Milla Ohinen

# Työntekijän yksityisyydensuoja

Tietosuoja-asetuksen asettamat velvollisuudet työnantajalle

Julkisoikeuden pro gradu -tutkielma
Johtamisen yksikkö

Vaasa 2022

**VAASAN YLIOPISTO**
**Julkisoikeuden pro gradu -tutkielma**
**Tekijä:** Milla Ohinen
**Tutkielman nimi:** Työntekijän yksityisyydensuoja : Tietosuoja-asetuksen asettamat velvollisuudet työnantajalle
**Tutkinto:** Hallintotieteiden maisteri
**Oppiaine:** Johtamisen akateeminen yksikkö
**Työn ohjaaja:** Niina Mäntylä
**Valmistumisvuosi:** 2022 **Sivumäärä:** **71**

**TIIVISTELMÄ :**

Työelämän yksityisyydensuoja on vahvistunut Euroopan Unionin yleisen tietosuoja-asetuksen (679/2016) voimaan tulon myötä. Asetus velvoittaa kaikkia EU:n jäsenvaltioita sellaisenaan sekä vahvistaa kansallista tietosuojalainsäädäntöä. Asetus on vahvistanut työntekijöiden oikeuksia yksityisyyteen sekä parempaan omien henkilötietojen hallintaan. Työntekijä on oikeutettu yksityisyyteen työpaikalla tapahtuvassa henkilötietojen käsittelyssä. Samalla asetus on puolestaan tuonut rekisterinpitäjille, työnantajalle lisää velvoitteita henkilötietojen käsittelyyn. Työnantajan on kaikessa henkilötietojen käsittelyssä toimittava voimassa olevan tietosuojalainsäädännön ja tietosuojaperiaatteiden mukaisesti. Kansallisesti työntekijöiden yksityisyyttä turvaa asetuksen lisäksi muun muassa tietosuojalaki (1050/2018) sekä laki yksityisyyden suojasta työelämässä (759/2004).

Työnantajan on luotava tietosuojalainsäädännön mukaiset prosessit jo siinä vaiheessa, kun se edes suunnittelee henkilötietojen käsittelyä ja keräämistä. Tietosuojalainsäädännön mukaiset prosessit pitävät sisällään myös sen, että tekniset aspektit, kuten tietojärjestelmät ovat tietoturvalliset lainsäädännön mukaisesti. Työnantaja on lakisääteisesti velvoitettu keräämään työntekijöistä tiettyjä henkilötietoja, mutta sen on aina henkilötietoja käsiteltäessä huolehdittava tarpeellisuusvaatimuksen toteutumisesta. Lähtökohtaisesti työntekijöiden arkaluontoisten tietojen käsittely ja kerääminen on kiellettyä, mutta on tilanteita, jolloin työnantajalla on oikeus käsitellä arkaluontoisia henkilötietoja, kuten terveystietoja. Työntekijöiden tekninen valvonta, kuten paikannustietojen seuranta voi tietyissä tilanteissa olla perusteltua. Työnantajan on kuitenkin aina huolehdittava, että se on työtehtävän suorittamisen kannalta perusteltua ja tarpeellista. On aina rekisterinpitäjän, työnantajan vastuulla huolehtia, että se ei kerää työntekijästä sijaintitietoja epähuomiossa.

Tietosuoja-asetus on tuonut jäsenvaltioille asetuksen vastaisesta henkilötietojen käsittelystä myös tarkemman sääntelyn tietoturvaloukkausten menettelylle sekä mahdollisuuden huomattavan korkeisiin hallinnollisiin seuraamusmaksuihin. Tietoturvaloukkaus muodostuu aina siinä vaiheessa, kun rekisteröidyn työntekijän henkilötietoja käsitellään voimassa olevan lainsäädännön vastaisesti. Mikäli rekisteröidylle aiheutuu tietoturvaloukkauksen myötä huomattavaa haittaa, kansallinen valvontaviranomainen voi määrätä rekisterinpitäjälle huomattavat hallinnolliset sakot. Työnantajan on rekisterinpitäjänä huolehdittava tarpeellisista toimista tietoturvaloukkauksen sattuessa, kuten ilmoitusvelvollisuuden täyttämisestä sekä riittävästä dokumentoinnista.

**AVAINSANAT:** Yksityisyydensuoja työelämässä, tietosuoja, henkilötieto, arkaluontoinen henkilötieto, työntekijän tekninen valvonta, tietoturvaloukkaus, korvausvastuu

## Sisällys

## LYHENTEET

EU Euroopan Unioni

EIT Euroopan ihmisoikeustuomioistuin

EIS Euroopan ihmisoikeussopimus

HE Hallituksen esitys

HaVM Hallintovaliokunnan mietintä

TSV Tietosuojavaltuutettu

KKO Korkein oikeus

HO Hallinto oikeus

TT Työtuomioistuin

# 1 JOHDANTO

Teknologia kehittyy, internet laajenee, maailma kansainvälistyy. Minkä tahansa yrityksen tai organisaation internetsivuille kirjaudummekaan, meistä jää aina jälki heidän tietoihinsa. Työsuhteen solmiminen ja työsuhteessa oleminen on meille kaikille, ainakin jossakin vaiheessa elämää, ajankohtainen ja eteen tuleva asia. On tärkeää, että työnantaja käsittelee oikein ja tarkoituksenmukaisesti työntekijöiden tietoja ja erityisesti mahdollisia arkaluontoisia tietoja. Vuonna 2012 tietosuojavaltuutetun toimisto tutki, kuinka hyvin suomalaiset yritykset ja yhtiöt ottavat huomioon henkilötietolainsäädännön asettamat vaatimukset verkkopalveluissa. Tarkastuksen alaisina olleet yritykset ja yhtiöt olivat olleet aikaisempana vuonna jonkinlaisen tietoturvaloukkauksen kohteena. Hälyttävää vastauksissa oli se, että ainoastaan 46 % yrityksistä olivat tietoisia henkilötietolain (523/1999) asettamista vaatimuksista. Lisäksi 30 % yrityksistä tiedotti, että he eivät olleet tehneet minkäänlaisia muutoksia tietoturvaloukkauksen jälkeen.[1]

Yksityisyyden suoja on kaikille kuuluva perusoikeus, josta säädetään laajasti lainsäädännössä. Tietosuojalaki (1050/2018), laki yksityisyyden suojasta työelämässä (759/2004) sekä kansainväliset sääntelyt suojaavat työntekijän yksityisyyttä. Euroopan unionin perusoikeuskirjan (2012/C 326/02) 8 artikla turvaa kansainvälisesti henkilötietojen suojaa yksityiselämää kunnioittaen. Artikla antaa puitteet lainsäädännölle siitä, että henkilötietojen hankkimisesta, käsittelystä sekä säilömisestä on säädettävä tarpeeksi huolellisesti.[2]

Teknologian kehittyessä yksityisyyden suojaa on säädetty turvaamaan EU:n tietosuoja-asetus (679/2016) General Data Protection Regulation, joka on vaikuttanut laajasti EU:n kansalaisten yksityisyyden suojaan ja yritysten henkilötietojen käsittelyyn. Asetus velvoittaa kaikkia EU:n jäsenmaita suoranaisesti, ja yksi sen tavoitteista onkin ollut yhtäläistää kaikkien jäsenvaltioiden tietosuojalakeja. Tarkoituksena on myös se, että palveluja on helpompi toteuttaa kansainvälisesti, kun jäsenmailla on yhtäläiset velvollisuudet

[1] Pitkänen ym. 2013: 9.
[2] Pitkänen ym. 2013: 19–20.

yksilöiden yksityisyyden- ja tietosuojaan. [3] EU on noteerannut teknologian pikaisen kansainvälisen kehittymisen ja tietosuoja-asetuksen roolina onkin edistää EU:n tietosuojalainsäädännön uudistamista.[4]

Teknologia on kehittynyt valtavasti kansallisten lakien säätelystä, joten tietosuoja-asetuksella pyritään turvaamaan paremmin nykyajan henkilötietojen käsittelyä. Edellinen vastaavanlainen säädös, henkilötietodirektiivi on otettu voimaan vuonna 1995. Näin ollen Euroopan komissio ehdotti vuonna 2012 uutta tietosuoja-asetusta, jotta säädökset pysyisivät ajantasaisina nykyajan hyvin erilaisessa teknisessä toimintaympäristössä.[5]

Asetus koskettaa laajasti luonnollisia henkilöitä ja tahoja, jotka ylläpitävät henkilöstörekistereitä. Tietosuojan tarkoituksena on kasvattaa henkilötietojen käsittelyn avoimuutta sekä vahvistaa luonnollisten henkilöiden mahdollisuuksia valvoa omia henkilötietojaan ja niiden käsittelyä.[6] Asetuksessa säädetään luonnollisten henkilöiden henkilötietojen prosessoinnista ja niiden lainmukaisesta käsittelystä. Yhtenä suurimpana muutoksena asetus on tuonut luonnollisille henkilöille laajemman ja vahvemman oikeuden omiin henkilötietoihin.

Jo ennen tietosuoja-asetusta kansallinen lainsäädäntö on turvannut työntekijöiden yksityisyydensuojaa. Asetus vaikuttaa laaja-alaisesti EU:ssa toimiviin organisaatioihin ja organisaatioiden onkin ollut tehtävä muutoksia omiin tietosuojakäytäntöihin.[7] Nyt tietosuoja-asetuksen myötä työntekijöiden oikeusturva ja yksityisyydensuoja on parantunut huomattavasti, mutta työnantajan vastuut ja velvollisuudet puolestaan jälleen kiristyneet entisestään. Työnantajat, erityisesti suuret työnantajat käsittelevät suuria määriä työntekijöiden henkilötietoja, joten oletettavasti asetus on vaatinut muutoksia työnantajien prosesseihin. Suomen laki ei esimerkiksi ennen vaatinut organisaatioita

[3] Hanninen ym. 2017: 13.
[4] HaVM 13/2018 & HE 9/2018.
[5] Pitkänen ym. 2013: 26.
[6] Oikeusministeriö 2017: 9.
[7] Hanninen ym. 2017: 13.

nimeämään tietosuosuojavastaavaa. Asetuksen myötä työnantajien on rekisterinpitäjinä nimettävä oma tietosuojavastaava. [8]

Tutkielma tarkastelee työntekijöiden nykyistä oikeutta yksityisyydensuojaan sekä työnantajien velvollisuuksia tietosuojassa.

### 1.1 Tutkimusmetodi, rakenne ja aineisto

Tutkielman tutkimusmenetelmänä toimii lainoppi eli oikeusdogmaattisuus. Lainoppi tutkii voimassa olevaa oikeutta sekä lain ja muiden oikeuslähteiden merkittävyyttä. Muilla oikeuslähteillä tarkoitetaan esimerkiksi lainvalmistelumateriaaleja, Euroopan Unionin tuomioistuimen tai kansallisten tuomioistuimien päätöksiä ja ratkaisuja, joista muodostuu voimassa olevaa oikeuskäytäntöä. Lainvalmistelumateriaalilla tarkoitetaan muun muassa hallituksen esityksiä eduskunnalle. [9] Lainoppi tutkimusmetodina tutkii normilinjauksia sekä tulkinnan myötä vakiintuneita linjauksia.[10] Lainopin perimmäinen tarkoitus on kuitenkin tutkia ja selvittää oikeusnormien sisällön perimmäinen merkitys tulkintakannanottojen kautta.[11] Oikeusdogmaattisuus nousee esiin lisäksi tutkielman lähteistä, jotka pohjautuvat pitkälti oikeuskirjallisuuteen, voimassa olevaan lainsäädäntöön sekä kansalliseen ja kansainväliseen oikeuskäytäntöön.

Tutkimuksen aineisto painottuu EU:n yleiseen tietosuoja-asetukseen, kansalliseen tietosuojalakiin, perustuslakiin, työoikeuteen, lakiin yksityisyydensuojasta työelämässä sekä kansalliseen ja kansainväliseen oikeuskäytäntöön. Kansallisen oikeuskäytännön aineistona tutkimuksessa toimivat tuomioistuinratkaisut sekä kansallisen tietosuojaviranomaisen, tietosuojavaltuutetun toimiston ratkaisut. Kansainvälistä oikeuskäytäntöä puoltavat Euroopan ihmisoikeustuomioistuimen ratkaisut.

---

[8] Vainio 2017: 59.
[9] Hirvonen 2011: 23.
[10] Hirvonen 2011: 22.
[11] Hirvonen 2011: 24.

Johdannon jälkeen tutkimus käsittelee ensimmäisessä pääluvussa yleisesti kansainvälistä ja kansallista sääntelyä tietosuojaan ja yksityisyydensuojaan. Luvussa käsitellään tietosuojaa ohjaavat periaatteet, keskeisimmät käsitteet sekä keskiössä olevat kansalliset lait. Toinen luku perehtyy siihen, milloin työnantajalla on oikeus kerätä, käsitellä ja säilöä työntekijöidensä henkilötietoja. Osio tarkastelee lisäksi työnantajan velvollisuuksia rekisterinpitäjänä. Kolmannessa luvussa käsitellään arkaluontoisten henkilötietojen käsittelyä, missä tilanteissa työnantajalla on oikeus kerätä ja käsitellä esimerkiksi työntekijöidensä terveyttä koskevia tietoja. Neljäs kappale tarkastelee työpaikoilla tapahtuvaa teknistä valvontaa ja sähköistä viestintää. Kappale käsittelee tilanteita, milloin työnantajalla on oikeus valvoa työntekijöitänsä sähköisesti ja milloin puolestaan ei. Viimeinen pääkappale syventyy tietoturvaloukkauksiin sekä yksityisyyden laiminlyönnistä säädettyihin korvaus- ja rangaistusvaatimuksiin. Johtopäätökset kokoavat yhteen tutkimuksessa havaitut työntekijöiden pääasialliset oikeudet sekä työnantajan tärkeimmät velvollisuudet.

