viestintäpalvelua tai maksullista tietoyhteiskunnan palvelua käytetään yhteisötilaajan antamien kirjallisten käyttöohjeiden vastaisesti. (L516/2004.)

Manuaalisella käsittelyllä tarkoitetaan sähköisessä muodossa olevien tunnistamistietojen käsittelyä siten, että luonnollinen henkilö jolle tehtävä on osoitettu, tapauskohtaisesti hakee esille jonkin tunnistamistiedon, kuten esimerkiksi tietyn käyttäjän yhteysosoitteen tai tietyn käyttäjäjoukon yhteysosoitteet. Automaattisen hakutoiminnon havaitsemalla poikkeamalla tarkoitetaan sellaisia viestejä, joista on niiden koon, tyypin, määrän, yhteystavan tai kohdeosoitteen perusteella tallentunut automaattiseen hakuun havainto. Lain rinnastuslauseke kattaa myös sellaiset tilanteet, joita ei ole lain säätämisvaiheessa pystytty luettelemaan, mutta joita voi myöhemmin esiintyä. (Helopuro, Perttula & Ristola 2009, 114-115.) (HE 48/2008, 24.)

Luvattoman käytön selvittämisen edellytyksenä edellä mainittujen seikkojen lisäksi on, että mahdollinen väärinkäytös aiheuttaa yhteisötilaajalle merkittävää haittaa tai vahinkoa. Ja että käsittelyllä saadut tiedot ovat välttämättömiä luvattoman käytön ja siitä vastuussa olevien selvittämiseksi sekä luvattoman käytön lopettamiseksi. (L516/2004.) Toisin sanoen automaattista hakua ei saa asettaa valvomaan tavallista viestintää, tai muuta sellaista asiaa, millä ei ole yhteisötilaajan liiketoiminnalle suurta taloudellista merkitystä tai tietoturvauhkaa. Merkittävä haitta konkretisoituu viimekädessä yhteisötilaajan antamilla ohjeilla. Pykälissä luvattoman käytön selvittämisen edellytyksissä korostuu vielä välttämättömyysedellytys, eli että tunnistamistietoja ei saa käsitellä muutoin kuin silloin kun se on aivan välttämätöntä. (Helopuro, Perttula & Ristola 2009, 116-117.)



Kuvio 1. Luvattoman käytön selvittäminen (Helopuro, Perttula & Ristola 2009, 136.)

9.2 Yhteisötilaajan käsittelyoikeus yrityssalaisuuksien paljastamisen selvittämiseksi

Sähköisen viestinnän tietosuojalain 13 e §:n 1 momentti mahdollistaa yhteisötilaajan käsitellä tunnistamistietoja yrityssalaisuuksien paljastamisen selvittämiseksi. Pykälä antaa yrityksille mahdollisuuden kerätä riittävästi tietoa mahdollisesta yrityssalaisuuden vuotamisesta ja saada sillä tavoin näyttöä esitutkinnan käynnistämiseksi. Tietoisuuden siitä, että yrityssalaisuuksien vuotamista voidaan valvoa ja estää, toivotaan vaikuttavan myös ennaltaehkäisevästi. Yrityssalaisuuksien paljastamisen selvittämiseksi yhteisötilaaja voi käsitellä tunnistamistietoja automaattisen hakutoiminnon avulla samoin edellytyksin ja kriteerein kuin luvattoman käytön selvittämisessä. (L516/2004.) (Helopuro, Perttula & Ristola 2009, 118-119.)

Sähköisen viestinnän tietosuojalain 13 e §:n 2 momentin mukaan yhteisötilaaja saa käsitellä tunnistamistietoja manuaalisesti, jos hänellä on perusteltu syy epäillä, että yrityssalaisuus on viestintäverkkoa tai viestintäpalvelua luvattomasti käyttämällä annettu ulkopuoliselle. Perusteltuja syitä lain mukaan on jos automaattisen hakutoiminnon avulla on havaittu viestinnässä poikkeama, tai jos yrityssalaisuus julkaistaan tai sitä käytetään luvatta. (L516/2004.) Poikkeamalla tarkoitetaan samaa kuin sähköisen viestinnän tietosuojalain 13 d pykälässä luvattoman käytön selvittämisessä. Yrityssalaisuuden julkaisemisella tai käyttämisellä luvatta tarkoitetaan sitä, että jonkun yrityksen yrityssalaisuus saatetaan julkaista esimerkiksi messuilla tai Internetissä. Tällöin on perusteltua, että yritys voi selvittää kaikkien muiden edellytysten täytyttyä myös viestiliikennettään, eli sitä kuka on mahdollisesti vuotanut tiedot ulkopuoliselle. Perusteltu syy epäillä yrityssalaisuuksien oikeudetonta paljastamista voisi olla esimerkiksi silloin, jos yrityssalaisuus on julkaistu tai sellaisen kehitystyön tietojen perusteella joku muu on kehittänyt kehitystyötä harjoittavan tahon kanssa samanlaisen laitteen tai palvelun. (Helopuro, Perttula & Ristola 2009, 119-120.)

Sähköisen viestinnän tietosuojalain 13 e §:än on pykälän 13 d:n tavoin myös otettu rinnastuslauseke, jonka mukaan yhteisötilaaja saa käsitellä tunnistamistietoja manuaalisesti yrityssalaisuuksien paljastamisen selvittämiseksi

myös jos yksittäistapauksessa muusta yleisesti havaittavissa olevasta seikasta voidaan päätellä, että yrityssalaisuus on luvattomasti annettu ulkopuoliselle. Yrityssalaisuuden luvattomalla antamisella ulkopuoliselle tarkoitetaan sitä, että viestintäverkon tai palvelun käyttäjä lähettää tai antaa luvatta sivulliselle pääsyn yrityssalaisuuksiin yhteisötilaajan viestintäverkon kautta tai viestintäpalvelua hyväksikäyttämällä. (L516/2004.) (Helopuro, Perttula & Ristola 2009, 119-120.)

