T-110.454 - Tietoturvallisuuden kehittämisprosessi
Yksityisyyden suojaa koskevat säädökset ja niiden merkitys pienten ja keskisuurten yritysten tietoturvallisuuden kehittämisprosessissa

Antti Nummiaho, 48004M, anummiah@cc.hut.fi

26. toukokuuta 2003

Sisältö

1 Tiivistelmä

Perustuslain 10 §, rikoslain 38:3 § ja 38:4 §, laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta, henkilötietolaki sekä laki yksityisyyden suojasta työelämässä ovat ne säädökset, jotka lähinnä koskevat yksityisyyden suojaa. Näistä yksityisyyden suojan kannalta keskeisimpiä ovat henkilötietolaki ja laki yksityisyyden suojasta työelämässä. Näiden merkitys tietoturvallisuuden kehittämisprosessissa näkyy ennen kaikkea henkilötietojen keräämisessä ja käsittelyssä sekä siinä millaista työntekijöiden testaamista ja teknistä valvontaa työnantaja voi suorittaa.

2 Johdanto

Tietoturvallisuuden järjestelmällinen ja kokonaisvaltainen kehittäminen on ainut keino parantaa pienen tai keskisuuren yrityksen tietoturvallisuuden tasoa pitkällä aikavälillä. Yrityksen tietoturvallisuus tulee nähdä kokonaisuutena, joka on yhtä vahva kuin sen heikoin lenkki, jos sitäkään. Yksityisyyden suojaa koskevat säädökset ovat pieni, mutta tärkeä osa tätä kokonaisuutta.

3 Yksityisyyden suojaa koskevat säädökset

Yksityisyyden suojaa koskevat lähinnä seuraavat säädökset:

- perustuslain 10 §
- rikoslain 38:3 § ja 38:4 §
- laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta
- henkilötietolaki
- laki yksityisyyden suojasta työelämässä

Näistä keskeisessä asemassa ovat erityisesti henkilötietolaki ja laki yksityisyyden suojasta työelämässä. Seuraavissa luvuissa käsitellään tarkemmin kutakin lakia ja sen merkitystä yrityksen tietoturvallisuuden kannalta.

4 Perustuslain 10 §

Perustuslain 10 §:n mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton sen mukaan kuin lainsäädännössä tarkemmin säädetään. Keskeistä on siis se, onko viestin lähettäjä tarkoittanut viestin luottamukselliseksi vai ei. Yleensä esimerkiksi sähköpostiviesti on tarkoitettu luottamukselliseksi, mutta uutisryhmiin lähetetty viesti ei ole. [1, 2]

Seuraavissa luvuissa tarkasteltavat lait tarkentavat perustuslain 10 §:ää eri tavoin. Laki yksityisyyden suojasta työelämässä tarkentaa sitä erityisesti työelämän tilanteiden osalta.

5 Rikoslain 38:3 § ja 38:4 §

Rikoslain 38:3 § ja 38:4 § käsittelevät viestintäsalaisuuden eli kansanomaisemmin kirjesalaisuuden loukkausta. Niiden tarkoitus on toisaalta ehkäistä ennalta tietoturvallisuusrikoksia ja toisaalta antaa rikoksen kohteiksi joutuneille lailliset mahdollisuudet korvausten saantiin. [3, 4]

38:3 §:n mukaan on rangaistavaa oikeudettomasti [3]

- avata toiselle osoitettu kirje tai muu suljettu viesti
- hankkia tietoa sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä
- hankkia tietoa televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä tai tällaisen viestin lähettämisestä tai vastaanottamisesta

Työnantajan valvontavalta voidaan kuitenkin katsoa oikeuttamisperusteeksi. Sekään ei kuitenkaan oikeuta yksityisten viestien kirjesalaisuuden loukkausta. Viestin yksityisen luonteen pitää kuitenkin ilmetä viestistä selkeästi (esimerkiksi otsikossa). Myös työntekijän suostumus, kuten asiasta tehty sopimus, toimii oikeuttamisperusteena. [2]

On myös huomattava, että viestintäsalaisuuden loukkaus edellyttää, että viestit on suojattu ulkopuolisilta. Tämä jo edellyttää jonkinlaisten salausteknisten ratkaisujen käyttöönottoa yrityksen tietoturvallisuuden kehittämisprosessissa.