### 1.2 Tutkimusaihe ja kysymykset

Tutkielma käsittelee organisaation velvollisuuksia, työnantajan tietosuojavelvollisuuksia sekä luonnollisen henkilön, työntekijän oikeuksia omiin henkilötietoihin sekä työntekijän yksityisyydensuojaa. Tutkielma syventyy EU:n tietosuoja-asetuksen sekä kansallisen lainsäädännön asettamiin velvollisuuksiin työnantajalle sekä siihen, milloin ja missä tilanteissa työnantajalla on oikeus käsitellä työntekijän henkilötietoja. Tutkimuskysymyksinä toimivat siis nimenomaisesti, milloin ja millä perustein työnantaja on oikeutettu työntekijän henkilötietojen käsittelyyn sekä mitkä ovat kansallisen ja kansainvälisen lainsäädännön ja oikeuskäytännön velvollisuudet työntekijöiden henkilötietojen käsittelylle. Tarkastelen tutkimuksessa myös työnantajan oikeutta ja asetettuja velvollisuuksia työntekijöiden arkaluontoisten henkilötietojen käsittelyyn sekä oikeutta tekniseen valvontaan.

## 2 KANSALLINEN JA KANSAINVÄLINEN SÄÄNTELY

Henkilötietojen käsittely ja yksityisyydensuojan sääntely ulottuu Suomen perustuslakiin asti. Perustuslain (731/1999, PL) 10 §:n mukaisesti jokaisen yksityiselämä, kunnia ja kotirauha tulee olla suojattu ja henkilötietojen tarkemmasta sääntelystä tulee säätää erikseen lailla. Tämä sovitettiin mukaan perustuslakiin perusoikeusuudistuksen yhteydessä, jossa yhdenmukaistettiin perustuslaki ja Euroopan ihmisoikeussopimus. Suomi on velvollinen yhdenmukaistamaan kansallisten lakien tulkinnat ihmisoikeussopimukseen Euroopan ihmisoikeustuomioistuimen tuomion uhalla.[12] Perustuslaissa henkilötietojen suoja on yhdistetty osaksi yksityiselämää, vaikka se sisältää huomattavasti laajemman alan.[13] Henkilötietosuojaa ei nähdä omana perusoikeutenaan, vaan se rinnastetaan osaksi yksityisyyden suojaa. Henkilötietojen suojaan luetaan mukaan tietosuoja, arkaluontoiset tiedot sekä muut periaatteet. Näin ollen henkilötietojen suoja olisi omana perusoikeuden pykälänä liian tekninen kokonaisuus.[14]

Keskeisimmät lait työelämän yksityisyydensuojaan ovat tietosuojalaki, laki yksityisyydensuojasta työelämässä sekä sähköisen viestinnän palveluista annettu laki. Tietosuojalaki on säädetty tarkentamaan EU:n tietosuoja-asetusta luonnollisten henkilöiden tietojenkäsittelystä. Tietosuojalaki on korvannut aikaisemmin kansallisen henkilötietolain.[15]Laki yksityisyyden suojasta työelämässä turvaa luonnollisesti työntekijöiden yksityisyyttä ja henkilötietoja työsuhteessa. Eduskunnan antaman päätöksen mukaan lakiin on tehty muutoksia vuonna 2019 liittyen direktiivin ja tietosuoja-asetuksen tuomiin muutoksiin. Sähköisen viestinnän palveluista annetun lain pääasiallisena tavoitteena on lisätä tarjontaa sähköisiin palveluihin, mutta olennaista myös turvata viestinnän ja palveluiden luottamuksellisuutta ja varmistaa se, että yksityisyydensuoja toteutuu myös sähköisessä viestinnässä.

[12] Neuvonen 2014: 39.
[13] Pitkänen ym. 2013: 15–16.
[14] Neuvonen 2014: 41.
[15] HaVM 13/2018 & HE 9/2018.

Kansainvälisesti yksityisyyden suoja on turvattu jo alun alkaen YK:n ihmisoikeusjärjestelmän yleissopimuksessa. Merkittävimpinä kansainvälisinä yksityisyydensuojan turvaajina toimii tietosuoja-asetus, Euroopan ihmisoikeussopimus sekä Euroopan tuomioistuinkäytäntö. EU:n tuomioistuimen oikeuskäytäntö on merkityksellinen osa tietosuojalainsäädännön tulkintaa. EU:n tuomioistuimen oikeuskäytäntö on oikeudellisesti jäsenvaltioita velvoittava. Tietosuoja-asetusta on kritisoitu sen vaikeaselkoisuudesta ja tulkinnanvaraisuudesta. EU:n tuomioistuimella on merkittävä rooli tulkintojen ja vaikeaselkoisten rakojen täyttämisessä.[16] Kansainvälisesti EU:n sisällä myös Euroopan tietosuojaneuvostolla on merkittävä rooli. Neuvoston pääasiallisena tehtävänä on antaa jäsenvaltioille ohjeita, tulkintoja ja suosituksia tietosuoja-asetuksen sisällöstä. [17]

## 2.1 Tietojenkäsittelyä ohjaavat käsitteet

Tietosuoja-asetuksessa henkilötiedot merkitsevät tietoja, jotka voidaan yhdistää tunnistettavaan luonnolliseen henkilöön, eli ihmiseen. Luonnollinen henkilö on tunnistettava silloin, kun häneen voidaan liittää esimerkiksi nimi, henkilötunnus tai taloudellinen tieto. Yksinkertaisesti kyseessä on henkilötieto, jos tiedon nojalla voidaan selvittää, kuka henkilö on kyseessä. Rekisteröidystä voidaan puolestaan puhua silloin, kun kyseessä on henkilö, jonka tietoja käsitellään. Henkilötietojen käsittely voi olla esimerkiksi luonnollisen henkilön tietojen keräilyä, säilömistä tai tallentamista. Myös henkilötietojen muokkaaminen ja eri tietojen yhdistäminen toisiinsa luetaan henkilötietojen käsittelyksi.[18]

Tietosuoja-asetus ja nykyinen tietosuojalaki pohjautuvat rekisteriin, rekisterinpitäjään sekä henkilötietojenkäsittelijään. Rekisterillä tarkoitetaan henkilötietojen kerättyä kokoelmaa henkilötiedoista. Luonnollisesti rekisterinpitäjä, esimerkiksi viranomainen tai yritys ylläpitää rekisteriä henkilötiedoista. Rekisterinpitäjä tekee päätöksen, mitä tietoja on tarpeellista kerätä ja mihin näitä kerättyjä tietoja on tarpeellista käyttää. Henkilötietojenkäsittelijä puolestaan ei ole päätäntävaltainen tietojen keräämisestä tai siitä,

[16] Kurvinen 2021: 991.
[17] Kurvinen 2021: 993.
[18] Hanninen ym. 2017: 20–22.

kuinka niitä käytetään. Käsittelijän tehtävänä on käsitellä jo kerättyjä tietoja rekisterinpitäjän ohjeistuksen mukaan. [19]

## 2.2 Tietosuojaperiaatteet

Tietosuoja-asetus asettaa yleiset periaatteet, joita rekisterinpitäjän ja henkilötietojen käsittelijän on seurattava ja noudatettava henkilötietoja käsiteltäessä. Asetuksen määrittämät periaatteet ovat henkilötietojen tietojenkäsittelyn lainmukaisuus, läpinäkyvyys, kohtuullisuus, käyttötarkoitussidonnaisuus ja tietojen minimointi ja täsmällisyys. Lisäksi tietosuojaperiaatteita ovat myös tietojen säilyttämisen rajoittaminen ja luottamuksellisuus sekä osoitusvelvollisuus, joka on rekisterinpitäjän vastuulla. [20]

Lainmukaisuuden vaatimuksella tarkoitetaan selvästi sitä, että rekisterinpitäjän on toimittava Suomen lainsäädännön, tietosuoja-asetuksen sekä työehtosopimusten mukaisesti käsiteltäessä henkilötietoja. Läpinäkyvyydellä viitataan luonnollisesti siihen, että työntekijän henkilötietojen käsittelyn on oltava läpinäkyvää. Työntekijän tulisi olla tietoinen, kun työnantaja kerää tai käsittelee hänen henkilötietojaan. Käyttötarkoitussidonnaisuuden mukaisesti työnantaja on oikeutettu keräämään työntekijästä henkilötietoja silloin, kun niitä kerätään johonkin tiettyyn tarkoitukseen, joka on lainmukainen. Asetuksen mukaan työnantajan on ennalta selvitettävä, mitä varten se kerää työntekijän henkilötietoja. Työnantaja ei näin ole oikeutettu keräämään työnhakijasta tai työntekijästä mitä tahansa henkilötietoja, vaan tietojen on näin ollen oltava asianmukaisia. [21] Tietojen minimoinnin periaate eli tarpeellisuusvaatimus on yksi tärkeimmistä ja keskeisimmistä henkilötietojen käsittelyn periaatteista. Tarpeellisuusvaatimuksen mukaisesti rekisterin pitäjän on kerättävä työntekijästä mahdollisimman vähän tietoja. Tietosuoja-asetus korostaa tarpeellisuusvaatimuksen merkitystä, mutta se on ollut kansallisessa lainsäädännössä jo ennestään. Yksityisyyden suojasta työelämässä annetun lain

[19] Hanninen ym. 2017: 22–23.
[20] Talus ym. 2017: 12.
[21] Härkönen ym. 2022: 517.

mukaisesti työnantaja saa käsitellä välittömästi tarpeellisia tietoja työntekijästä. Lain 3 §:n mukaan tarpeellisuusvaatimuksesta ei ole oikeutta poiketa edes työntekijän suostumuksella. [22] Työntekijä voi työskennellä yrityksen sisällä eri työsuhteissa, joten työntekijän tietojen tarpeellisuutta tulee arvioida työsuhdekohtaisesti. Eri tehtävissä eri tiedot ovat tarpeellisia. Työnantajan tulee tämän lisäksi huomioida myös erot työnhakijoiden ja työntekijän välillä; työnhakijasta ei ole tarpeellista kerätä samoja tietoja kuin työsuhteeseen palkatulta työntekijältä. [23]

Tietosuojaperiaatteiden lisäksi asetus on tuonut mukanaan myös sisäänrakennetun ja oletusarvoisen tietosuojaperiaatteen. Sisäänrakennetulla periaatteella viitataan siihen, että yllä käsitellyt periaatteet aktiivisesti huomioidaan kaikessa henkilötietojen käsittelyssä sekä prosesseissa. Oletusarvoisuuden periaate puolestaan viittaa siihen, että rekisterinpitäjä käsittelee henkilötietoja oletusarvoisesti vain tiettyyn tarkoitukseen ja tarkoituksen mukaisesti vain tarpeellisia tietoja. Sekä sisäänrakennettu että oletusarvoinen periaate velvoittaa, että kaikki tietosuojaperiaatteet huomioidaan jo henkilötietojen käsittelyn ensimmäisessä vaiheessa. Henkilötietojen käsittelyn ensimmäisenä vaiheena voidaan pitää sitä, kun rekisterinpitäjä alkaa kehittelemään henkilötietojen keräämistä ja käsittelyä. Periaatteet on siis huomioitava esimerkiksi siinä vaiheessa, kun luodaan ja muodostetaan erilaisia järjestelmiä. [24]

### 2.3 Tietosuoja-asetus

Tietosuoja-asetuksen tavoitteena on parantaa luonnollisten henkilöiden henkilötietojen käsittelyä sekä antaa heille paremmat ja laajemmat oikeudet heidän omiin henkilötietoihinsa. Näin ollen asetuksella pyritään siis myös tasapainottamaan rekisterinpitäjien ja luonnollisten henkilöiden suurta eroa henkilötietoihin pääsyssä. Rekisterinpitäjille luodaan asetuksella selkeämmät ja yhtenäisemmät lailliset raamit henkilötietojen

[22] Nyyssölä 2020: 75–76.
[23] Nyyssölä 2020: 76–77.
[24] Talus ym. 2017: 13.

käsittelylle. Asetuksen tavoitteena on lisäksi parantaa henkilötietojen vapaata liikkuvuutta EU:n jäsenvaltioiden välillä sekä suojata paremmin luonnollisten henkilöiden verkko- ja internetkäyttäytymistä.[25] Kaiken kaikkiaan asetuksen perimmäisenä tarkoituksena on luoda EU:lle vahva ja laaja tietosuojalainsäädäntö nykyajan digitalisaatiossa. Asetus on jokaista jäsenmaata sitova sellaisenaan, vaikkakin se jättää tulkintavaraa jäsenmaille. Tarkoituksena on se, että jokainen jäsenvaltio voi itse kansallisella lainsäädännöllä täsmentää asetusta. Suomessa tietosuojalaki on säädetty täsmentämään asetuksen asettamia velvoitteita.[26]

Ennen tietosuoja-asetuksen voimaan tuloa jäsenvaltioiden tietosuojasäätelyä on turvannut henkilötietodirektiivi. Euroopan parlamentin ja neuvoston antama henkilötietodirektiivi 95/46/EY on Suomessa toimeen pantu henkilötietolailla vuonna 1999. Henkilötietodirektiivi on korvattu tietosuoja-asetuksella erityisesti kehittyvän teknologian takia ja verkkoympäristön kasvun takia. Tietosuoja-asetus on Suomessa toteutettu tietosuojalailla, ja näin ollen henkilötietolaki on kumottu. Yrityksille, viranomaisille ja muille rekisterinpitäjille asetus on tuonut lisäkustannuksia, jotka muodostuvat muun muassa uusista järjestelmistä sekä koulutuksien tarpeesta. Lisäkustannuksista huolimatta henkilötietojen käsittelyn lainsäädännön toteuttaminen sen vaatimalle tasolle lisää ihmisten luottamusta rekisterinpitäjiä kohtaan.[27]

Tietosuoja-asetus on jo itsessään jäsenvaltioita sitovampi kuin aikaisemmin annettu henkilötietodirektiivi. EU:n antamat asetukset ovat sitovia, ja näitä on toteutettava kokonaisuudessaan kaikissa jäsenvaltioissa. Direktiivit puolestaan antavat jäsenvaltioille tietyt tavoitteet ja päämäärät, johon niiden tulee ulottua. Jäsenvaltiot ovat vapaita itse määrittämään lait, joilla direktiivi pannaan täytäntöön. [28]

[25] Korpisaari ym. 2018: 34.
[26] Kurvinen 2021: 990–991.
[27] Korpisaari ym. 2018: 35–36.
[28] Euroopan Unioni: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_fi.