Automaattisen ja manuaalisen tunnistamistietojen käsittelyn edellytyksenä on lisäksi, että epäilty yrityssalaisuuden paljastaminen kohdistuu yhteisötilaajan tai sen yhteistyökumppanin elinkeinotoiminnan kannalta keskeisiin yrityssalaisuuksiin taikka teknologisen tai muun kehitystyön tuloksiin, jotka ovat todennäköisesti merkittäviä elinkeinotoiminnan käynnistämisen tai sen harjoittamisen kannalta. (L516/2004.) Keskeisiä yrityssalaisuuksia ovat muun muassa tiedot, jotka antavat yritykselle kilpailuedun ja joita ei voi selvittää julkisista lähteistä. Yrityssalaisuuksia ovat myös ne tiedot, joiden käsittelystä ja suojaamisesta elinkeinonharjoittaja on laatinut erityiset ohjeet ja suojaamiskäytännöt. Säännökseen on erikseen otettu maininta kehitystyön tuloksista, koska vaikka esimerkiksi tutkimuksen välivaiheen tuloksia ei sinänsä voi vielä pitää liiketoiminnan kannalta keskeisinä, tuloksilla voi siitä huolimatta olla elinkeinonharjoittajalle merkittävää hyötyä, jos välivaiheen tuloksilla voidaan osoittaa esimerkiksi kehittämistyön jatkamisen kannattamattomuus. Automaattisen ja manuaalisen tunnistamistietojen käsittelyn edellytyksenä on myös, niin kuin luvattoman käytönkin kohdalla, että käsittelyllä saadut tiedot ovat välttämättömiä yrityssalaisuuden paljastamisen ja siitä vastuussa olevien henkilöiden selvittämiseksi. (L516/2004.) (Helopuro, Perttula & Ristola 2009, 121-122.)

Kuvio 2. Yrityssalaisuuden paljastamisen ehkäiseminen ja selvittäminen (Helopuro, Perttula & Ristola 2009, 137.)

9.3 Käsittelyoikeuden rajoitukset

Sähköisen viestinnän tietosuojalain 13 f § sääntelee tunnistamistietojen käsittelyoikeuden erityisiä rajoituksia väärinkäytöstapauksissa. Sen 1 momentin mukaan automaattista hakua ei saa kohdistaa eikä tunnistamistietoja saa hakea esille eikä ottaa manuaalisesti käsiteltäviksi lähdesuojan piiriin kuuluvien tietojen selville saamiseksi. (L516/2004.) Säännöksellä suojataan nimenomaan toimittajia. Automaattinen hakutoiminto ei voi kohdistua tiedotusvälineisiin osoitettuihin sähköpostiosoitteisiin. Toimittajien lähettämien tai vastaanottamien viestien tunnistamistietoihin ei saa puuttua toimittajan työpaikalla. Jos yrityssalaisuus julkaistaan esimerkiksi lehdessä, ei toimittajaa voida velvoittaa paljastamaan tietolähdettään, tai sitä kuka kirjoituksen on laatinut. Yrityssalaisuusvuodon kohteeksi joutunut yritys sen sijaan saa käsitellä omasta viestintäverkosta kerättyjä tunnistamistietoja vuodon löytämiseksi. Tällöin hakukriteeri ei kuitenkaan voi olla toimittajan sähköpostiosoite, vaan sen tulee olla esimerkiksi tiedoston tyyppi tai koko. (HE 48/2008, 26.) (Helopuro, Perttula & Ristola 2009, 123-124.)

Sähköisen viestinnän tietosuojalain 13 f §:n 2 momentin mukaan 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. (L516/2004.) Säännöksellä rajataan käsittelyoikeus koskemaan yrityssalaisuuksien paljastamisen selvittämiseksi vain työnantaja-asemassa olevia yhteisötilaajia. Pääsyn antaminen yhteisötilaajan muulla hyväksymällä tavalla voi tapahtua esimerkiksi käyttäjäoikeuksia hallinnoimalla. Henkilötahoja, joilla on pääsy yrityssalaisuuksiin, ovat ensisijaisesti asiantuntija- ja kehitystehtävissä työskentelevät henkilöt, joiden tehtäviin yrityssalaisuuksien käsittely kuuluu. Lisäksi yrityssalaisuudet voivat tulla erilaisissa avustavissa tehtävissä työskentelevien sekä tietojärjestelmien ylläpidosta ja huollosta vastaavien henkilöiden tietoon työtehtävien tai laajojen käyttäjäoikeuksien kautta. (HE 48/2008, 26.)

10 YHTEISÖTILAAJAN TIEDONANTOVELVOLLISUUS VÄÄRINKÄYTÖSTAPAUKSISSA

Kun tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty luvattoman käytön tai yrityssalaisuuden paljastamisen selvittämiseksi, on yhteisötilaajan tiedotettava siitä kirjallisella selvityksellä tietoverkkonsa käyttäjälle, työntekijöiden edustajalle ja tehtävä vuosittain selvitys tietosuojavaltuutetulle. Selvitys on laadittava sähköisen viestinnän tietosuojalain 13 g §:n mukaan.

Selvityksestä on käytävä ilmi: 1) käsittelyn peruste, ajankohta ja kesto 2) syy, minkä vuoksi tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty 3) käsittelijät ja 4) käsittelystä päättänyt henkilö. Käsittelyyn osallistuneiden henkilöiden on lisäksi allekirjoitettava selvitys. Selvitys on säilytettävä vähintään kaksi vuotta tunnistamistietojen käsittelyn päättymisestä, koska henkilötietojen vastainen käsittely ja rekisteriin tunkeutuminen ovat kriminalisoituja tekoja, joiden syyteoikeus vanhentuu kahdessa vuodessa. (L156/2004.)

10.1 Yhteisötilaajan tiedonantovelvollisuus käyttäjälle

Selvitys on tarpeen viestintäverkkojen ja palvelujen käyttäjien, tietojen käsittelyyn osallistuneiden ja siitä päättäneen henkilön oikeusturvan kannalta. Jälkikäteen on voitava selvittää kuka tietoja on käsitellyt, mihin ajankohtaan ja kenen aloitteesta. Tiedoilla voidaan jälkikäteen selvittää mahdollisia väärinkäytöksiä. Selvityksistä tai tallennetuista tiedoista muodostuu henkilötietolain tarkoittama henkilörekisteri, jota tietosuojavaltuutettu on ohjeistanut käsiteltäväksi henkilötietolain mukaan. (HE 48/2008, 26.)