Rikoslain 38:4 § kertoo milloin viestintäsalaisuuden loukkaus on törkeä. Sen perusteella voidaan määrätä ankarampia rangaistuksia kuin 38:3 § perusteella. Viestintäsalaisuuden loukkaus on törkeä, jos [3]

- rikoksentekijä käyttää rikoksen tekemisessä hyväksi asemaansa teleyrityksen palveluksessa tai muuta erityistä luottamusasemaansa
- rikoksentekijä käyttää rikoksen tekemistä varten suunniteltua tai muunnettua tietokoneohjelmaa tai teknistä erikoislaitetta tai rikos muuten tehdään erityisen suunnitelmallisesti
- rikoksen kohteena oleva viesti on sisällöltään erityisen luottamuksellinen
- teko huomattavasti loukkaa yksityisyyden suojaa ja viestintäsalaisuuden loukkaus on myös kokonaisuutena arvostellen törkeä

6 Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta

Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta eli kansantajuisemmin televiestinnän tietosuojalaki säädettiin 22.4.1999. Sen mukaan televiestintä on luottamuksellista, ellei sitä ole tarkoitettu yleisesti vastaanotettavaksi. Televiestinnällä tarkoitetaan millä tahansa teknisellä apuvälineellä, kuten kännykällä tai sähköpostilla, tapahtuvaa viestintää. Lähtökohtaisesti viestintä tulkitaan luottamukselliseksi, jos siihen osallistumista on rajoitettu. Esimerkiksi neuvottelupuhelut ja videokonferenssit ovat siis yleensä luottamuksellisia. Viestintään osallistumisen rajoittamattomuus merkitsee sen luottamuksellisuuden poistamista. [5, 6]

Laissa määrätään myös, että se, joka on ottanut vastaan tai muutoin saanut tiedon luottamuksellisesta televiestistä, jota ei ole hänelle tarkoitettu, ei saa oikeudettomasti ilmaista tietoa televiestin sisällöstä tai käyttää hyväksi tietoa televiestin sisällöstä tai sen olemassaolosta. [5]

7 Henkilötietolaki

Henkilötietolaki säädettiin 1.6.1999 EU:n tietosuojadirektiivin johdosta korvaamaan vanha henkilörekisterilaki. Henkilötietolakia sovelletaan henkilötietojen keräämiseen ja käsittelyyn. Henkilötiedolla tarkoitetaan mitä tahansa henkilöä tai hänen ominaisuuksiaan kuvaavaa merkintää, joka voidaan tunnistaa kyseistä henkilöä koskevaksi. Keskeisiä henkilötietoja ovat mm. nimi ja sosiaaliturvatunnus. [7, 8]

Henkilötietojen käsittelyssä on noudatettava seuraavia yleisiä velvoitteita: [7]

- huolellisuusvelvoite
- henkilötietojen käsittelyn suunnittelu
- käyttötarkoitussidonnaisuus
- tarpeellisuusvaatimus
- virheettömyysvaatimus

Huolellisuusvelvoite edellyttää, että henkilötietojen käsittelyssä on noudatettava huolellisuutta ja hyvää tietojenkäsittelytapaa. Yksityiselämän ja yksityisyyden suojaa ei saa loukata. [7]

Henkilötietojen käsittelyn suunnittelun lähtökohtana on puolestaan se, että henkilötietojen käsittely on perusteltua rekisterinpitäjän toiminnan kannalta. Myös henkilörekisterin tarkoitus ja se, mistä tietoja hankitaan ja mihin niitä luovutetaan, on määritettävä ennen henkilörekisterin perustamista. [7]