### 2.3.1 Oikeus omiin henkilötietoihin

Tietosuoja-asetus toi mukanaan laajemman oikeuden luonnollisille henkilöille, ja rekisteröidyillä on oikeus saada kaikki itseään koskevat henkilötiedot pyydettäessä. Itse henkilötietojen saamisen lisäksi rekisteröidyllä on oikeus saada tieto siitä, mihin tarkoitukseen hänen tietojaan käsitellään, ketkä osapuolet hänen tietojaan käsittelevät, yhteistyötahot, joille organisaatio on luovuttanut henkilötietoja ja tietojen säilytysajat. Lisäksi tietojen pyynnön yhteydessä, rekisterinpitäjän on ilmoitettava ja informoitava rekisteröityä hänen valitusoikeudestaan sekä valvontaviranomaisesta. [29] Rekisteripitäjän on välitettävä rekisteröidylle häntä koskevat henkilötiedot viimeistään yhden kuukauden sisällä siitä, kun se on vastaanottanut pyynnön. Rekisterinpitäjälle on tietyissä tilanteissa jätetty mahdollisuus pidentää tietojen toimittamisaikaa kahdella kuukaudella, jos tietojen saantipyyntö on esimerkiksi äärimmäisen laaja. Rekisterinpitäjän tulee ilmoittaa mahdollisesta määräajan pidentämisestä rekisteröidylle normaalin aikarajan puitteissa, eli yhden kuukauden sisällä. Rekisterinpitäjän on myös määritettävä ja osoitettava perusteet aikarajan pidentämiselle.[30]

Organisaation on tunnistettava rekisteröity aina, jos rekisteröity haluaa hyödyntää oikeuksiaan esimerkiksi tietojensaannin yhteydessä. Jos esimerkiksi työntekijä tai työnhakija pyytää kaikkien henkilötietojensa saamista, on työnantajan pystyttävä tunnistamaan henkilö oikeaksi. [31] Lähtökohtana toimii se, että rekisteröity esittää pyyntönsä kirjallisesti, yleensä sähköisessä muodossa.

Yleensä työnantaja luovuttaa henkilötietoja työntekijöistään muillekin tahoille, kuten työterveyshuollon tarjoajalle, palkanlaskennalle sekä vakuutuksien tarjoajille. Työntekijän pyytäessä kaikkia henkilötietoja on työnantajan annettava myös henkilötiedot, jotka se on luovuttanut muille organisaatioille. Työntekijä voi myös rajata

[29] Hanninen ym. 2017: 59–60.
[30] Talus ym. 2017: 24.
[31] Hanninen ym. 2017: 57.

tietojensaantipyynnön vain työnantajan hallussa oleviin tietoihin tai esimerkiksi vain rekrytointiprosessin aikaisiin haastattelumuistiinpanoihin.

Työnantajan on huolehdittava tietojen tietoturvallisesta toimittamisesta. Rekisteröidyn henkilötietojen lähettäminen pelkän sähköpostin välityksellä ei esimerkiksi ole kaikista tietosuojaystävällisin tapa. Tietoturvallisena tapana voidaan esimerkiksi pitää salatun muistitikun lähettämistä kirjattuna kirjeenä, jonka noutamiseen rekisteröidyn tulee näyttää henkilöllisyystodistus. Muistitikun salasanan lähettäminen voidaan puolestaan toteuttaa muun muassa salatun sähköpostin välityksellä.

### 2.3.2 Oikeus tulla unohdetuksi

Yhtä lailla kuin rekisteröidyllä on oikeus saada kaikki tiedot itsestään, on rekisteröidyllä myös oikeus tulla unohdetuksi. Tietosuoja-asetuksen 17 artikla määrittää luonnollisen henkilön, rekisteröidyn oikeuden tulla unohdetuksi.[32] Rekisteröidyllä on näin oikeus esittää organisaatiolle pyyntö omien henkilötietojensa poistosta. [33] Tietosuoja-asetus ei tarkkaan erittele, mitä tietojen poistolla tarkoitetaan ja mikä katsotaan asianmukaiseksi ja riittäväksi menettelyksi tietojen poistolle. Määrittely kuitenkin asettaa, että tietojen poiston jälkeen kukaan ei pääse niitä näkemään. [34]

Henkilötiedot tulee poistaa silloin, kun näiden säilyttämiseen ei ole enää tarvetta alkuperäiseen tarkoitukseen. [35] Työnantajalla voi kuitenkin olla lakisääteisiä perusteita tietojen sälyttämiselle, vaikka työnhakija tai työntekijä olisi tehnyt virallisen tietojen poistopyynnön. Monesti rekisteröidyt olettavat oikeutensa olevan hyvin suoraviivainen ja heillä on oikeus vaatia kaikki henkilötietonsa poistettaviksi. Työnantajalla on kuitenkin lakisääteisiä velvollisuuksia ja perusteita, joiden myötä kaikkia tietoja ei ole mahdollista poistaa edes pyynnöstä. Työnhakijan osalta lakisääteisiä perusteita voivat esimerkiksi olla se,

[32] Alén-Saavikko 2015: 414.
[33] Hanninen ym. 2017: 61.
[34] Korpisaari ym. 2022: 247–248.
[35] Korpisaari ym. 2022: 249.

että työnhakijalla on oikeus yhdenvertaisuuslain (1325/2014) ja lain naisten ja miesten tasa-arvosta (1986/609) perusteella haastaa työnantaja, jos hakija epäilee tulleensa syrjityksi hakuprosessin aikana. Työnhakijan on nostettava haaste kahden vuoden sisällä siitä, kun rekrytointiprosessi on päättynyt. Näiden mukaisesti työnantaja voi katsoa, että sillä on oikeus säilyttää rekrytointiprosessin tietoja kaksi vuotta prosessin päättymisen jälkeen, kuten tietoja-asetuksen artikla 17 määrittää.

Työnantajan on lisäksi huolehdittava tasaisin väliajoin työntekijöidensä henkilötietojen poistosta, kun tiedot eivät enää ole tarpeellisia. Työnantajan on siis aina huomioitava tietojen poistoajat sekä tietosuoja-asetuksen myötä rekisterinpitäjän on ilmoitettava säilytysajat rekisteröidylle.[36] Työntekijän tai jo lopettaneen työntekijän osalta työnantaja ei voi poistaa kaikkia tietoja edes pyydettäessä. [37] Työsopimuslain (2003/743) luvun 13 9§ mukaisesti työntekijän palkka vanhenee viiden vuoden jälkeen erääntymispäivästä. Työntekijällä on siis tämän nojalla oikeus pyytää työnantajalta tarkistusta palkkasaatavista vielä viiden vuoden kuluessa työsuhteen päättymisestä. Näin ollen työnantaja ei voi poistaa esimerkiksi työntekijän palkkatietoja, edes vaikka työntekijä pyytäisikin kaikkien henkilötietojensa poistoa. Jos työnantaja olisi poistanut työntekijän palkkatiedot, työnantaja ei voisi osoittaa myöhemmin, että palkka on maksettu työntekijälle oikein.

### 2.3.3 Tietojen oikaisu

Rekisterinpitäjän on oikaistava tietoja, jos rekisteröidyllä on tietokannassa virheellisiä henkilötietoja. Tietojen oikaisu perustuu tietosuoja-asetuksen 16 artiklaan sekä myös Euroopan Unionin perusoikeuskirja säätää tietojen oikaisemisesta. Rekisteröidyillä on oikeus tulla tarkasteltavaksi paikkansapitävien tietojen perusteella, esimerkiksi rekrytointiprosessissa tietojen oikeellisuus ja arviointi näiden perusteella on tärkeää. [38]

[36] Korpisaari ym. 2022: 211.
[37] Korpisaari ym. 2022: 107.
[38] Korpisaari ym. 2022: 241–242.

Rekisteröidyllä ei ole velvollisuutta antaa perustetta sille, miksi hän haluaa oikaista omia henkilötietojaan. Vaikka rekisteröidyllä ei ole perusteluvelvollisuutta, on hänen puolestaan pystyttävä näyttämään, että henkilötieto on virheellinen. [39]

[39] Korpisaari ym. 2022: 243.

# 3 TYÖNANTAJAN OIKEUS HENKILÖTIETOIHIN

On perusteltua, että työnantaja kerää työntekijästä henkilötietoja, ja myös työntekijän oikeuksien näkökulmasta tämä on olennaista työpaikan saamiseksi.[40] Työntekijän tietojen kerääminen alkaa väistämättä jo työhönottotilanteessa, eli jo rekrytointiprosessissa, kun työntekijä hakee kyseistä työpaikkaa. Jo itse työhönottotilanteessa työntekijä luovuttaa itsestään henkilötietoja, jotka ovat olennaisia työntekijän valinnassa ja riippuvaisia työpaikan saamiseksi, kuten työnhakijan aikaisempi työkokemus. Näin ollen sekä työnantajalla että työntekijällä itsellään on motivaatio kaventaa yksityisyydensuojaa. Vaikka molemmilla osapuolilla onkin kannustin yksityisyydensuojan alentamiseen, on tärkeää muistaa, että työnantaja on aina vahvempi osapuoli niin työhönottovaiheessa kuin työsuhteessakin.[41] Jo työnhakutilanteessa työnantajan on siis käsiteltävä mahdollisen tulevan työntekijänsä antamia tietoja henkilötietolain ja yleisten periaatteiden mukaisesti. [42]

Tietosuoja-asetuksen artikla 13 käsittelee rekisteröidyn suostumusta henkilötietojen käsittelyyn. Suostumuksella rekisteröity hyväksyy henkilötietojensa käsittelyn.[43] Erityisesti arkaluontoisten henkilötietojen käsittelyssä, joka perustuu työntekijän suostumukseen, on tärkeää huomioida se, että työnantaja on aina vahvempi osapuoli työntekijään nähden. Vahvemman ja heikomman osapuolen asetelma on siis tärkeää huomioida uusien prosessien tietosuoja-arvioinneissa.

## 3.1 Tietojenkäsittelijän vastuu ja velvollisuudet

Henkilötietoja käsittelee sekä rekisterinpitäjä että henkilötietojen käsittelijä, joten on hyvin tärkeää erottaa vastuut näiden kahden tahon välillä. Viime kädessä rekisterinpitäjä vastaa aina tietojenkäsittelyn lainmukaisuudesta, ja henkilötietojen käsittelijä toimii

[40] Neuvonen 2014: 93.
[41] Neuvonen 2014: 93.
[42] Neuvonen 2014: 95.
[43] Hanninen 2017: 23.

rekisterinpitäjän ohjeiden mukaisesti. Vastuu jakautuu täten mahdollisesti rekisterinpitäjän ja henkilötietojen käsittelijän kesken.

Tietosuoja-asetuksen 37 artikla määrittää, että tietyillä organisaatioilla on velvollisuus nimittää organisaation tietosuojavastaava. Nimittämisvelvollisuus tulee kyseiseen silloin, kun organisaation toiminta edellyttää rekisteröityjen vakituista ja systemaattista seurantaa ja valvontaa. Tietosuojavastaava tulee myös nimittää, jos organisaatio käsittelee erityisten henkilöryhmien henkilötietoja. Nimitetty tietosuojavastaava voi olla yrityksen työntekijä tai organisaatio voi halutessaan ulkoistaa tietosuojavastaavan roolin kokonaan ulkopuoliselle taholle. Tietosuojavastaavan tehtävänä on muun muassa antaa ohjeistuksia organisaatiolle sekä tehdä seurantaa siitä, kuinka organisaatio noudattaa tietosuojalainsäädäntöä. Helposti voidaan ajatella, että tietosuoja-asetuksen asettama velvollisuus tietosuojavastaavan nimittämiselle kohdistuisi vain rekisterinpitäjään. Sama nimittämisvelvollisuus pätee kuitenkin myös henkilötietojen käsittelijään, jos tämän toiminta on sellaista, että henkilötietoja käsitellään laajalla mittakaavalla. [44]

Erityisesti suuremmat työnantajat keräävät ja käsittelevät laaja-alaisesti työntekijöidensä henkilötietoja. On siis väistämättä tärkeää, että työnantaja huomioi asetuksesta tulevan velvollisuuden tietosuojavastaavan nimittämiselle. Toki pienille työnantajille tietosuojavastaavan nimittäminen tai palvelun ulkoistaminen voi olla huomattavakin kustannus. Toisaalta tietosuojavastaavan nimeämisellä myös pienemmät työnantajat pystyvät oikeaoppisemmin huolehtimaan tietosuojalainsäädännön soveltamisesta sekä säästymään mahdollisilta seuraamuksilta ja sanktioilta. [45]

[44] Parkkamäki 2018:146.
[45] Parkkamäki 2018:146–147.