Selvitys käsittelystä on annettava tiedoksi käsittelyn kohteena olevan viestintäverkon tai viestintäpalvelun käyttäjälle heti, kun se voi tapahtua käsittelyn tarkoitusta vaarantamatta. Saatuaan tiedon tunnistamistietojensa käsittelystä, käyttäjällä on mahdollisuus varmistua toimien lainmukaisuudesta ja kääntyä tarvittaessa tietosuojavaltuutetun, poliisin tai työntekijän ammattijärjestön puoleen. 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. (L156/2004.) Säännöksessä ei ole annettu ehdotonta takarajaa selvityksen tiedoksi antamiselle, mutta selvitys on pyrittävä antamaan mahdollisimman pian käsittelyn päätyttyä. Tunnistamistietoja ei saa käsitellä yhtään sen enempää kuin on välttämätöntä, ja heti kun epäiltyä väärinkäytöstä on selvitetty riittävästi, on käsittely lopetettava ja siitä on laadittava ja annettava käyttäjälle selvitys. (HE 48/2008, 27.)

10.2 Yhteisötilaajan tiedonantovelvollisuus työntekijöiden edustajalle

Sähköisen viestinnän tietosuojalain 13 h §:n mukaan yksityisyyden suojan tehokkaan valvonnan toteuttamiseksi on työnantaja-asemassa olevan yhteisötilaajan annettava selvitys tunnistamistietojen käsittelystä myös työntekijöiden edustajalle. Työntekijöiden edustajalle vuosittain tehtävästä selvityksestä on käytävä ilmi mitä 13 g §:n 1 momentissa on sanottu, eli käsittelyn peruste, sen ajankohta ja kesto, syy minkä vuoksi tunnistamistietojen manuaaliseen käsittelyyn on ryhdytty, käsittelijät ja käsittelystä päättänyt henkilö. Lisäksi selvityksestä on käytävä ilmi millä perusteella ja kuinka monta kertaa tunnistamistietoja on vuoden aikana käsitelty. (L516/2004.)

Tunnistamistietojen käsittelystä tehty selvitys on annettava lähtökohtaisesti työehtosopimuksen perusteella valitulle luottamusmiehelle. Jos luottamusmiestä ei ole valittu, on selvitys annettava työsopimuslain (55/2001) 13 luvun 3 §:ssä tarkoitetulle luottamusvaltuutetulle. Jos jonkin henkilöstöryhmän työntekijät eivät ole valinneet luottamusmiestä eikä luottamusvaltuutettua, on selvitys annettava yhteistoiminnasta yrityksissä annetun lain 8 §:ssä tarkoitetulle yhteistoimintaedustajalle. Jos yhteistoimintaedustajaakaan ei ole valittu, selvitys on annettava kaikille tähän henkilöstöryhmään kuuluville työntekijöille. (L516/2004.)

Yhteistoimintamenettelyn tai tiedottamisen piiriin kuuluvista tiedoista osa ei ole julkisia. Elinkeinotoiminnan jatkumisen ja menettelyjen tarkoituksen kannalta on

tärkeää etteivät tiedot mahdollisista yrityssalaisuuksien loukkaamisista leviä tarpeettomasti. Sähköisen viestinnän tietosuojalain 13 g §:n 3 momentin mukaan selvityksestä tiedon saaneiden työntekijöiden ja heidän edustajien on pidettävä salassa tietoonsa saamat yrityssalaisuuden loukkaukset ja epäilyt yrityssalaisuuden loukkaamisesta koko työsuhteen voimassaoloajan, riippumatta siitä hoitaako henkilö koko työsuhteensa ajan sitä tehtävää, jossa hän on tiedon saanut vai ei. Salassapitovelvollisuus ei kuitenkaan estä tietojen luovuttamista valvontaviranomaisille. Tietoyhteiskunnan palvelujen tai viestintäverkkojen luvaton tai ohjeen vastainen käyttö tai rikollinen toiminta ei automaattisesti ole peruste työsuhteen päättämiseen. Työsuhteen päättäminen tulee ratkaista tapauskohtaisesti työsopimuslain ja muun työoikeudellisen lainsäädännön perusteella. Työsuhteen päättämistä koskevissa oikeudenkäynneissä työnantaja on velvollinen näyttämään toteen työsuhteen päättämisperusteen olemassaolon. (L516/2004.) (HE 48/2008, 27-28.) (Helopuro, Perttula & Ristola 2009, 129.)

10.3 Ennakkoilmoitus ja vuosittainen selvitys tietosuojavaltuutetulle

Sähköisen viestinnän tietosuojalain 13 i §:n mukaan yhteisötilaajan on annettava ennalta tietosuojavaltuutetulle kertaluonteinen selvitys tunnistamistietojen käsittelyn aloittamisesta. Ennakkoilmoituksesta on käytävä ilmi 13 d ja 13 e §:ssä tarkoitetussa tunnistamistietojen käsittelyssä noudatettavien menettelyjen perusteet ja käytännöt. Tunnistamistietojen käsittelyssä automaattisen hakutoiminnon avulla noudatettavia perusteita voivat olla viestin koko, yhteenlaskettu koko, tyyppi, määrä, yhteystapa tai kohdeosoite. Ilmoituksesta tulee selvitä ne henkilöt, joiden tehtäviin tunnistamistietojen käsittely kuuluu ja tehtävät, joissa tietoja käsitellään. Ilmoituksesta on myös käytävä ilmi miten yhteisötilaaja on hoitanut käsittelyä edeltävän tiedottamisvelvollisuutensa. Eli miten yhteisötilaaja on tiedottanut tai tiedottaa näistä seikoista viestintäverkkojen ja –palvelujen käyttäjille. (L516/2004.) Jos selvityksen kohteena olevissa seikoissa tapahtuu olennaisia muutoksia, tulee muutoksista toimittaa uusi selvitys tietosuojavaltuutetulle. Yhteisötilaajan ilmoitusvelvollisuudella parannetaan käyttäjien oikeusturvaa. Tietosuojavaltuutettu saa myös näin etukäteen tiedon niistä tahoista, jotka ryhtyvät käyttämään käsittelyoikeuttaan ja voi toimintansa

tarkoituksenmukaisella järjestämisellä ryhtyä toteuttamaan lain soveltamisen valvontaa. 30. huhtikuuta 2010 mennessä tietosuojavaltuutetun toimistoon ei ollut tullut yhtään sähköisen viestinnän 13 i §:n mukaista ennakkoilmoitusta tunnistamistietojen käsittelyn aloittamisesta. (Sähköpostitiedustelu 30.4.2010 tietosuojavaltuutetun toimistosta.) (HE 48/2008, 28.) (Helopuro, Perttula & Ristola 2009, 130.)