Käyttötarkoitussidonnaisuus tarkoittaa sitä, että kerättyjä tietoja saa käyttää vain siihen tarkoitukseen, jota varten ne on kerätty (rekisterin tarkoitus). Yrityksen asiakasrekisterin tietoja ei siis saa käyttää esimerkiksi syntymäpäiväonnittelujen lähettämiseen, jos kyseistä tarkoitusta ei ole määritetty ennen tietojen keräämistä. [7]

Rekisteriin kerättävien tietojen tulee myös olla rekisterin tarkoitukseen nähden tarpeellisia. Lisäksi on huolehdittava siitä, ettei käsitellä virheellisiä, epätäydellisiä tai vanhentuneita tietoja. Se, että käsiteltävät tiedot ovat aina ajan tasalla, vaatii tarkkaa suunnittelua ja huolellista tietojen käsittelyä. [7]

Erityistä huomiota on kiinnitettävä arkaluonteisten tietojen, kuten sairaustietojen ja henkilötunnuksen käsittelyyn, sillä tämä on pääsääntöisesti kielletty, ellei rekisteröity ole antanut nimenomaista suostumustaan. [7]

Mitään henkilötietoja ei saa kerätä tai käsitellä ilman laillista perustetta. Laillisiin perusteisiin kuuluvat: [7]

- rekisteröidyn suostumus tai toimeksianto
- tiedon käsittely on tarpeen rekisteröidyn elintärkeän edun suojaamiseksi
- käsittelystä on säädetty laissa
- rekisteröidyllä on asiakas- tai palvelussuhteen tms. perusteella asiallinen yhteys rekisterinpitäjän toimintaan
- kyse on yrityksen tms. asiakkaita tai työntekijöitä koskevista tiedoista ja tietoja käsitellään yrityksen sisällä
- tiedon käsittely on tarpeen rekisterinpitäjän toimesta tapahtuvaa maksupalvelua, tietojenkäsittelyä tms. varten
- tieteellinen tutkimus, tilastointi yms. ovat myös tietyin edellytyksin hyväksyttäviä perusteita henkilötietojen käsittelylle

Jokaisesta henkilörekisteristä on laadittava rekisteriseloste, josta ilmenee: [7]

- rekisterinpitäjän nimi ja yhteystiedot
- henkilötietojen käsittelyn tarkoitus

- kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista
- mihin tietoja luovutetaan
- kuvaus rekisterin suojauksen periaatteista

Rekisteriselosteessa on kerrottava luovutetaanko tietoja EU:n ulkopuolelle, sillä tämä on sallittu ainoastaan, jos ko. maassa on taattu tietosuojan riittävä taso. Lisäksi on siis laadittava kuvaus siitä, miten henkilötiedot on suojattu niin, että niihin pääsevät käsiksi vain ne, joilla on siihen oikeus. Vaadittava suojauksen taso riippuu rekisterin luonteesta. Esimerkiksi yrityksen asiakasrekisteri vaatinee yleensä vahvaan todentamiseen perustuvaa pääsynvalvontaa, kun taas yrityksen työntekijöiden muodostaman valokuvauskerhon jäsenrekisterin suojaamiseen riittänee vähempikin. [7]

Lähtökohtaisesti rekisteriselosteen on oltava jokaisen saatavilla. Jokainen henkilö on myös pääsääntöisesti oikeutettu tietämään, mitä häntä koskevia tietoja henkilörekisteriin on talletettu. Henkilötietolain noudattamista valvovat tietosuojavaltuutettu ja tietosuojalautakunta. [7]

Käytännössä jokainen yritys kerää ja käsittelee työntekijöitään, asiakkaitaan yms. koskevia henkilötietoja ja on näin velvollinen noudattamaan henkilötietolaissa määrättyjä asioita. Näin henkilötietolakia voidaan tarvittaessa käyttää myös motivoimaan sellaisen yrityksen johtoa, jonka mielestä yrityksellä ei ole mitään salattavaa eikä näin mitään tarvetta tietoturvallisuuden kehittämistyölle.