### 3.1.1 Rekisterinpitäjän velvollisuudet

Rekisterinpitäjällä, työnantajalla on aina lainmukainen vastuu; sen on pystyttävä turvaamaan ja osoittamaan, että tietosuoja-asetuksen ja lain mukaiset vaatimukset toteutuvat.[46] Rekisterinpitäjällä on vastuu siitä, että tietosuojaperiaatteet toteutuvat kaikessa sen henkilötietojen käsittelyssä. Rekisteripitäjän on implementoiva periaatteet osaksi organisaation tietojen käsittelyä ja tehtävä tarvittava toimenpiteet. Sen on esimerkiksi luotava prosessit, jotka noudattavat tietosuojalainsäädäntöä, järjestettävä henkilöstölle koulutusta, jotta sillä on tarvittava tietotaito henkilötietojen oikeaoppiselle käsittelylle, kehitettävä mahdollisia salassapitosopimuksia sekä varmistettava, että se suorittaa valvontaa ja auditointeja organisaation sisällä. [47]

Rekisterinpitäjällä on vastuu myös järjestelmien tietoturvasta ja riittävistä teknisistä salauksista.[48] Näin ollen rekisterinpitäjän on huolehdittava siitä, että se on toteuttanut tarpeelliset tekniset vaatimukset tietojen käsittelylle. Tekniset vaatimukset riippuvat siitä, kuinka laajasti ja minkälaisia henkilötietoja käsitellään, organisaation on suoritettava arviointi tietojen käsittelyn riskeistä. [49] Suurelle työnantajalle riski voi olla suurempi, koska työntekijöiden määrä ja tätä myötä käsitelty tieto on suurempaa. Sen lisäksi, että työnantaja käsittelee suurta määrää työntekijöidensä henkilötietoja, käsittelee se myös aina väistämättä myös arkaluontoisia henkilötietoja.[50] Näiden myötä työnantajan on oltava rekiterinpitäjänä tarkka ja huolellinen siitä, että sillä on oikeat ja täsmälliset prosessit henkilötietojen käsittelylle.

Kuten aikaisemmin on mainittu, rekisterinpitäjä on vastuussa siitä, että tietosuojaperiaatteita seurataan kaikessa henkilötietojen käsittelyssä.[51] Tietosuoja-asetuksen myötä rekisterinpitäjän osoitusvelvollisuus on kasvanut ja ottanut tärkeämmän roolin.

[46] Hanninen ym. 2017: 26.
[47] Talus ym. 2017: 13.
[48] Talus ym. 2017: 13.
[49] Hanninen ym. 2017: 26.
[50] Hanninen ym. 2017: 27.
[51] Talus ym. 2017: 12.

Tietosuoja-asetuksen myötä osoitusvelvollisuus sitoo rekisterinpitäjää laillisesti. Osoitusvelvollisuudella tarkoitetaan tietosuoja-asetuksessa sitä, että rekisterinpitäjän on kyettävä osoittamaan se, että se on käsitellyt henkilötietoja vaatimusten mukaisesti. [52] Osoitusvelvollisuus on jälleen yksi laillinen velvoite, joka toki suojaa työntekijää ja rekisteröityä entistä paremmin, mutta asettaa jälleen työnantajalle uusia velvollisuuksia. Sinänsä osoitusvelvollisuuden perimmäinen tarkoitus on hyvä, koska sillä lisätään rekisterinpitäjän vastuuvelvollisuuksia ja sen on enemmän mietittävä tietojen käsittelyn prosesseja ja toimia käytännön tasolla.[53] Osoitusvelvollisuutta ei voi suoraan määritellä tarkasti, sillä on hyvin tapauskohtaista, kuinka laajasti rekisterinpitäjän on noudatettava vaatimusta. Yksi tärkeimmistä osoitusvelvollisuuden aspekteista on dokumentaatio.[54] Dokumentaation tärkeys korostuu esimeriksi siinä, jos työnantaja suorittaa prosessimuutoksen. On tärkeää, että työnantaja pystyy näyttämään toteen, että se on tehnyt tarvittavan tietosuoja- arvioinnin uudelle prosessille.

Rekisterinpitäjän velvollisuutena on tunnistaa mahdolliset riskit, mitä voi syntyä henkilötietojen käsittelystä. Rekisterinpitäjän yhtenä velvollisuutena on toteuttaa vaikutustenarviointi tietyissä tilanteissa, joissa se arvioi mahdolliset riskit henkilötietojen käsittelylle. Arviointia tehdessä on huomioitava esimerkiksi henkilötietojen käsittelyn laatu, käsittelyn laaja-alaisuus ja tausta. Rekisterinpitäjän on syytä tehdä vaikutusarviointi varsinkin silloin, kun se käsittelee erityisten henkilöryhmien henkilötietoja, implementoi uusia teknologioita ja teknisiä ominaisuuksia tai kun käsitellään suuria massoja henkilötietoja.[55] Työnantajalla on tietyissä tilanteissa lainmukainen velvollisuuskin kerätä ja käsitellä työntekijöidensä arkaluontoisia henkilötietoja. Työnantajan on siis oltava erityisen tarkkana riskien arvioinnissa ja tunnistamisessa, arkaluontoisten henkilötietojen käsittelyyn kohdistuu korkeampi riski kuin muiden tietojen käsittelyyn.

[52] Vainio 2017: 45.
[53] Vainio 2017: 46.
[54] Vainio 2017: 55.
[55] Talus ym. 2017: 17.

### 3.1.2 Henkilötietojen käsittelijän velvollisuudet

Ennen asetuksen voimaantuloa käsittelijän tehtävät ovat olleet pitkälti vain sopimusvelvoitteisia. Pohjimmaisena sääntönä on se, että henkilötietojen käsittelijän tulee noudattaa ohjeita, jotka se on saanut rekisterinpitäjältä. Näin ollen henkilötietojen käsittelijällä ei ole itsenäistä oikeutta laatia toimintatapoja tietojen käsittelylle, vaan sen on seurattava rekisterinpitäjän määräyksiä.[56] Henkilötietojen käsittelijän vastuulla on kuitenkin toimittaa todisteet rekisterinpitäjälle siitä, että se toimii ja käsittelee henkilötietoja tietosuojalainsäädännön mukaisesti. [57]

Nykyisin, asetuksen määritelmän mukaan, henkilötietojen käsittelijä katsotaan rekisterinpitäjäksi, jos käsittelijä itsenäisesti päättää tarkoituksista, joihin henkilötietoja käytetään. Tällaisissa tilanteissa rekiterinpitäjän vastuut velvoittavat myös henkilötietojen käsittelijää. Käsittelijän vastuulle tulee esimerkiksi osoitusvelvollisuus sekä vastuu antaa vastauksia suoraan rekisteröidyille heidän sitä pyytäessään. Koska rekisterinpitäjän velvollisuudet ovat huomattavasti suuremmat, henkilötietojen käsittelijän on oltava tarkka omasta toimenkuvastaan. [58]

Tietosuoja-asetuksen voimaantulon myötä myös henkilötietojen käsittelijän vastuu on huomattavasti korkeampi kuin aikaisemmin. Tämä on sinänsä luonnollista, koska organisaatiot ulkoistavat enenevissä määrin palveluitaan ja toimintojaan. Rekisterinpitäjät eivät välttämättä aikaisemmin ole kiinnittäneet niin paljon huomiota siihen, kuinka perimmäinen vastuu henkilötiedoista säilyy kuitenkin rekisterinpitäjällä. [59] On luonnollista, että työnantaja siirtää esimerkiksi palkkahallinnon kokonaan ulkoistetulle palkanlaskennalle. Tällöin työnantaja säilyy yhä rekisterinpitäjänä, mutta palkkahallinnon palveluntuottaja henkilötietojen käsittelijänä. Työnantajan on siis tärkeää ottaa huomioon riskien arvioinnissa myös henkilötietojen käsittelijän rooli. Vaikka työnantaja olisi ulkoistanut

[56] Parkkamäki 2018: 139.
[57] Talus ym. 2017: 22.
[58] Hanninen ym. 2017: 27.
[59] Parkkamäki 2018: 126.

palkkahallinnon, on se silti perimmäisessä vastuussa siitä, että ulkopuolinen palveluntarjoaja käsittelee sen työntekijöiden henkilötietoja laillisesti. Työnantajan on pystyttävä todentamaan, että se on valinnut palveluntarjoajaksi sellaisen tahon, jolla on tarpeelliset tietosuojakäytännöt. [60]

### 3.2 Työntekijästä kerättävät tiedot

Kuten edellä on mainittu, työnantaja kerää jo heti työsuhteen solmimisvaiheessa työntekijästä henkilötietoja, jotka ovat olennaisia työsuhteen kannalta. Yksityisyydensuojasta työelämässä annetun lain mukaan työnantajan on ensisijaisesti hankittava tiedot työntekijältä itseltään. Lain 4 §:n mukaan työnantajan on pyydettävä työntekijältä suostumus, mikäli se hankkii tietoja muuta kautta.[61] Pääasiassa työnantaja voi siis kerätä työntekijästä tietoja mistä vain siinä määrin, kun ne ovat tarpeellisia.[62] Lisäksi EU:n perusoikeuskirjan 8 artikla tukee työntekijän suostumusta henkilötietojen keräämiseen. Suostumus ei kuitenkaan tarkoita sitä, että työntekijä voisi itse päättää omien henkilötietojensa käytöstä. Lähinnä laissa ja perusoikeuskirjassa suostumuksella tarkoitetaan sitä, että henkilötietojen käsittelijällä ja rekisterinpitäjällä on informaatiovelvollisuus.[63] Lain 4 §:ä sovelletaan ainoastaan siis henkilötietojen keräämiseen, kun on kyse tiedoista, jotka ovat paperilla tai tietokoneella. Näin ollen suullisesti luovutetut tiedot eivät kuulu lain sovellettavuuden piiriin, niin kauan kuin niitä ei tallenneta mihinkään rekisteriin.[64] Työntekijän henkilötiedoiksi luetaan myös ne tiedot, jotka muodostuvat työntekijän tekemistä testeistä, sähköpostiviestinnästä tai teknisestä valvonnasta.[65]

---

[60] Parkkamäki 2018: 127.
[61] Nyyssölä 2020: 69.
[62] Nyyssölä 2020: 67.
[63] Neuvonen 2014: 65.
[64] Nyyssölä 2020: 70–71.
[65] Telaranta & Neuvonen 2022: 778.

### 3.3 Direktio-oikeus

Työnantajalla on johto- ja valvontaoikeus eli direktio-oikeus työsuhteessa, mikä tarkoittaa sitä, että työnantajalla on oikeus määrittää, minkälaista ja miten työtä yrityksessä tehdään sekä minkälaiset laatuodotukset työnantajalla on työntekijän työltä. Työnantajan ja työntekijän solmima työsopimus määrittää pitkälti vaatimukset johto- ja valvontaoikeudelle. Työnantajan asettamien määräyksien tulee olla asiallisia, kohtuullisia sekä tasavertaisia. Työntekijällä on oikeus kieltäytyä työstä, jota hän ei kykene tekemään työajan puitteissa. Mikäli työntekijällä ja työnantajalla on erimielisyyksiä työsopimuksen ehdoista, on työnantajalla tulkintaoikeus siihen asti, kunnes erimielisyys ratkaistaan. Eli työntekijän on pitäydyttävä työnantajan tulkinnassa. [66]

Työnantaja ei voi omavaltaisesti muuttaa ja lisätä työsopimuksen ehtoja työnjohto-oikeuden nojalla, kuten selviää Korkeimman oikeuden ratkaisusta KKO 2010:60.

> Työntekijä työskenteli kuntosaliyhtiössä siivoojana toistaiseksi voimassa olevassa työsuhteessa. Työntekijän siivoamiin tiloihin kuului yhtiön 600 neliöinen tila. Vuoden 2006 alusta alkaen työnantaja määräsi työntekijän siivoamaan 600 neliöisen tilan lisäksi yhtiön ostaman 400 neliöisen tilan. Työntekijän tuli tehdä lisätyötä samalla työtuntimäärällä ja palkalla kuin aikaisemmin, jotta hän sai myös uudet, laajennetut tilat siivottua. Työnantaja antoi työntekijälle kirjallisen varoituksen, johtuen puutteellisesta siivouksesta. Yhtiö päätti työntekijän työsuhteen seuraavana päivänä varoituksen antamisesta. Yhtiö perusteli irtisanomista painavalla syyllä, jonka se perusteli työnteon laiminlyönnillä ja piittaamattomuudella työaikoihin. Asia eteni Vaasan Käräjäoikeuden käsittelyyn, jossa Käräjäoikeus katsoi, että yhtiö oli toiminut johto- ja valvontaoikeuden puitteissa. Käräjäoikeuden mukaan lisätyö oli kuulunut työntekijän pätevyyteen ja kirjallinen varoitus oli ollut aiheellinen. Tapaus eteni Vaasan Hovioikeuden kautta Korkeimpaan oikeuteen. Hovioikeus katsoi, että lisätilan siivoaminen oli suuri muutos, joka muutti olennaisesti työntekijän työsuhteen ehtoja. Näin ollen Hovioikeus katsoi, että yhtiön olisi pitänyt neuvotella yhdessä työntekijän kanssa työsopimuksen ehtojen muuttamisesta. Yhtiölle annettiin valituslupa Korkeimpaan oikeuteen. Korkein oikeus katsoi myös, että pelkästään työnjohto-oikeus ei oikeuttanut yhtiötä yksin määräämään lisätilojen siivouksesta. Korkein oikeus päätyi ratkaisussaan samaan lopputulokseen Hovioikeuden kanssa ja näin ollen Hovioikeuden ratkaisua ei muuteta.[67]

[66] Nieminen 2014: 18–19.
[67] KKO 2010:60.