Sähköisen viestinnän tietosuojalain 13 i §:n mukaan yhteisötilaajan on lisäksi annettava tietosuojavaltuutetulle vuosittain jälkikäteen selvitys tunnistamistietojen manuaalisesta käsittelystä. Automaattisesta käsittelystä selvitystä ei tarvitse antaa. Selvityksestä on käytävä ilmi, onko käsittelyn perusteena ollut maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai viestintäpalvelun luvaton käyttö vai yrityssalaisuuden paljastaminen ja kuinka monta kertaa tunnistamistietoja on vuoden aikana käsitelty. (L516/2004.) (HE 48/2008, 28.)

11 TIETOTURVASTA HUOLEHTIMINEN

Tietoturvasta huolehtiminen kuuluu yhteisötilaajan huolehtimisvelvollisuuteen ja on yksi tärkeä edellytys tunnistamistietojen käsittelyn aloittamiselle. Sähköisen viestinnän tietosuojalain 19 § velvoittaa yhteisötilaajan huolehtimaan tietoturvasta ja 20 § velvoittaa niihin toimenpiteisiin, mitä yhteisötilaajan tulee tehdä asianmukaisen tietoturvan toteuttamiseksi. Sähköisen viestinnän tietosuojalain 19 §:n mukaan yhteisötilaajan on huolehdittava käyttäjiensä tunnistamistietojen käsittelyn tietoturvasta. Tämä tarkoittaa toimenpiteitä toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Nämä toimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin. Tietoturvan huolehtimisvelvoitteen laiminlyönti voi johtaa rikosoikeudelliseen vastuuseen. (L516/2004.)

Tietoturvatoimia toteuttaessa tiedossa oleviin uhkiin tulee varautua uskottavin tietoturvatoimin. Sähköisen viestinnän tietosuojalaki ei kuitenkaan edellytä yhteisötilaajaa käyttämään normaalin toiminnan kannalta kohtuuttomia summia rahaa tietoturvatoimiin. Toiminnan turvallisuudella tarkoitetaan sitä, että ylläpidetään kirjallisia ohjeita siitä, miten tietoturvavaatimukset toteutetaan, oman tietoturvan tasoa seurataan säännöllisesti, varmistetaan tietoturvavaatimusten toteutuminen käytettäessä alihankkijoita ja suojataan laitteet ja tiedostot luvatonta pääsyä ja käyttöä vastaan. Lisäksi yhteisötilaajan on pidettävä rekisteriä kunkin järjestelmän osalta siitä, kenellä on järjestelmän käyttäjätunnuksia ja mitä oikeuksia milläkin käyttäjätunnuksella on. Yhteisötilaajan tulee myös valvoa tietojen, asiakirjojen, viestintäverkkojen, laitteistojen, palvelujen ja tiedostojen tietoturvaan vaikuttavia tapahtumia niin, että tietoturvan kannalta merkittävät tapahtumat havaitaan. (Helopuro, Perttula & Ristola 2009, 194-196.)

Tietoliikenneturvallisuudella tarkoitetaan sitä, että viestintäverkkojen avulla välitettävät viestit ja tunnistamistiedot eivät paljastu asiaankuulumattomille ja että asiaankuulumattomat eivät pääse muuttamaan tai tuhoamaan viestintäverkoissa välitettäviä viestejä, eikä pääse käsittelyä koskeviin tietoihin. Lisäksi

viestintäverkoissa on toiminnan kannalta oltava riittävät todentamis- ja kiistättömyysmenettelyt. (Helopuro, Perttula & Ristola 2009, 196.)

Laitteisto- ja ohjelmistoturvallisuudella tarkoitetaan sitä, että käytetään sellaisia laitteistoja, tietojärjestelmiä ja ohjelmistoja, joista aiheutuva tietoturvauhka on vähäinen, sekä järjestetään toiminnan kannalta tärkeiden ohjelmistojen varmuuskopiointi ja turvallinen säilytys. Lisäksi tietoaineistoturvallisuudella tarkoitetaan sitä, että järjestetään tietoaineistojen turvallinen käsittely hyvän tietojenkäsittelytavan mukaisesti ja tietoaineistojen varmuuskopiointi ja turvallinen säilytys sekä että tärkeät asiakirjat, tietovarastot ja yksittäiset tiedot suojataan. (Helopuro, Perttula & Ristola 2009, 196.)

11.1 Roskapostin ja haittaohjelmien suodattaminen

Tekniikan kehittyessä ja elinkeinonharjoittamisen pääpainon siirtyessä verkkoon, myös verkossa tapahtuva rikollisuus ja muu vahingonteko on lisääntynyt. Rehellistä elinkeinotoimintaa verkossa harjoittavien riesana ovat jatkuvasti lisääntyneet tahalliset tietoturvaloukkaukset. Näitä ovat tahallinen haittaohjelmien levittäminen ja käyttö, erilaiset roskapostiviestit tai muut tyypillisesti ulkopuolelta viestintäverkkoon tai -palveluihin kohdistuvat tunkeutumiset. Luvattomilla tunkeutumisilla pyritään saamaan selville käyttäjien tietoja, tai ottamaan haltuun tietokoneita, roskapostiviestien lähettämiseksi, tai tunkeutumisilla pyritään heikentämään, jopa kokonaan lamauttamaan tietoliikenne ja tietojärjestelmät. Roskapostiviestejä ovat sellaiset ei-toivotut sähköpostiviestit, joihin vastaanottaja ei ole antanut suostumustaan tai hänellä ei ole mahdollisuutta kieltää kyseisten viestien vastaanottamista. Suomessa roskapostiviestien lähettäminen on ollut laitonta jo vuodesta 1999, mutta koska suurin osa roskapostista lähetetään ulkomailta, ei laittomaksi säätämisellä ole ollut toivottuja vaikutuksia. Muita verkon käytettävyyteen liittyviä häiriöitä voi syntyä myös jos käyttäjät esimerkiksi hakevat ja käyttävät suuressa määrin tietoja toistensa päätelaitteilta, tai jos työntekijä asettaa sähköpostiinsa automaattisen vastaustoiminnon poissaolonsa ajaksi ja toinen käyttäjä on toiminut samoin, voi keskinäisten automaattisten vastausten määrä nousta lyhyessäkin ajassa ennakoimattoman

suureksi ja näin vaarantaa tietojärjestelmien toimintakyvyn. (Helopuro, Perttula & Ristola 2009, 200-201.)