8 Laki yksityisyyden suojasta työelämässä

Laki yksityisyyden suojasta työelämässä eli ns. työelämän tietosuojalaki säädettiin 8.6.2001 täydentämään aiemmin säädettyä henkilötietolakia. Se ottaa kantaa ennen kaikkea siihen millaista työntekijöiden teknistä valvontaa ja testaamista työnantaja voi harjoittaa. Lain lähtökohtana on, että työnantaja saa kerätä, tallentaa ja muokata vain välittömästi työsuhteen kannalta tarpeellisia tietoja eikä tästä voida poiketa edes työntekijän suostumuksella. Tiedot on kerättävä pääasiassa työntekijältä itseltään. Tietyissä laissa erikseen mainituissa poikkeustapauksissa tietoja voidaan kerätä muualtakin, kunhan tästä tiedotetaan työntekijälle. Tällaisia poikkeuksia ovat esimerkiksi työntekijän luotettavuuden selvittäminen ja työnantajan asiakassuhteiden turvaaminen. [9]

Tekninen valvonta käsittää mm. työntekijän sähköpostiviestien ja WWW:n käytön seurannan. Laki edellyttää, että työnantaja ja työntekijä sopivat näistä asioista yhteistoimintamenettelyssä. Työnantajan on määriteltävä valvonnan tarkoitus ja siinä käytettävät menetelmät ja niistä on tiedotettava henkilöstölle. [9]

Aiemmin tässä esseessä käsiteltyjen lakien tapaan myös laki yksityisyyden suojasta työelämässä painottaa sitä, että työntekijän yksityisluonteisten luottamuksellisten viestien salaisuutta sähköpostin ja tietoverkon käytössä ei saa vaarantaa. Käytännössä, jos työntekijän sähköpostiviestintää halutaan seurata, tämä edellyttää sitä, että joko sähköpostin käyttö yksityisiin tarkoituksiin kielletään tai yksityisiin tarkoituksiin ja työtehtäviin käytetään eri osoitteita. Yksityisiin tarkoituksiin voidaan käyttää esimerkiksi tyyppiä etunimi.sukunimi@yritys.fi olevia sähköpostiosoitteita ja työtehtäviin tyyppiä toimenkuva@yritys.fi olevia osoitteita. Esimerkiksi webmaster@yritys.fi on tyypillinen esimerkki jälkimmäisestä. Jos työntekijä nimittäin joutuu käyttämään samaa osoitetta yksityisiin ja työtehtäviin liittyviin viesteihin ja työtehtäviin liittyviä viestejä halutaan seurata esimerkiksi työntekijän ollessa lomalla, ei tämä onnistu vaarantamatta yksityisluonteisten viestien salaisuutta. Tällöin nimittäin joudutaan päättelemään viestin luonne otsikosta ja lähettäjästä ja ehkä jopa lukemaan muutama rivi viestin alusta.

Laki edellyttää myös, että testattaessa työntekijöitä henkilö- ja soveltuvuusarvioinneilla on varmistuttava siitä, että testimenetelmä on luotettava, testaaja asiantunteva ja testitulos virheetön. Työnantaja ei myöskään saa käsitellä tai kerätä työntekijän terveydentilaa koskevia tietoja ilman työntekijän suostumusta ja tällöinkin vain, jos niiden käsitteleminen on tarpeen esimerkiksi sairausajan palkan maksamiseksi tai jos se perustuu muuhun lainsäädäntöön. Terveydentilan tarkastamiseen sekä

huume- ja alkoholitesteihin (puhalluttamista lukuunottamatta) on käytettävä aina terveydenhuollon ammattihenkilöitä ja palveluita. [9]

Lain lisäksi keskeisessä asemassa ovat yrityksen omat selkeät, yksikäsitteiset ohjeet, jotka ottavat kantaa myös sellaisiin seikkoihin, kuten työnantajan oikeuteen käyttää teknistä valvontaa ja valvoa sähköpostin ja tietoverkon käyttöä, joista lainsäädännössä ei ole toistaiseksi määrätty.