Työsopimuksen ehdot ovat sitovia molemmille osapuolille, sekä työnantajalle että työntekijälle. Sopimuksen ehtojen muuttaminen yksipuolisesti ei ole sallittua, jos kyseessä on olennainen ja pysyvä muutos ehtoihin. Työnantaja on oikeutettu ehtojen muuttamiseen direktio-oikeutensa rajoissa huomioiden sen, että isommista ja pysyvistä muutoksista tulee keskustella yhdessä työntekijän kanssa.[68] Kuten edellä mainitusta Korkeimman oikeuden tapauksesta selviää, on noin suuren tilan lisääminen iso ja pysyvä muutos, joka ei ole enää pelkästään yksin työnantajan päätettävissä ja direktio-oikeuden rajoissa.

Työntekijällä on mahdollisuus hyväksyä työnantajan esittämät muutokset ehtoihin joko sananmukaisesti tai hiljaisesti. Hiljainen hyväksyntä tarkoittaa sitä, että työntekijä alkaa työskentelemään muutettujen ehtojen mukaisesti. Aina, kun sopimuksen ehtoja muutetaan, tulee tehdä selvitys, miten uudet ehdot vaikuttavat esimerkiksi työntekijän palkkaan. Mikäli työntekijä kieltäytyy esitetyistä uusista ehdoista eikä irtisanomisperustetta ole, työntekijä voi velvoittaa, että sopimus jatkuu samoin ehdoin, kun aikaisemmin. Ymmärrettävästi työntekijän on välillä vaikea arvioida, onko työnantajalla oikeus yksipuoliseen ehtojen muuttamiseen. Näissä epävarmoissa tapauksissa työntekijällä on mahdollisuus tutkia tapauksen lainmukaisuus, esimerkiksi ammattiliiton avustuksella. Ehdoton ja perusteettomasti tapahtunut kieltäytyminen esimerkiksi uusista työtehtävistä voi johtaa työsopimuksen purkamiseen.[69]

### 3.4 Luottamusmiehen oikeudet

Luottamusmiehellä tarkoitetaan työehtosopimuksen perusteella valittua henkilöstöryhmän edustajaa.[70] Yleisesti ammattiosasto on asettanut luottamusmiehen tähän tehtävään. Luottamusmiehen tehtäviin kuuluu valvoa sitä, että työehtosopimuksia noudatetaan työpaikalla, selvittää mahdollisia erimielisyys- ja konfliktitilanteita työntekijöiden ja työnantajien välillä sekä turvata työpaikan työrauha. [71] Lähtökohtaisesti

[68] Nieminen 2017: 52–53.
[69] Nieminen 2017: 52–53.
[70] Lamponen 2016: 64.
[71] Orasmaa 2001: 4.

luottamusmiehellä ei ole erityisiä oikeuksia saada tietoonsa työntekijöiden henkilötietoja. Kuitenkin tietyissä tilanteissa työnantaja voi olla velvoitettu luovuttamaan luottamusmiehelle työntekijöiden henkilötietoja.

Osa työehtosopimuksista voivat velvoittaa työnantajaa tietojen luovutukselle, mutta henkilötietojen luovutusvelvollisuus on kuitenkin rajattu esimerkiksi ulkopuolisen työvoiman henkilötietoihin. Työtuomioistuimen 2018:101 tapauksessa käsiteltiin tilannetta, jossa tulkittiin työehtosopimuksen tulkintaa liittyen työnantajan velvollisuuteen luovuttaa luottamusmiehelle vuokratyöntekijän henkilötietoja. Viestinvälitys- ja logistiikka-alan työehtosopimuksen mukaan työnantajan on annettava luottamusmiehelle tiedoksi uuden työntekijän työsopimuksesta tiettyjä tietoja, kuten nimi, yksikkö, sovitut työajat, määräaikaisen työsopimuksen kesto sekä määräaikaisen työsopimuksen perusteet. Työehtosopimuksen mukaan luottamusmies on oikeutettu saamaan nimenomaisesti saman työnantajan palveluksessa aloittavien työntekijöiden tiedot. Henkilötietojen luovutus ei työtuomioistuimen päätöksen mukaan kuitenkaan ulotu vuokratyöntekijään. [72]

On täysin luonnollista, että luottamusmies ei ole oikeutettu saamaan vuokratyöntekijän työsopimuksen tietoja. Henkilöstöpalveluyritys toimii vuokratyöntekijän virallisena työnantajana eikä henkilöstöpalveluyritys ole edes oikeutettu luovuttamaan vuokratyöntekijän tietoja asiakasyrityksilleen, saati asiakasyrityksen luottamusmiehelle.

Luottamusmiehen tiedonsaantioikeus voi perustua myös luottamusmiessopimuksiin. Luottamusmiessopimukset voivat määrittää tiettyjä erityistilanteita, jolloin valitulla luottamusmiehellä on oikeus saada työntekijöiden henkilötietoja. Työtuomioistuimen tapauksessa 2020:74 oli kyse työnantajan ja luottamusmiehen välisestä erimielisyydestä liittyen tiedonsaantioikeuteen.

> Pääluottamusmies oli pyytänyt työnantajaa toimittamaan hänelle tiedot koskien työpaikalla aiheutunutta erimielisyyttä palkkojen erityislisiä. Pääluottamusmies oli pyytänyt työnantajaa toimittamaan tiedon kaikista työntekijöistä, joille työnantaja oli

[72] TT 2018:101.

> maksanut erityistyölisää. Työnantaja ei ollut suostunut toimittamaan kyseisiä tietoja, samalla kannalla oli ollut myös työnantajaliitto, jolta työnantaja oli pyytänyt linjausta asiaan. Työtuomioistuin katsoi, että luottamusmiessopimuksen mukaisesti luottamusmiehellä on oikeus saada kaikki tiedot työntekijöistä, jotka liittyvät erimielisyyteen. Työtuomioistuin määräsi tuomiossaan työnantajan työehtosopimuksen vastaisesti menettelystä sekä työnantajaliiton valvontavelvollisuuden suorittamatta jättämisestä hyvityssakkoon.[73]

Joissakin työehtosopimuksissa on lisäksi säädetty, että valitulla luottamusmiehellä on oikeus yrityksen omistaman tietokoneen käyttöön. Luottamusmiehellä on oikeus käyttää yrityksen tietokonetta sähköpostien hoitamiseen ja muuhun internet-käyttöön silloin, kun nämä liittyvät ammattiyhdistystoimintaan. Teknologiateollisuuden työehtosopimuksessa on linjattu, että luottamusmiehellä on oikeus käyttää yrityksen yleisiä toimistotarvikkeita ja IT-laitteita, joihin luetaan mukaan sähköposti.[74] Teknologiateollisuuden toimihenkilöiden työehtosopimuksen säännöksen mukaisesti luottamusmiehellä on oikeus saada tietoja työntekijöiden palkoista mutta ei kuitenkaan silloin, jos kyseinen työntekijäryhmä koostuu kolmea pienemmästä työntekijästä.[75] Tällöin työnantaja ei ole tietoja velvoitettu luovuttamaan yksityisyydensuojan nojalla. Työehtosopimuksen mukaan työnantaja on velvollinen luovuttamaan myös muita työntekijöiden henkilötietoja luottamusmiehelle. Työnantajan on esimerkiksi ilmoitettava toimihenkilöiden nimet, työsuhteen alkamisaika sekä työn vaativuusluokka.[76]

[73] TT 2020:74.
[74] Teknologiateollisuuden työehtosopimus.
[75] Teknologiateollisuuden toimihenkilöiden työehtosopimus, yhteistoimintasopimus.
[76] Teknologiateollisuuden toimihenkilöiden työehtosopimus, yhteistoimintasopimus.

# 4 ARKALUONTOISET HENKILÖTIEDOT

Lähtökohtaisesti arkaluontoisten henkilötietojen käsittely ei ole sallittua, luonnollisesti tietojen käsittelyn huolellisuus ja yksityisyydensuoja saavat suuremman merkityksen. Arkaluontoisiksi henkilötiedoiksi luetaan tiedot, jotka koskevat työntekijän etnistä alkuperää, uskonnollista tai poliittista vakaumusta, rikoksen tietoja, terveystietoja tai vammaisuutta, seksuaalista suuntautumista tai sosiaalisia etuuksia. Kuten aikaisemmin on mainittu, työnantaja saa kerätä ja säilöä ainoastaan työsuhteen kannalta olennaisia ja tarpeellisia tietoja. Henkilötiedot, jotka eivät ole työtehtävän kannalta olennaisia ja tarpeellisia, tulee hävittää.[77] Sen lisäksi se, että työnhakija tai työntekijä antaisi suostumuksen arkaluontoisten tietojen käsittelylle, ei vielä yksinään riitä. Työnantajan on osoitettava lain mukainen peruste sille, miksi arkaluontoisten tietojen kerääminen ja käsittely on tarpeen. Työnantaja ei saa esittää kysymyksiä arkaluontoisista tiedoista esimerkiksi rekrytointiprosessin aikana sekä työnantajan on ohjattava keskustelua niin, että hakijakaan ei ota arkaluontoisia tietoja esille prosessin aikana. [78]

Vaikka arkaluontoisten tietojen käsittely on pääsääntöisesti kiellettyä, työnantajalla on kuitenkin muutamia poikkeustilanteita, jolloin sen on lain mukaan saatava tieto tietyistä arkaluontoisiksi katsottavista tiedoista. Esimerkiksi tiettyjä terveystietoja työnantajan on pakko käsitellä, esimerkiksi lääkärintodistuksia sekä työntekijän henkilötunnusta esimerkiksi palkanmaksua varten.[79] Lisäksi muun muassa ulkomaalaislaki (301/2004) velvoittaa työnantajaa käsittelemään esimerkiksi työntekijöiden oleskelulupia ja passikopioita.

Työnhakijan ja työntekijän poliittinen vakaumus katsotaan arkaluontoiseksi henkilötiedoksi, eikä työnantaja saa tällaista tietoa käsitellä tai kysyä esimerkiksi rekrytointiprosessin yhteydessä. Kuitenkin eri asia on, jos työnhakija tai työntekijä on itse tuonut tiedon julkiseksi. Esimerkiksi työnantaja saa käsitellä tietoa poliittisesta vakaumuksesta, jos

[77] Nieminen 2018: 33.
[78] Koskinen 2004: 18.
[79] Koskinen 2004: 18–19.

työnhakija tai työntekijä on ollut puolueen ehdokkaana. [80] Nämä ovat poikkeuksia, missä tilanteissa työnantajalla on oikeus arkaluontoisten tietojen keräämiseen ja käsittelyyn. Myös EIT on ottanut kantaa arkaluontoisten henkilötietojen käsittelyyn. EIT on antanut syyskuussa 2022 ratkaisun koskien tapausta, jossa Ranskan veripalvelu käsitteli tarpeettomasti henkilöiden tietoja seksuaalisesta suuntautumisesta. Tapauksessa veripalvelu käsitteli verenluovuttajiensa tietoja seksuaalisesta suuntautumisesta, jota veripalvelu perusteli sillä, että sen oli varmistuttava veren laadusta. Valittaja ei suostunut vastaamaan kysymykseen, mutta lääkäri oli tämän perusteella tehnyt arvion valittajan seksuaalisesta suuntautumisesta. Lisäksi EIT katsoi, että Ranskan hallitus mahdollisti tiedoille aivan liian pitkän säilytysajan. EIT katsoi päätöksessään, että Ranska oli rikkonut EIS:n 8 artiklaa, jossa määritellään yksilön oikeudesta yksityisyyteen. Ratkaisussaan EIT antoi päätöksen Ranskalle, että se joutuu maksamaan kyseisen tapauksen oikeudenkäyntikulut sekä korvaamaan 3000 euroa valittajalle. [81]

### 4.1 Terveystiedot

Yleisesti suurimmat henkilötietojen keräämiseen liittyvät ongelmat koskevat nimenomaan terveystietojen keräämistä. Työnantajan on kerättävä työntekijää koskevat terveystiedot työntekijältä suoraan tai mahdollisesti muualta, mutta työntekijän kirjallisella hyväksynnällä.[82] Uuden tietosuoja-asetuksen mukaan terveystietojen käsittely ja kerääminen on lähtökohtaisesti kielletty, mutta se antaa näiden käsittelylle mahdollisuuden, mikäli tietyt ehdot täyttyvät. Työantajan on siis mahdollista käsitellä työntekijän terveystietoja, mikäli tämä antaa käsittelylle suostumuksensa tai lainsäädännön ehdot terveystietojen käsittelylle täyttyvät. Kaikkiin henkilötietojen keräämiseen sovelletaan yleisiä tietosuojaperiaatteita niin myös terveystietojen keräämiseen. Yksi keskeisimmistä periaatteista terveystietojen keräämiseen on tarpeellisuusvaatimuksen periaate;[83] työnantaja saa kerätä vain työtehtävän suoriutumisen kannalta olennaisia terveystietoja.

[80] Koskinen 2004: 18.
[81] EIT Drelon c. France.
[82] Nieminen 2018: 33.
[83] Salokannel 2016: 537–539.