Tietoturvauhat on pyritty minimoimaan sähköisen viestinnän tietosuojalain 20 §:n uudistetuilla säännöksillä. Suomessa toimivia tahoja on uudistuksella pyritty velvoittamaan huolellisesti toteutettuun roskapostiviestien, muun haittaliikenteen ja haittaohjelmien suodattamiseen. Nämä tietoturvatoimenpiteet kohdistuvat usein miten viestintäverkkoon tai palveluun saapuvaan liikenteeseen, tai joissain tilanteissa lähtevän liikenteen tietoturvauhan selvittämiseksi. Säännöksen keskeinen tarkoitus on viestinnän eri osapuolten etujen mukaisesti turvata tietoverkkojen toimivuutta ja turvallisuutta sekä näin luoda edellytyksiä sananvapauden käyttämiselle ja viestinnän luottamuksellisuudelle viestintäverkossa. (Helopuro, Perttula & Ristola 2009, 200-201, 298.)

Sähköisen viestinnän tietosuojalain 20 §:n 1 momentin mukaan yhteisötilaajalla ja sen lukuun toimivalla on oikeus ryhtyä välttämättömiin tietoturvatoimiin havaitakseen viestintäverkkojen tai niihin liitettyjen palvelujen tietoturvalle haittaa aiheuttavat häiriöt, häiriöiden estämiseksi, selvittämiseksi, ja esitutkintaan saattamiseksi. Tietoturvatoimin tulee ryhtyä myös viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi, toisin sanoen yhteisötilaajan on huolehdittava siitä, että yksittäisen käyttäjän roskapostiviestit tai muut ei-toivotut viestit eivät nouse niin korkeiksi, että viestintämahdollisuudet estyvät kokonaan, vaikka tällaisten viestien määrä ei vaikuttaisikaan koko viestintäverkon tai –palvelun toimintaan. Yhteisötilaajan tulee laittaa tietoturvansa kuntoon myös estääkseen viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelu. Eli pyrkiä estämään niin sanottu phisning, tietojen kalastelu, jolloin suurelle käyttäjäjoukolle toimitetaan viestejä, joilla pyritään hankkimaan tietoja käyttäjistä tai heidän maksuvälineistään laittomiin käyttötarkoituksiin. (L516/2004.) (Helopuro, Perttula & Ristola 2009, 202.)

Yhteisötilaaja voi toteuttaa edellä tarkoitetut toimet esimerkiksi viestin automaattisen sisällöllisen analyysin avulla, jossa haitalliset ohjelmat ja käskyt tunnistetaan ennalta määriteltyjen kriteerien perusteella, esimerkiksi jos tietty sana

sisältyy viestiin usein toistuvana, tällöin viestin sisältö ei tule luonnollisen henkilön tietoon. Tai viestin välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen avulla, esimerkiksi niin, että järjestelmä lukee ensin teknisesti itse viestin ja suodattaa sellaiset viestit pois missä on käytetty tiettyjä avainsanoja, esimerkiksi, only for you, sex tai viagra, koska roskapostiviestien lähettäjät käyttävät yleensä näitä sanoja. Tietoturvaa vaarantavat haitalliset tietokoneohjelmat voidaan myös poistaa viesteistä automaattisesti erilaisten teknisluonteisten toimenpiteiden avulla. (L516/2004.) (Helopuro, Perttula & Ristola 2009, 203.)

Jos viestin tyypin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn eikä viestin automaattisella sisällöllisellä analyysillä pystytä turvaamaan 1 momentissa tarkoitettujen tavoitteiden toteutumista, yksittäisen viestin sisältöä saa käsitellä manuaalisesti. Manuaalisesta viestin sisällön käsittelystä on ilmoitettava viestin lähettäjälle ja vastaanottajalle, jos ilmoittamisella ei todennäköisesti vaaranneta 1 momentissa tarkoitettujen tavoitteiden toteutumista. (L516/2004.)

Sähköisen viestinnän tietosuojalain 20 §:n säännökset tietoturvatoimenpiteistä on toteutettava huolellisesti ja ne on mitoitettava torjuttavan häiriön vakavuuteen. Toimenpiteitä toteuttaessa 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 20 pykälässä säädettyjä edellytyksiä. (L516/2004.) Roskapostin suodatus tulee siis olla välttämätöntä ja huolellista. Kun yhteisötilaaja alkaa suodattaa viestejä tietoturvansa toteuttamiseksi, on hänen huomioitava, että toimet saattavat suodattaa pois myös toivottuja ja luottamuksellisia viestejä. (HE 48/2008, 29-31.)

12 LAKIEN OHJAUS JA VALVONTA

Sähköisen viestinnän tietosuojalain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuus ja yksityisyyden suoja, sekä edistää sähköisen viestinnän tietoturvaa ja sen monipuolisten palvelujen tasapainoista kehittämistä. Lain tarkoituksen toteutumista ohjaa ja kehittää liikenne- ja viestintäministeriö. Ohjaus- ja kehittämisvastuu vaatii kansallisesti kiinteää yhteistyötä muiden alan toimijoiden, erityisesti viestintäviraston, tietosuoja-, kuluttaja- ja muiden keskeisten viranomaisten, teleyritysten, lisäarvopalvelun tarjoajien, laitevalmistajien ja tilaajia ja käyttäjiä edustavien yhteisöjen kanssa. Lain tarkoituksen toteutumiseksi tarvitaan myös kansainvälisesti aktiivista vaikuttamista, erityisesti tietosuoja- ja tietoturva –asioiden valmisteluun osallistumista Euroopan unionissa. Sähköisen viestinnän lainkohdat 30 §, 31 § ja 32 § määrittelevät mikä viranomainen valvoo lakia ja mitä tehtäviä viestintävirastolla ja tietosuojavaltuutetulla on lain toteutumisen valvonnassa. (Helopuro, Perttula & Ristola 2009, 295-296.)