Laki yksityisyyden suojasta työelämässä koskee kaikkia palvelussuhteita ja myös työnhakijoita. Sitä valvovat tietosuojavaltuutettu ja työsuojeluviranomaiset. [9]

9 Yhteenveto

Tässä esseessä käsiteltiin seuraavia yksityisyyden suojaa koskevia säädöksiä yleisesti ja erityisesti yrityksen tietoturvallisuuden kannalta: perustuslain 10 §, rikoslain 38:3 § ja 38:4 §, laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta, henkilötietolaki sekä laki yksityisyyden suojasta työelämässä.

Perustuslain 10 §:n keskeiseksi sanomaksi nähtiin se, että luottamuksellisen viestin salaisuus on loukkaamaton. Tämä ajatus toimii punaisena lankana muissa käsitellyissä laeissa, jotka tarkentavat perustuslain 10 §:ää eri tavoin.

Rikoslain 38:3 §:n ja 38:4 §:n todettiin käsittelevän viestintäsalaisuuden loukkausta. Viestintäsalaisuuden loukkauksen todettiin edellyttävän, että viestit on suojattu ulkopuolisilta.

Lain yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta todettiin puolestaan käsittelevän televiestinnän luottamuksellisuutta. Todettiin, että sen mukaan televiestintä on luottamuksellista, ellei sitä ole tarkoitettu yleisesti vastaanotettavaksi.

Keskeisimmiksi yksityisyyden suojaa koskeviksi säädöksiksi nähtiin henkilötietolaki ja laki yksityisyyden suojasta työelämässä. Henkilötietolain todettiin ottavan kantaa henkilötietojen keräämiseen ja käsittelyyn ja lain yksityisyyden suojasta työelämässä työntekijöiden testaamiseen ja siihen millaista työntekijöiden teknistä valvontaa työnantaja voi suorittaa.

Viitteet

[1] Suomen perustuslaki - Perustuslain teksti, 11.6.1999 [viitattu 26.5.2003]
URL: http://www.om.fi/perustuslaki/3312.htm

[2] Törnqvist I., Työntekijän sähköposti- ja Internet-liikenteen valvonta,
11.9.2002 [viitattu 26.5.2003]
URL: http://myy.helia.fi/ torir/laki/ttnoikeudet.htm

[3] Heikniemi J., Suomen rikoslaki, 38 luku, 1.1.2002 [viitattu 26.5.2003]
URL: http://www.heikniemi.net/rikoslaki/rl38.html

[4] Koukkula H., T-110.454 - TKK - Kevät 2003 - Luentokalvot, 31.3.2003 [viitattu 26.5.2003]
URL: http://www.tcm.hut.fi/Opinnot/T-110.454/2003/luentokalvot2003-1.pdf

[5] Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta,
22.4.1999 [viitattu 26.5.2003]
URL: http://www.finlex.fi/linkit/ajansd/19990565

[6] Korpela J., Tietosuojavaltuutetun kannanotto sähköpostin käytöstä työpaikalla,
5.10.1999 [viitattu 26.5.2003]
URL: http://www.cs.tut.fi/ jkorpela/tsv1999.html

[7] Henkilötietolaki, 22.4.1999 [viitattu 26.5.2003]
URL: http://www.finlex.fi/linkit/ajansd/19990523

[8] Korpela J., Henkilörekistereistä lain kannalta, 24.3.2003 [viitattu 26.5.2003]
URL: http://www.cs.tut.fi/ jkorpela/hlorek.html

[9] Laki yksityisyyden suojasta työelämässä, 8.6.2001 [viitattu 26.5.2003]
URL:http://www.finlex.fi/linkit/ajansd/20010477