Työnantaja saattaa esimerkiksi tarvita työntekijän terveystietoja sairausajan palkan maksamiseen. [84]

Kuten aikaisemmin on mainittu, terveystietojen kerääminen on mahdollista, mikäli työntekijä on antanut suostumuksensa käsittelylle. Huomioitavaa on se, että terveystietojen käsittelylle annettu suostumus on tiukemmin säädelty kuin yleinen suostumus henkilötietojen keräämiselle. Tietosuoja-asetuksen mukaan suostumuksen tulee olla kirjallinen ja selkeästi ilmaistu. Jos suostumuksen kirjallisessa annossa annetaan suostumus myös muihin tietoihin, tulee terveystietojen käsittelylle annettu suostumus selkeästi erotella muista asioista. Tietosuoja-asetuksessa säädetty lähtökohta suostumukselle on lisäksi se, että suostumuksen tulee rajoittua johonkin tiettyyn tarkoitukseen eli työnantaja ei voi hyväksyä ilmeisen avointa kirjallista suostumusta. Lisäksi huomioitavaa on se, että työntekijällä on oikeus perua suostumuksensa terveystietojensa käsittelylle. Suostumuksen peruminen ei kuitenkaan laillisesti voi vaikuttaa ennen peruutusilmoituksen antoa tapahtuneeseen terveystietojen käsittelyyn. Työntekijän on pystyttävä näyttämään, että suostumus on annettu näiden tietojen käsittelylle. [85]

Kuitenkin työnantajalla on mahdollisuus käsitellä työntekijän terveystietoja ilman tämän suostumusta, mikäli se on lakisääteisesti perusteltua. EU-oikeus tai kansallinen lainsäädäntö määrittelee nämä lainsäädännölliset perusteet. Tietosuoja-asetuksen mukaan terveystietoja saa käsitellä silloin, kun se on tarpeen sosiaalisen suojelun kannalta, rekisteröidyn etujen suojaamiseksi, kun hän on estynyt antamaan suostumuksen, työterveydenhuoltoa koskevaa tarkoitusperää varten tai työntekijän työkyvyn analysoimiseksi sekä kansanterveyden etuun koskevissa tapauksissa tai yleisiin edun mukaisiin arkistointitarkoituksiin. Mikäli työntekijän terveystietoja käsitellään ilman hänen suostumustansa työterveyshuollon tarkoituksiin, tulee käsittelystä vastata henkilö, jolla on lakisääteinen vaitiolovelvollisuus.[86] Työntekijän terveystietoja ovat siis oikeutettuja käsittelemään vain

[84] Nieminen 2018: 33.
[85] Salokannel 2016: 539–540.
[86] Salokannel 2016: 541–542.

henkilöt, jotka ovat vastuussa työsuhdetta koskevista päätöksistä sekä heidän on huolehdittava siitä, että terveystiedot säilytetään eri paikassa kuin muut työntekijästä kerätyt henkilötiedot.[87]

Kansallisen lainsäädännön mukaan arkaluontoisten henkilötietojen käsittelystä ei voida poiketa edes työntekijän suostumuksella. Kuitenkin tietosuoja-asetuksessa on annettu suhteellisen laaja mahdollisuus esimerkiksi terveystietojen käsittelyyn pelkän suostumuksen perusteella. Tästä voidaan todeta, että kansallinen lainsäädäntö on ottanut huomattavasti tiukemman linjan arkaluontoisten henkilötietojen käsittelylle ja keräämiselle.

### 4.2 Huumausainetiedot

Työntekijän huumausaineiden käyttöä koskevat tiedot luetaan myös arkaluontoisiksi terveydentilaan kuuluviksi tiedoiksi. Huumausainetietojen käsittelyllä pyritään siihen, että työpaikka olisi huumeeton sekä käsittelyllä pyritään ennalta ehkäisemään vahingollisia seurauksia. Lisäksi sääntelyllä pyritään edistämään turvallisuuden ja omaisuuden suojan turvaamista. [88]

Laissa yksityisyyden suojasta työelämässä määritetään, että työntekijän huumetestit tulee tehdä terveydenhuollon henkilöstön toimesta. Ammattihenkilöstön tekemästä testistä toimitetaan todistus työnantajalle, jonka työntekijä tai työnhakija toimittaa. Jotta huumetesti voidaan tehdä, tulee lain mukaisten ehtojen täyttyä. Laki yksityisyyden suojasta työelämässä määrittää, että huumetestin tekeminen on perusteltua, kun tehtävään valittu hakija tulee työskentelemään esimerkiksi opetuksen ja lasten parissa, jos työnhakija tulee työskentelemään huumausaineiden parissa, työtehtävä vaatii erityistä luottamusta, esimerkiksi valtion ja maanpuolustuksen tehtävät. Laki yksityisyydensuojasta työelämässä 9 § määrittää, että työnantajan on jo hakuvaiheessa informoitava työnhakijaa siitä, että tehtävään valitulle tullaan tekemään huumetesti.

[87] Nieminen 2018: 33.
[88] Koskinen ym. 2016: 6.

### 4.3 Rikostiedot

Rikosrekisterilaki määrittää puitteet, milloin yksityinen henkilö on oikeutettu saamaan itseään koskevat rikostiedot. Henkilöllä on mahdollisuus saada omat rikostietonsa silloin, kun hänen täytyy osoittaa luotettavuutensa jollekin ulkomaiselle viranomaiselle, esimerkiksi viisumia tai työlupaa varten. Silloin, kun henkilö pyytää omia tietojaan, hänen tulee kertoa näiden tietojen käyttötarkoitus. Mikäli hän ilmoittaa tietojen menevän työnantajalle, oikeusrekisterikeskus ei luovuta hänelle omia tietojaan. Kuitenkin henkilöllä on oikeus katsoa ja tarkistaa omia tietojaan sekä saada nämä kirjallisena itselleen. Tällöin työhakija tai työntekijä voi omasta tahdostaan tai työnantajan toiveesta välittää nämä tiedot työnantajalle. [89]

Vain erityistilanteissa työnantajalla on oikeus tarkastaa työnhakijan tai työntekijän rikostiedot. Lain lasten kanssa työskentelevien rikostaustan selvittämisestä (504/2002) mukaan yksi poikkeustilanne rikostietojen tarkistukselle on silloin, kun työntekijä tulee työskentelemään lasten parissa. Kun työnhakija on valittu kyseiseen tehtävään, voi työnantaja pyytää työntekijän rikosrekisterin tarkistettavaksi. Työnantajan on pyydettävä rekisteriä suoraan itse työntekijältä.

Työntekijä voi syyllistyä rikokseen työsuhteen aikana, ja jo itse epäily rikoksesta voi vaikuttaa työntekijän työsuhteeseen. Työtuomioistuimen tapauksessa TT 2016:124 työnantaja lomautti ja sittemmin irtisanoi työntekijän, koska tämä oli epäiltynä rikoksesta ja myöhemmin myös tuomittuna kahden vuoden ehdottomaan vankeuteen.

> Työntekijä oli lomautettu sillä perusteella, että hänet oli vangittu epäiltynä vakavasta rikoksesta. Myöhemmin työntekijä tuomittiin kahden vuoden ehdottomaan vankeuteen. Työnantaja ilmoitti, että se purkaa työsopimuksen Käräjäoikeuden antaman tuomion jälkeen. Tuomio ei kuitenkaan ollut vielä lainvoimainen, kun työnantaja oli jo purkanut työntekijän työsuhteen. Asia eteni hovioikeuteen, joka kumosi Käräjäoikeuden antaman tuomion. Työtuomioistuin katsoi, että työnantajalla oli oikeus lomauttaa työntekijä. Lomauttamista puolsi se, että työntekijä oli estynyt suoriutumaan työstään vangitsemisen vuoksi,

[89] Koskinen 2004: 28.

> eikä työnantaja tiennyt vielä tulevista tuomioista. Lisäksi lomauttaminen on alkuun työsuhteen purkamista lievempi vaihtoehto. Työtuomioistuimen mukaan, mikäli työntekijä syyllistyy vapaa-ajallaan rikokseen, se voi olla peruste työsuhteen purkamiselle. Tuomioistuin katsoi, että työnantajan purkuperusteena ollut vakava luottamuspula työntekijää kohtaan, oli tässä tapauksessa perusteltu syy työsuhteen päättämiselle. [90]

Oikeuskäytäntö osoittaa, että sillä on paljonkin merkitystä, minkälaisesta rikoksesta työntekijä on tuomittu. Edellä käsitellyssä tapauksessa työntekijä oli muiden rikoksien lisäksi syyllistynyt myös ampuma-aserikokseen ja hän työskenteli aseteollisuudessa toimivassa yrityksessä. Näin ollen voitiin katsoa vakavan luottamuspulan syntyvän ja työntekijän mahdollisesti haittaavan yrityksen mainetta. Työnantajalla ei ole velvollisuutta odottaa tai lykätä työntekijän työsuhteen purkamista rikosprosessin ajaksi. [91]

### 4.4 Turvallisuusselvitys

Tiettyjen perusteiden täyttyessä työnantajalla on oikeus teettää tehtävään valitusta työntekijästä turvallisuusselvitys sekä käsitellä siellä ilmenneitä henkilötietoja. Turvallisuusselvitys merkitsee sitä, että suojelupoliisi selvittää tehtävään valitun työntekijän taustat ja tarpeen tullen myös haastattelee turvallisuusselvityksen kohdetta. Suojelupoliisi tekee arvion siitä, mitkä tiedot ovat työnantajalle tarpeellisia ja toimittaa nämä tiedot sille. Turvallisuusselvityksiä on mahdollista hakea kolmea erilaista; perusmuotoista, laajaa ja suppeaa selvitystä. Työnantajan on tehtävä arvio siitä, mihin selvitykseen sillä on oikeus huomioiden työntekijän yksityisyyden suoja. [92] Turvallisuusselvityslaki (2014/726) määrittää puitteet sille, milloin työnantajalla on tätä oikeus anoa. Näin ollen turvallisuusselvityslaki on myös säädetty turvaamaan työntekijän yksityisyydensuojaa. Laki määrittää myös sen, että turvallisuusselvityksen teettäminen tulee antaa tiedoksi työntekijälle jo hakuvaiheessa. Tämä tarkoittaa sitä, että työnantajan on siis ilmoitettava tästä esimerkiksi jo työpaikkailmoituksessa.

---

[90] TT 2016:124.
[91] TT 2016/124.
[92] Nyyssölä 2020: Rikostietojen, henkilötunnuksen ja luottotietojenkäsittely. Turvallisuusselvitys.

# 5 TEKNINEN VALVONTA

Teknisellä valvonnalla tarkoitetaan työpaikan kameravalvontaa ja sähköistä viestintää. Työntekijöiden tekninen valvonta on yleistynyt valtavasti ja monet työpaikat käyttävät joitain teknisiä välineitä tiedon saantiin.[93] Laki yksityisyyden suojasta työelämässä ja sähköisen viestinnän palveluista annettu laki sääntelevät työpaikkojen teknistä valvontaa. Lisäksi Suomen lainsäädäntö velvoittaa työnantajan tiettyihin valvonnan muotoihin. Työaikalaki (872/2019) edellyttää työnantajaa seuraamaan työntekijän työaikaa.[94] Tekninen valvonta voi keskittyä esimerkiksi työn suorittamiseen eli työprosessiin, työympäristöön tai yksilöityyn työntekijään.[95] Nykyajan teknologian kehityksen myötä on hyvin tärkeää tehdä selkeät rajanvedot ja säännöt kameravalvonnalle, sähköpostiviestinnälle sekä paikannustiedoille, jotka esittävät työntekijän sijainnin. Ongelmallisen asiasta tekee se, missä menee työntekijöiden yksityisyyden raja rinnastettuna työturvallisuuteen.

Valvonnan puolesta on esitetty monia perusteita, joista keskeisin on se, että työnantajalla on oikeus pyrkiä työn tehokkuuteen ja tuottavuuteen tarkastelemalla työn sujuvuutta ja tasoa sekä työpaikan määräysten noudattamista. Lisäksi valvonnan etuna on pidetty sitä, että se antaa työantajalle tilaisuuden työn objektiiviselle arvioinnille. Teknistä valvontaa on puolusteltu myös työturvallisuuden ja työhyvinvoinnin kannalta sekä työnantajien oikeudella turvata materiaalista omaisuutta. Moni tutkimus on kuitenkin osoittanut, että tekninen valvonta heikentää työntekijöiden hyvinvointia työpaikalla ja kasvattaa työntekijöiden stressitasoja.[96]

[93] Kuokkanen, Alvesalo-Kuusi 2014: 30.
[94] Kuokkanen, Alvesalo-Kuusi 2014: 30.
[95] Kuokkanen, Alvesalo-Kuusi 2014: 34.
[96] Kuokkanen, Alvesalo-Kuusi 2014: 36.