Perustuslakivaliokunta pitää tärkeänä, että sähköisen viestinnän tietosuojalain noudattamista seuraamaan asetettu liikenne- ja viestintäministeriö arvioi lain soveltamista myös perusoikeuksien kannalta. Käytännössä tulisi kiinnittää huomiota siihen, miten laajasti työnantajat ovat turvautuneet lain mahdollistamiin oikeuksiin, miten tietosuojavaltuutetun valvontatehtävä on toiminut sekä miten työntekijöiden luottamuksellisten viestin salaisuuden suoja on toteutunut. Liikenne- ja viestintävaliokunta pitää kattavaa seurantaa lain toimivuudesta välttämättömänä. (LiVM 19/2008 vp, 8-9.) (HE 48/2008, 31-32.)

12.1 Viestintäviraston tehtävät

Viestintävirasto on keskeisin sähköisen viestinnän tietosuojalain soveltamista valvova viranomainen. Sen tehtävänä on valvoa sähköisen viestinnän tietosuojalain sekä sen nojalla annettujen säännösten ja määräysten noudattamista, ellei tietosuojavaltuutetun tehtävistä muuta johdu. Viestintäviraston tehtävänä on myös kerätä tietoa ja selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvat tietoturvaloukkaukset ja kerätä tietoa niiden

uhkista sekä näiden palvelujen merkittävistä vikatilanteista ja häiriötilanteista. Viestintäviraston tulee lisäksi tiedottaa ajankohtaisista tietoturva-asioista. Viestintäviraston on myös kuultava liikenne- ja viestintäministeriötä valmistellessaan sähköisen viestinnän tietosuojalain perusteella annettavia määräyksiä ja toimittava yhteistyössä näiden ministeriöiden kanssa. (L516/2004.)

12.2 Tietosuojavaltuutetun tehtävät

Tietosuojavaltuutettu valvoo yhteisötilaajan tunnistamistietojen käsittelyä tilanteissa, joissa maksullista tietoyhteiskunnan palvelua tai viestintäverkkoa on käytetty luvattomasti tai kun viestintäpalvelua käytetään ohjeen vastaisesti ja yrityssalaisuuksien oikeudettomassa paljastamisessa. Tietosuojavaltuutetun tehtävänä on valvoa henkilötietolain mukaisesti henkilötietojen käsittelyä, ja työelämän tietosuojalakia valvovat työsuojeluviranomaiset yhdessä tietosuojavaltuutetun kanssa. Yritykset työnantajina ovat yksi suurimmista yhteisötilaajan ryhmistä, niin on johdonmukaista, että tietosuojavaltuutettu valvoo osin myös sähköisen viestinnän tietosuojalain noudattamista. Valvonnasta aiheutuvista toimenpiteistä voidaan periä maksu yhteisötilaajalta. Maksuvelvollisuuden tulee olla oikeassa suhteessa valvottavan kokoon ja toiminnan luonteeseen. (LiVM 19/2008 vp, 8-9.) (HE 48/2008, 31-32.)

12.3 Valvontaviranomaisten tiedonsaantioikeus ja salassapitovelvollisuus

Ohjaus- ja valvontaviranomaisilla, eli liikenne- ja viestintäministeriöllä, viestintävirastolla ja tietosuojavaltuutetulla on oikeus saada välttämättömät tiedot tehtäviensä hoitamiseksi salassapito- tai muiden tietojen luovuttamista koskevien rajoitusten estämättä. Tietojen saamisen edellytyksenä on kuitenkin, että viestintävirastolla tai tietosuojavaltuutetulla on todennäköinen syy epäillä jotain seuraavista rikkomuksista: tietosuojarikkomus, luvaton käyttö, vaaran aiheuttaminen tietojenkäsittelylle, vahingonteko, salassapitorikos, viestintäsalaisuuden loukkaus, tietoliikenteen häirintä, tietomurto, suojauksen purkujärjestelmärikos tai henkilörekisteririkos. Valvontaviranomaisten on hävitettävä saamansa tiedot heti, kun ne eivät enää ole tarpeen valvontaviranomaisten tehtävien hoitamiseksi tai niitä koskevan rikosasian

käsittelemiseksi. Kuitenkin viimeistään kahden vuoden, tai jos kysymys on tietoturvaloukkausten selvittämistä koskevista tiedoista viimeistään kymmenen vuoden kuluttua tietojen saamisesta tai tuomion antamisesta. (L516/2004.) (HE 48/2008, 32.)

Sähköisen viestinnän tietosuojalain 34 §:n mukaan valvontaviranomaisilla on vaitiolovelvollisuus tietoonsa saamista luottamuksellisista viesteistä ja tunnistamistiedoista. Muilta osin valvontaviranomaisten tulee pitää salassa saamansa tiedon sen mukaan, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään. (L516/2004.) (HE 48/2008, 32.)

12.4 Viestintäviraston ja tietosuojavaltuutetun pakkokeinot

Tiedonsaantioikeuksien lisäksi valvovilla viranomaisilla on käytettävissään pakkokeinoja, joista säädetään sähköisen viestinnän tietosuojalain 41 §:ssä. Pykälän mukaan jos joku rikkoo sähköisen viestinnän tietosuojalakia tai sen nojalla annettuja säännöksiä tai määräyksiä eikä kehotuksesta huolimatta kohtuullisessa määräajassa oikaise menettelyään, viestintävirasto ja tietosuojavaltuutettu voi velvoittaa rikkojan korjaamaan virheensä tai laiminlyöntinsä. Viestintävirasto ja tietosuojavaltuutettu voi asettaa velvoitteen noudattamisen tehosteeksi uhkasakon tai uhan, että tekemättä jätetty toimenpide teetetään asianomaisen kustannuksella. Jos rikkomus on vakava, asetettava uhka voi koskea myös sitä, että toiminta keskeytetään osaksi tai kokonaan. Viestintävirasto ja tietosuojavaltuutettu voi saattaa käsiteltävänään olevan asian esitutkinnan kohteeksi. (L516/2004.) (Helopuro, Perttula & Ristola 2009, 302-303.)