## 5.1 Lex Nokia

Sähköisen viestinnän tietosuojalain muutos (125/2009) eli Lex Nokia tuli voimaan kesäkuussa 2009. Lex Nokian mukaisesti työnantajalla on oikeus käsitellä työntekijän sähköpostiviestinnän ja tietoverkkoliikenteen tunnistamistietoja silloin, kun on aiheellista epäillä työntekijää tietoverkon ohjeiden vastaisesta väärinkäytöstä. Eli muutoksen mukaisesti työnantajalla on oikeus tarkastella myös työntekijän yksityisiä viestejä, joissa työnantaja ei ole millään tavalla osapuolena. Sähköpostin tunnistamistiedoilla tarkoitetaan käyttökirjanpitoon arkistoituvia tietoja, kuten kuka on lähettänyt tai vastaanottanut viestin sekä mihin ajankohtaan tämä on tapahtunut. Ristiriitaisuus syntyy siitä, että periaatteen mukaisesti jokaisella työntekijällä tulisi olla oikeus yksityisyyteen töissä ja työpaikalla. Kuitenkin esityksessä työnantajan oikeus tiedonsaannille on asetettu olennaisemmaksi ja tärkeämmäksi osaksi kuin työntekijöiden yksityisyydensuoja. [97] Hallituksen esityksen mukaan (HE 48/2008) lakimuutos tarjoaa mahdollisuuden parantaa teleyritysten ja lisäarvopalvelun tarjoajien ja tilaajien tietoturvaa ja huolehtia tietoturvallisuudesta paremmin.[98]

Yksityiselämän kunnioittaminen puoltaa sitä, että työntekijöillä on oikeus rakentaa ja kehittää ihmissuhteita. Ihmissuhteita kehittyy ja niitä ylläpidetään työpaikalla, joten tämä rajaa paljolti työnantajan valvontaoikeutta. Kaikilla on lisäksi oikeus sananvapauteen, johon sisältyy oikeus lähettää ja vastaanottaa viestejä myös työajalla. Sananvapauden kannalta laki ei ole kannustava, kun yksityisiä viestejä saatetaan seurata työnantajan puolesta. Täten jotta sananvapaus täyttyy, on mahdollisuus yksityiseen viestintään mahdollistettava, vaikka tämä tarkoittaisikin työnantajalle sitä, että se ei enää niin laajasti pystyisi kontrolloimaan omaisuuttaan. [99]

Euroopan ihmisoikeustuomioistuin on antanut näkemyksen siitä, että Euroopan ihmisoikeussopimuksen voidaan nähdä puoltavan työntekijöiden oikeutta yksityisyyteen. EIT on

[97] Pesonen 2008: 2–3.
[98] HE 48/2008.
[99] Pesonen 2008: 4.

katsonut, että Euroopan ihmisoikeussopimuksen 8 artiklan määreitä yksityiselämästä ja kirjeenvaihdosta voidaan soveltaa työelämän sähköiseen viestintään. EIT 16.12.1992 Niemietz vs Saksa -tapauksessa käsiteltiin asianajotoimistolla tapahtunutta kotietsintää ja sitä, rikkoiko kyseinen kotietsintä yksityiselämän suojaa ja kirjeenvaihdon salaisuutta. EIT katsoi päätöksessään, että EIS:n 8 artikla soveltuisi vain henkilön kotiin. Näin ollen työympäristöä ja -elämää ei voi jättää yksityiselämän suojan ulkopuolelle. EIT:n päätöksen ja artiklan tulkinnan mukaisesti käsityksiä yksityiselämästä ja kodista ei voida rajata suppeiksi, vaan näitä on sovellettava kattavasti. Kattavan tulkinnan perusteena EIT:n mukaan toimii se, että artiklan keskeisimpänä päämääränä on turvata luonnollisia henkilöitä viranomaistahojen liialliselta sekaantumiselta heidän yksityiselämäänsä.[100] EIT:n tulkinnasta voidaan päätellä, että jos artiklaa sovelletaan näin tiukasti viranomaistoimintaan, on varmasti työnantajan liiallinen puuttuminen vielä moitittavampaa.

Näin ollen laki soti myös Euroopan ihmisoikeussopimusta ja ihmisoikeustuomioistuimen oikeuskäytäntöä vastaan. Sähköisen viestinnän tietosuojalaki on sittemmin kumottu kokonaan.

### 5.2 Kameravalvonta

Yksityisyyden suojasta työelämässä säädetyn lain 16§:n mukaan työnantaja on oikeutettu kameravalvontaan työpaikalla silloin, kun kyseessä on turvallisuuden valvominen, omaisuudesta huolehtiminen tai tuotantoprosessin ajan tasalla pysyminen. Kameravalvonta on luonnollisesti kielletty wc-tiloissa, pukuhuoneissa ja henkilöstön omissa tiloissa. Työnantaja ei saa myöskään käyttää kameravalvontaa tiettyjen työntekijöiden seuraamiseen tai työhuoneessa, joka on annettu jonkun työntekijän yksityiseen käyttöön.[101]

Helsingin Hovioikeuden ratkaisussa oli kyse työntekijän oman työaikakirjaamisen ja työnantajan kirjaamien tehtyjen työtuntien ristiriidasta.

---

[100] Pesonen 2008: 4.
[101] Nieminen 2019: 36.

> Työntekijä oli työskennellyt vajaan vuoden osa-aikaisena kokkina vuonna 2017 avatussa ravintolassa. Työntekijä ilmoitti työsuhteen ajalta huomattavasti suuremmat tehdyt työtunnit kuin työnantaja. Työnantajan mukaan työntekijä oli liioitellut kirjauksissaan tuntien määrää ja hänen mukaansa työntekijän kirjaamat tunnit eivät olleet luotettavia. Työpaikalle oli asennettu kameravalvonta ravintolassa tapahtuneen häirintätapauksen vuoksi. Työnantaja oli lisäksi seurannut työntekijän toteutuneita työtunteja kameravalvontaa hyödyntäen. Työnantaja kertoi Käräjäoikeudessa, että työtuntien seuraaminen kameravalvonnalla olisi ollut työntekijän oma toive. Työntekijän kertomat työpäivät olivat olleet todella pitkiä, suurin osa 14 tuntisia. Käräjäoikeus katsoi, että työntekijän ilmoittamat työtunnit olivat uskottavia, koska kyseessä oli juuri avattava ravintola. Lisäksi työntekijän ja todistajan kertomukset tehdyistä työtunneista olivat yhtenevät. Ravintolan aukiolojen muutos ja työntekijän vähäisemmät työtuntikirjaukset tukivat kirjauksien uskottavuutta. Käräjäoikeus ei katsonut, että työntekijän pyyntö kameravalvonnasta olisi millään tavalla uskottava. Näin ollen valvontakameran nauhoitukselle ei annettu Käräjäoikeuden käsittelyssä arvoa. Työnantaja vaati Helsingin Hovioikeudessa valituslupaa, mutta perusteluja luvan myöntämiselle ei ollut. Hovioikeus katsoi, että Käräjäoikeuden ratkaisu jää pysyväksi. Työnantaja määrättiin korvaamaan työntekijän palkkavaatimukset sekä oikeudenkäynnistä aiheutuneet kulut. [102]

Kyseisessä Hovioikeuden ratkaisemassa tapauksessa kameravalvonnalle ei annettu merkitystä. Työnantaja kohdisti kameravalvonnan ainoastaan yhden tietyn työntekijän seuraamiseen. Ravintolan muilla työntekijöillä oli käytössä työaikakirjaus.

### 5.3 Sähköinen viestintä

Laki yksityisyyden suojasta työelämässä ja sähköisen viestinnän palveluista annettu laki suojaavat työsuhteen sähköistä viestintää. Lisäksi Perustuslaissa määritetään, että kirjeen tai muun samanlaisen luottamuksellisesti lähetetyn viestin sisältö on koskematon.[103] Viime aikoina on kehitetty uusia sovelluksia, joilla pystytään valvomaan ja seuraamaan työntekijän sähköpostin käyttöä. Suomessa tällaiset sovellukset on pääasiassa estetty, mutta esimerkiksi muissa maissa, kuten Yhdysvalloissa valvontasovelluksien käyttö ja hyödyntäminen on suhteellisen yleistä.[104] Työntekijällä on oikeus luottamukselliseen ja yksityiseen sähköpostiviestintään ja tietoverkon käyttöön. Työnantajalla ei ole oikeutta vaarantaa tätä työntekijän sähköisen viestinnän yksityisyydensuojaa, eikä seurata

[102] HO 2020:6.
[103] Saarinen 2011: 141.
[104] Kuokkanen, Alvesalo-Kuusi 2014: 34.

työntekijän sähköpostiviestintää. Työnantaja ja työntekijä eivät voi sopia, että työnantaja olisi oikeutettu lukemaan viestejä jatkuvasti muuten kuin poissaolon aikana työntekijän sähköposteja. On mahdollista, että tulee tilanteita, jolloin työnantajan täytyy etsiä työntekijän sähköpostista hänelle kuuluvia viestejä. Yksityisyyden suojasta työelämässä annetun lain 18§ määrittää käytännöt, miten tällaisessa tilanteessa tulee menetellä.[105]

Yksityisyyden suoja työelämässä annetun lain 18§:ssä säädetään seuraavasti:

*''..työntekijä voi käytettävän sähköpostijärjestelmän automaattisen vastaustoiminnon avulla lähettää viestin lähettäjälle ilmoituksen poissaolostaan ja sen kestosta sekä tiedon henkilöstä, joka hoitaa poissa olevalle työntekijälle kuuluvia tehtäviä..''*

*''työntekijä voi antaa suostumuksensa siihen, että työntekijän poissa ollessa tämän valitsema työnantajan tehtävään hyväksymä toinen 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.''*

Kun työnantaja hakee hänelle kuuluvia viestejä työntekijän sähköpostista, vaatimuksena on, että työnantaja on täyttänyt huolellisuusvelvollisuuden. Huolellisuusvelvollisuudella tarkoitetaan sitä, että työntekijän poissaolon aikana työpaikalla on huolehdittu siitä, että sähköpostit ohjataan jollekin muulle. Näin vähennetään aihetta avata työntekijän luottamuksellista sähköpostia. Työnantajan oikeus hakea viestejä työntekijän sähköpostista liittyy nimenomaan työntekijän tilapäiseen tai pysyvään poissaoloon.[106] Mikäli työnantaja on hakenut ja avannut työntekijän sähköpostiviestejä hänen poissaolonsa aikana, tulee työntekijälle laatia kirjallinen selvitys tapahtuneesta. Työnantajan tulee

[105] Nieminen 2019: 36–37.
[106] Äimälä ym. 2012: 47.

selvityksessä selittää, miksi ja milloin viesti on avattu sekä kuka on avannut kyseisen viestin ja kenelle kaikille on tiedotettu viestin sisällöstä. [107]

Vaikka työntekijän työsuhde päättyisi, työnantajalla ei tässäkään tilanteessa ole oikeutta purkaa salasanoja tai lukea työntekijän sähköposteja ilman hänen suostumustaan. Työntekijä on oikeutettu poistamaan henkilökohtaiset viestit. Lisäksi työntekijällä on työsuhteen päättyessä velvollisuus siirtää hänelle lähetetyt sähköpostit eteenpäin, jos ne ovat yritykselle tarpeellisia.[108] Työntekijän kuollessa tai hänen pysyvän poissaolon aikana, työnantajalla on oikeus edellytysten täyttyessä selvittää hänelle kuuluvat sähköpostit niin kauan kuin työnantajan toimintaa ei pystytä muuten turvaamaan.[109]

Euroopan ihmisoikeussopimuksen 8 artiklan mukaan jokaisella tulee olla oikeus siihen, että heidän yksityiselämäänsä ja kirjeenvaihtoaan kunnioitetaan. 8 artiklan mukaan lailla voidaan poiketa yksityisyyden kunnioittamisesta, mikäli kyse on yleisestä turvallisuudesta, rikollisuuden estämisestä, terveyden suojaamisesta tai henkilön oikeuksien turvaamisesta.

EIT:n suuren jaoston ratkaisemassa tapauksessa Bărbulescu v. Romania oli kyse siitä, että työnantaja oli tarkkaillut työntekijän viestejä ja päättänyt tämän työsuhteen johtuen epäasiallisista henkilökohtaisista viesteistä.

> Työntekijä oli luonut Yahoo Messengerin ja hän oli käyttänyt tätä palvelua työajallaan henkilökohtaisten viestien lähettämiseen. Tämä oli vastoin yrityksen sisäistä ohjeistusta. Heinäkuussa 2007 työnantaja tiedotti työntekijälle, että he olivat seuranneet hänen viestiliikennettä muutaman viikon ajan. Työntekijän oman kannan mukaan hän oli käyttänyt palvelua vain yrityksen asioiden hoitamiseen, jonka jälkeen työnantaja esitti viestit, joissa työntekijä oli keskustellut omista henkilökohtaisista asioistaan. Elokuussa 2007 työnantaja päätti työntekijän työsuhteen perustellen, että työntekijä oli hyödyntänyt yrityksen tarjoamia resursseja omiin tarkoituksiin, mikä oli vastoin annettua ohjeistusta. Asia eteni kansalliseen oikeusprosessiin ja sieltä EIT:n 4. jaoston käsittelyyn. EIT:n 4. jaosto katsoi, että työntekijän yksityisyydensuojaa ei ollut loukattu, vaikka EIS:n 8 artikla soveltui tapaukseen. Jaoston mukaan ei ollut kohtuutonta, että työnantaja halusi

[107] Saarinen 2011: 143.
[108] Nieminen 2019: 37.
[109] Saarinen 2011: 144.

> tarkastella sitä, että työntekijä hoiti hänelle annetut tehtävät ajallaan. Asia eteni EIT:n suureen jaostoon ja se antoi ratkaisunsa tapauksesta syksyllä 2017. Suuren jaoston mukaan kansalliset oikeusistuimet eivät huomioineet sitä, että työntekijälle ei ollut ilmoitettu viestien seurannan laajuudesta tai kuinka syvällisesti siihen puututtiin. Suuren jaoston mukaan kansalliset tuomioistuimet eivät olleet myöskään tuoneet ilmi mikä oikeutti työnantajan valvontaan, mitä vähäisempien toimenpiteitä olisi voitu käyttää sekä pääsikö työnantaja viesteihin ilman työntekijän tietoa. Nämä huomioiden EIT:n suuri jaosto katsoi, että kansallisissa tuomioistuimissa ei suojattu riittävästi työntekijän yksityisyyden suojaa ja EIS:n 8 artiklaa oli rikottu.[110]

EIS:n 8 artiklan perusteella romanialaisen työntekijän yksityisyydensuojaa oli loukattu seuraamalla hänen viestiliikennettään. Toki työnantajalla on oikeus luoda ohjeistukset ja säännöt mihin työaikaa ja työvälineitä käytetään työajalla. Työnantajalla ei kuitenkaan ole oikeutta valvoa yksittäisen työntekijän viestiliikennettä.