Uhkasakkolain (1113/1990) 3 luvun 14 §:n teettämis- ja keskeyttämisuhan mukaan teettämisuhka asetetaan määräämällä päävelvoite noudatettavaksi uhalla, että tekemättä jätetty työ tehdään laiminlyöjän kustannuksella. Keskeyttämisuhka asetetaan määräämällä päävelvoite noudatettavaksi uhalla, että työnteko tai muu toiminta keskeytetään taikka laitteen tai muun esineen käyttö estetään. Teettämisestä tai keskeyttämisestä päättänyt viranomainen voi huolehtia teettämisestä tai keskeyttämisestä suorittamalla tarpeelliset toimet itse tai

antamalla ne muun viranomaisen tai yksityisen suoritettaviksi. Poliisin on tällöin annettava tarpeellista virka-apua. Teettämiskustannukset maksetaan etukäteen valtion varoista. Kustannukset saadaan periä ilman tuomiota tai päätöstä siinä järjestyksessä kuin verojen ja maksujen perimisestä ulosottotoimin on säädetty. (L1113/1990.)

13 RANGAISTUKSET

Sähköisen viestinnän tietosuojalain 42 §:n 1 momentissa viitataan niihin rikoslain pykäliin, joiden mukaan rangaistus määräytyy jos tietosuojalakia rikotaan. Sähköisen viestinnän tietosuojalain rikkomisesta tuomitaan rikoslain seuraavien pykälien mukaisesti: viestintäsalaisuuden loukkaaminen ja törkeää viestintäsalaisuuden loukkaaminen, rangaistus tietomurrosta ja vaitiolovelvollisuuden rikkomisesta. (L516/2004.)

13.1 Rikoslain säännökset

Rikoslain (39/1889) 38 luvun 3 ja 4 §:ssä viestintäsalaisuuden loukkaus on säädetty rangaistavaksi teoksi. Rikoslain 38 luvun 3 §:ssä säädetään rangaistus sille, joka oikeudettomasti avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä tai hankkii tiedon televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan-, tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta, on tuomittava sakkoon tai vankeuteen enintään yhdeksi vuodeksi. 38 luvun 4 §:ssä törkeän tekomuodon tunnusmerkeiksi on säädetty erityisen luottamusaseman käyttö taikka suunnitelmallisuus tai teon kohdistuminen erityisen luottamukselliseen viestiin tai huomattava yksityisyyden suojan loukkaus, ja jos teko on kokonaisuutena arvostellen törkeä on rikoksentekijä tuomittava vankeuteen enintään kolmeksi vuodeksi. Viestintäsalaisuuden ja törkeän viestintäsalaisuuden loukkauksen yritys on myös rangaistava. (HE 48/2008, 4.) (L39/1889.)

Rikos tietomurrosta on säädetty rangaistavaksi teoksi rikoslain 38 luvun 8 §:ssä. Pykälän mukaan, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan on tuomittava tietomurrosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan

tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon tietojärjestelmässä olevasta tiedosta. Tietomurron yritys on myös rangaistava. (L39/1889.)

Rangaistus sähköisen viestinnän tietosuojalain 5 §:n vaitiolovelvollisuuden ja hyväksikäyttökiellon rikkomisesta tuomitaan rikoslain 38 luvun 1 §:n tai 2 §:n mukaan. Rikoslain 38 luvun 1 §:n mukaan salassapitorikokseen tuomitaan se, joka laissa tai asetuksessa säädetyn taikka viranomaisen lain nojalla erikseen määräämän salassapitovelvollisuuden vastaisesti 1) paljastaa salassa pidettävän seikan, josta hän on asemassaan, toimessaan tai tehtävää suorittaessaan saanut tiedon, taikka 2) käyttää tällaista salaisuutta omaksi tai toisen hyödyksi, jollei teko ole rangaistava rikoslain 40 luvun 5 §:n mukaan, salassapitorikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. (L39/1889.) Rikoslain 38 luvun 2 §:n mukaan salassapitorikkomuksesta tuomitaan sakkoon, jos rikos on kokonaisuutena arvostellen vähäinen. Arvostelussa on otettava huomioon teon merkitys yksityisyyden tai luottamuksellisuuden suojan kannalta ja muut rikokseen liittyvät seikat. (L39/1889.)

Rikoslain 38 luvun 5 §:n mukaan myös virkasalaisuuden rikkominen ja tuottamuksellinen virkasalaisuuden rikkominen on säädetty rangaistavaksi teoksi. Pykälän mukaan jos virkamies tahallaan palvelussuhteensa aikana tai sen päätyttyä oikeudettomasti 1) paljastaa sellaisen asiakirjan tai tiedon, joka viranomaisten toiminnan julkisuudesta annetun lain (621/1999) tai muun lain mukaan on salassa pidettävä tai jota ei lain mukaan saa ilmaista, taikka 2) käyttää omaksi tai toisen hyödyksi taikka toisen vahingoksi 1 kohdassa tarkoitettua asiakirjaa tai tietoa, hänet on tuomittava, jollei teosta muualla säädetä ankarampaa rangaistusta, virkasalaisuuden rikkomisesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi. Virkamies voidaan tuomita myös viralta pantavaksi, jos rikos osoittaa hänet ilmeisen sopimattomaksi tehtäväänsä. Jos virkamies huolimattomuudesta syyllistyy 1 momentissa tarkoitettuun tekoon, eikä teko huomioon ottaen sen haitallisuus ja vahingollisuus sekä muut tekoon liittyvät seikat ole kokonaisuutena arvostellen vähäinen, hänet on tuomittava, jollei teosta

muualla säädetä ankarampaa rangaistusta, tuottamuksellisesta virkasalaisuuden rikkomisesta sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi. (L39/1889.)

Sähköisen viestinnän tietosuojalain rikkomuksesta on tuomittava sakko, jollei teosta muualla laissa säädetä ankarampaa rangaistusta sille joka tahallaan rikkoo 42 §:n 2 momentissa lueteltuja kohtia. Yhteisötilaajan kannalta merkittävimmät perusteet sakkoon tuomitsemiseksi ovat seuraavat 2 momentin kohdat: 3) jos yhteisötilaaja laiminlyö 19 §:ssä säädetyn velvollisuuden huolehtia käyttäjiensä tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta. 5) jos yhteisötilaaja käsittelee tunnistamistietoja 3 luvun säädetyn vastaisesti. Ja 9) jos yhteisötilaaja laiminlyö, mitä 13 g - 13 i §:ssä säädetään selvityksen tai ennakkoilmoituksen laatimisesta ja antamisesta käyttäjälle, työntekijöiden edustajalle tai tietosuojavaltuutetulle. Rangaistusta ei tuomita, jos rikos on vähäinen. (L516/2004.)

Jos työantaja avaa ja lukee työntekijän sähköpostiviestin ilman työntekijän lupaa, on teko rangaistava, vaikka sähköposti on työnantajan tarjoama ja otsikkotiedoista voi päätellä viestin liittyvän yrityksen liiketoimintaan. Työantaja välttyy rangaistusseuraamukselta vain, jos hän on tehnyt kaikki edellä mainitut toimenpiteet, mitä edellä käsitellyt lait edellyttävät, eli täyttänyt huolehtimis- ja ilmoitusvelvollisuutensa.

13.2 Työsuhteen päättäminen

Sähköisen viestinnän tietosuojalaki ei sääntele mitä tapahtuu jos yrityssalaisuus vuotaa tai jos sitä käytetään väärin, eikä laki sääntele myöskään tiedonsaajan vastuista asiassa. Vaikutus työsuhteen päättämiseen ja varoitusmenettely määräytyvät erikseen työ- ja virkaoikeudellisin perustein kokonaisharkinnan pohjalta. Kokonaisharkinta merkitsee jokaisessa yksittäistapauksessa intressivertailua, jossa vastakkain asetetaan irtisanomisperusteen täyttymistä puoltavat ja sitä vastustavat seikat. Vertailussa huomioon otettavien tekijöiden painoarvo joudutaan arvioimaan tilannekohtaisesti. Työnantajan on näytettävä toteen irtisanomisperusteet. (LiVM 19/2008 vp, 7.)

14 LOPUKSI

Ennen opinnäytetyön aloittamista tiesin vain vähän Lex Nokiasta. Media oli pitänyt huolen siitä, että mahdollisesta lakiuudistuksesta tuotiin esille kaikki negatiiviset puolet. Eli kun laki tulee voimaan, niin se käytännössä heikentäisi työntekijöiden yksityisyyttä merkittävästi työpaikoilla, ja että työnantaja saa lain voimaantulon jälkeen melkeinpä mielivaltaisesti puuttua työntekijöidensä sähköiseen viestintään ja verkon käyttöön työpaikoilla. Halusin selvittää, onko Lex Nokian kritisoimiseen ollut todellista syytä ja miksi suomalaiset olivat niin tuohtuneita asiasta kun lakia valmisteltiin.

Sähköisen viestinnän tietosuojalakiin tarkemmin tutustuessa huomasin, että tunnistamistietojen käsittely ja sähköpostin lukeminen on tehty työnantajan kannalta niin monimutkaiseksi prosessiksi, että käytännössä työnantaja ei ryhdy lukemaan työntekijänsä sähköposteja tai selvittämään tunnistamistietoja kovin helposti. Laissa on myös korostettu välttämättömyysperiaatetta, eli ihan jokaisessa työpaikassa, kenen tahansa henkilön sähköpostia ja verkkoliikennettä ei ole mitään syytä, eikä oikeutta seurata. Lakiuudistus ei näin ollen ole vielä kaventanut työntekijän yksityisyyttä työelämässä. Opinnäytetyöntyötäni kirjoittaessa ja aiheesta muiden kanssa keskusteltaessa on ollut mielenkiintoista huomata, kuinka monet muistaa Lex Nokiasta nousseen mediakohun ja negatiivisen keskustelun, mutta ei osaa sen tarkemmin sanoa, mitä lakiuudistus oikeasti toi tullessaan. Tietosuojavaltuutetun antaman tiedon perusteella lakia ei ole vielä keväällä 2010 ryhdytty soveltamaan tunnistamistietojen manuaalisen käsittelyn aloittamisen osalta. Tästä herääkin kysymys, onko laki ollut tarpeellinen tai hyvä, jos sitä ei ole ryhdytty soveltamaan. Itse haluan uskoa, että lailla on ennaltaehkäisevä vaikutus yrityssalaisuuksien oikeudettoman paljastamisen ja luvattoman käytön estämisissä. Toivon, että jatkossakaan aiheesta ei ole luettavissa oikeuskäytäntöä, koska tällöin mitään väärinkäytöksiä ei olisi tapahtunut. Olen tyytyväinen aiheeni valintaan, koska nyt tiedän ja voin kertoa muille, että ei ole mitään syytä huolestua yksityisyyden suojan heikkenemisestä työpaikoilla. Toivon, että mahdollisimman moni innostuu lukemaan työni ja selvittämään, mitä tuo niin paljon tunteita kuohuttanut lakiuudistus oikeasti tarkoitti.

15 LÄHTEET

Defensor Legis N:o 4/2008. Yrityssalaisuuksien suojaaminen ja oma henkilöstö. Nyblin, Klaus.

Hallituksen esitys 162/2003 vp. HE 162/2003.

Hallituksen esitys 48/2008 vp. HE 48/2008.

Hallituksen esitys 66/1988 vp. HE 66/1988.

Helopuro, Sanna, Perttula, Juha & Ristola, Juhapekka 2009. Sähköisen viestinnän tietosuoja. 2 p. Helsinki. Talentum.

L1061/1978. Laki sopimattomasta menettelystä elinkeinotoiminnassa. 22.12.1978.

L1113/1990. Uhkasakkolaki. 14.12.1990.

L39/1889. Rikoslaki. 19.12.1889.

L516/2004. Sähköisen viestinnän tietosuojalaki. 16.6.2004.

L731/1999. Suomen perustuslaki. 11.6.1999.

L759/2004. Laki yksityisyyden suojasta työelämässä. 13.8.2004.

Liikenne- ja viestintävaliokunnan mietintö 19/2008 vp. LiVM 19/2008.

Nyblin, Klaus 2009. Työelämän sähköposti. 3 p. Helsinki. Talentum.

Nyyssölä, Mikko 2009. Yksityisyyden suoja työsuhteessa. 5p. Helsinki. WSOYpro.