### 5.4 Netin käytön valvonta

Työnantajan direktio-oikeus ulottuu tietyissä määrin myös netin käyttöön silloin, kun se selkeästi liittyy työpaikan asioihin.[111] Työnantajalla on näin siis direktio-oikeuden alla mahdollisuus antaa määräyksiä ja ohjeita työpaikalla tapahtuvasta netin käytöstä. Osan tulkintojen mukaan työnantajalla olisi myös oikeus valvoa työntekijöiden netin käyttöä luonnollisella tavalla.[112] Tulkinta on mielenkiintoinen ja ongelmallinen siltä kannalta, mitä luonnollisella ja normaalilla tavalla tarkoitetaan. Mihin työntekijöiden internetin valvonnassa vedetään raja, mikä on normaalia valvontaa ja mikä ei? Tietosuojavaltuutetun mukaan normaali internetin valvonta on perusteltua, mutta esimerkiksi työntekijän internetin käytön tekninen valvonta ei. [113] Toki on ymmärrettävää, että direktio-oikeuden nojalla työnantaja voi luonnollisesti valvoa netin käyttöä esimerkiksi, jos työntekijä työpäivän aikana lukisi sähköisiä lehtiä, on huomauttaminen perusteltua. Rajan veto voi olla kuitenkin häilyvää, mihin raja valvonnan suhteen vedetään.

---

[110] EIT Bărbulescu v. Romania.
[111] Koskinen 2013: 3.
[112] Koskinen 2013: 5.
[113] Koskinen 2013: 5.

Tietosuojavaltuutettu on antanut organisaatiolle vastauksen kysymykseen, jossa luottamusmies tiedusteli tietosuojavaltuutetulta työnantajan oikeutta valvoa sitä, millä sivustoilla työntekijä vierailee, minkälaisia tietoja työnantaja on oikeutettu keräämään sivustoilla käymisestä. Samassa tiedustelussa luottamusmies tiedusteli myös sitä, onko työntekijän mahdollista antaa suostumustaan siihen, että työnantaja tekee seurantaa sivustovierailuista kertyvistä tunnistetiedoista. Tietosuojavaltuutettu toteaa vastauksessaan, että työnantaja ei ole oikeutettu edes direktio-oikeuden nojalla valvomaan tai keräämään työntekijöiden sivustoselailusta muodostuvia tietoja. Voidaan myös katsoa, että työntekijöiden sivustovierailutiedot katsotaan henkilötiedoiksi, jonka myötä voimassa oleva tietosuojalainsäädäntö soveltuu myös sivustovierailujen tunnistamistietoihin.[114]

Työnantajan on toki mahdollista valvoa työntekijän netin käyttöä työnantajan tarjoamilla koneilla esimerkiksi sulkemalla pääsy tietyille sivustoille. On esimerkiksi yleistä, että työnantaja rajoittaa työkoneilla työntekijöiden pääsyn esimerkiksi pelisivustoille. Kuten muussakin työntekijöiden kohtelussa, on työnantajan sivustoille pääsyn estämisissä toimittava yhdenvertaisesti ja tasapuolisesti kaikkia työntekijöitä kohtaan. Tietosuojavaltuutettu antoi vastauksessaan kannanoton myös siihen, saako työnantaja estää työntekijöiden pääsyjä tietyille sivustoille. Tähän kysymykseen tietosuojavaltuutettu totesi työnantajan direktio-oikeuden ulottuvan. Työnantaja voi siis tämän perusteella päättää nettisurffailun pelisäännöistä sekä myös asettaa rajoituksia tietyille sivustoille pääsemisessä. Kannanoton mukaan työnantaja saa myös väärinkäytön ja sääntöjen vastaisen menettelyn huomatessaan kieltää ja huomauttaa työntekijää tästä ja vaatia työntekijää olla vierailematta näillä sivustoilla.[115]

Myös internetin valvontaan pätevät yleiset tietosuojan periaatteet. Työnantajan nettisurffailun valvonnassa on pidettävä mielessä tarpeellisuusvaatimus, onko valvonta

[114] Koskinen 2013: 6.
[115] Koskinen 2013: 6.

todella tarpeellista, vaikka se toteutuisikin luonnollisella tavalla.[116] Tämä vahvistaa sitä, että työnantajan on kaikessa toiminnassaan noudatettava yleisiä periaatteita.

### 5.5 Paikannustiedot

Nykypäivänä, kehittyneen teknologian myötä työnantajan tulee huomioida myös esimerkiksi puhelimien ja ajoneuvojen paikannustiedot teknisen valvonnan osalta. Laissa paikkatietoinfrastruktuurista (421/2009) paikkatieto määritellään olevan tietoa, joka antaa joko suoran tai epäsuoran ilmaisun johonkin yksilöityyn paikkaan tai maantieteelliseen alueeseen.[117] Osa paikannustiedoista voivat olla hyvinkin arkaluontoisia tietoja, jos ne yhdistetään muihin työntekijän henkilötietoihin. Lisäksi arkaluontoisuutta voi lisätä paikkatietojen käsittelytapa, jolloin tiedoista voi tulla hyvin arkaluontoisia.[118]

Tietosuojavaltuutettu on antanut näkemyksenä työntekijän työajoneuvon paikkatunnistamiseen sekä sallittavuuteen ja käyttötarkoitukseen. Ammattiliitolta tulleen selvityspyynnön mukaan kyseessä on asentaja, jolla on huoltoajoneuvo käytössä. Ajoneuvossa paikannuslaite on koko ajan päällä, eikä sitä saa kytkettyä pois päältä. Paikannuslaite muun muassa kerää tietoa siitä ketä, mihin ajankohtaan ja kuinka kauan työntekijä on tavannut. Lisäksi laite kerää myös tietoa reiteistä ja paikoista missä autolla on ajettu työajan ulkopuolella eli työntekijän vapaa-ajalla. Tietosuojavaltuutettu antaa yleistä ohjeistusta, eikä sillä ole oikeutta yleiseen lupa- tai kieltovaltaan. Näin ollen se nosti esiin nyt jo kumotun henkilötietolain (523/1999), Lain yksityisyydensuojasta työelämässä (759/2004) sekä sähköisen viestinnän tietosuojalain (516/2004). Työnantajan täytyy määritellä etukäteen paikannukselle perusteet sekä käyttötarkoitus, mikäli työnantaja aikoo paikantaa työntekijöitään. Tosiasiallinen peruste voi olla esimerkiksi se, että paikantamisella pyritään huolehtimaan työntekijöiden turvallisuudesta tai paikantamisen avulla työnantaja voi kohdistaa resurssit oikeisiin paikkoihin. Tietosuojavaltuutettu huomioi lausunnossaan myös työnantajan direktio-oikeuden eli johto- ja valvontaoikeuden.

---

[116] Koskinen 2013: 6.
[117] Korpisaari 2018: 36.
[118] Salokannel 2016: 545.

Direktio-oikeuden nojalla työntekijä on antanut sitoumuksen sille, että se työskentelee työnantajan johdon ja valvonnan alla. Paikannus voi siis olla tarpeellista ja perusteltua niissä tilanteissa, kun kyse on huoltohälytyksistä ja työnantajan tulee ohjata esimerkiksi lähinnä olevin asentaja tiettyyn paikkaan. Edellisissä lausunnoissaan tietosuojavaltuutettu on linjannut, ettei paikannustietojen hyödyntäminen esimerkiksi työajan valvontaan ole perusteltua. Työnantajan tulee varmistua siitä, että työntekijät, joita paikannus koskee, ovat tästä tietoisia.[119]

Nykyään myös puhelimien paikannustiedoista selviää sen maantieteellinen sijainti. Työnantajalla ei ole oikeutta paikantaa työntekijää tämän puhelimen paikkatietojen avulla ilman työntekijän antamaa suostumusta. Ainoa poikkeus työntekijän puhelimen paikannukseen on hätätilanne, jolloin työnantaja toimii yhteistyössä viranomaisten kanssa.[120] Myös työajanseurannasta voi selvitä työntekijöiden sijaintiedot. Tapauksessa 3843/163/20 tietosuojavaltuutetun toimisto on ottanut selvää, oliko työnantajalla oikeutta käsitellä työntekijöiden paikannustietoja heidän tekemien työaikaleimauksien kautta.

> Rekisterinpitäjä, työnantaja oli alkanut käyttää mobiilisovellusta, jota kautta työntekijät leimasivat työtuntinsa. Sovelluksen edellytyksenä oli se, että työntekijöiden on annettava hyväksyntä sijaintitietojen keräämiselle. Työnantaja kertoi, että se ei käsittele kyseisiä paikannustietoja mutta työaikaleimauksen aikainen paikka tieto tallennetaan ja tieto poistetaan heti, kun tallennukselle ei ole enää teknistä syytä. Työnantaja nosti esiin sen, että sovelluksen käyttö työaikojen leimaamiselle perustui työntekijöiden suostumukseen, sovellusta ei siis ollut pakko käyttää. Apulaistietosuojavaltuutettu totesi, että paikkatietojen kerääminen ei ollut tarpeellista. Näin ollen tarpeellisuusvaatimus ei täyttynyt, eikä tätä voida ohittaa suostumuksella. Tämän perusteella apulaistietosuojavaltuutettu katsoi, että tietojen käsittely on ollut tietosuojalainsäädännön vastaista. Seuraamuskollegio antoi asiasta päätöksen, jonka perusteella rekisterinpitäjä määrättiin tietosuojalainsäädännön vastaisesta toiminnasta 25 000 euron suuruiseen sakkoon.[121]

[119] TSV 87/41/2010.
[120] Saarinen 2011: 146.
[121] TSV 3843/163/20.

Työtekijöiden työajan seuraaminen on työnantajan vastuu. Vaikka työnantaja ajattelisi uuden sovelluksen tuovan parannusta työntekijöille ja työaikojen merkkaamiselle, ei asia ole tietosuoja näkökulmasta näin yksinkertainen. Työnantaja on ollut tietoinen siitä, että kyseinen sovellus kerää työtekijöiden sijaintietoja ja se on perustanut sovelluksen käytön ainoastaan suostumukselle. Työnantajan on aina huomioitava tietosuoja-asetuksen määrittämä tarpeellisuusvaatimus, josta ei voida poiketa edes suostumuksella.

Sijaintitietojen virheellisestä hallinnoimisesta voi koitua työnantajalle tietoturvaloukkaus, kuten 6813/ 171/21 apulaistietosuojavaltuutetun päätöksestä voidaan todeta. Pohjois-Savon sairaanhoitopiirin työntekijöiden tietokoneet sallivat tietokoneiden sijaintitiedot.

> Rekisterinpitäjä, Pohjois-Savon sairaanhoitopiiri oli ilmoittanut 19.8.2021 tietosuojavaltuutetun toimistolle tietoturvaloukkauksesta. Ilmoituksen mukaan työntekijöiden tietokoneet olivat automaattisesti sallineet paikannustiedot. Työntekijöiden ei ollut mahdollisuutta sammuttaa sijaintietoja tietokoneista. Rekisterinpitäjä on antanut ilmoituksesta lisätietoja tapahtuneesta, jonka mukaan se on aloittanut selvitykset sijaintietojen poissaamiseksi heti seuraavana päivänä. Lisäselvitysten mukaan rekisterinpitäjä on 14.3.2022 todennut, että paikannustiedot on poistettu käytöstä tietokoneista. Apulaistietosuojavaltuutetun toimisto tarkasteli, onko sijaintietojen käyttö noudattanut lain yksityisyydensuojasta työelämässä 3§ sekä onko rekisterinpitäjällä ollut mahdollisuutta tarkastella työntekijöiden tietoja. Lisäksi toimisto tutki, onko toiminta ollut tietosuoja-asetuksen 25 (2) artiklan mukaista. Apulaistietosuojavaltuutetun toimisto totesi, että menettely ei ole täyttänyt lain yksityisyydensuojasta työelämässä 3§ eikä tietosuoja-asetuksen 25 (2) artiklan vaatimuksia. Päätöksen mukaisesti rekisterinpitäjälle annetaan käsky poistaa mahdolliset historia dataan tallentuneet henkilötiedot. Lisäksi rekisterinpitäjä sai huomautuksen paikannustietojen päällä pitämisestä.[122]

Rekisterinpitäjän on aina huomioitava, että vaikka kerättyjä henkilötietoja ei käytettäisi mihinkään, ei se kuitenkaan saa näitä tietoja käsitellä eikä kerätä. Sijaintiasetukset ovat olleet Windows:in automaattisesti määrittämä oletusasetus, mutta vastuu tietojenkäsittelyn laillisuudesta säilyy aina rekisterinpitäjällä. Näin ollen rekisterinpitäjän vastuulla on huolehtia myös siitä, että tekniset asetukset noudattavat asetusta ja kansallisia lakeja. Loppukädessä osoitusvelvollisuus henkilötietojen käsittelystä, keräämisestä ja

[122] TSV 6813/ 171/21.

säilyttämisestä on aina rekisterinpitäjällä, eikä se voi tätä velvollisuutta ulkoistaa. Työnantajan on tietosuojalainsäädännön mukaisesti huomioitava myös työvälineiden tekniset asetukset. Velvoite on toki välttämätön työntekijöiden yksityisyydensuojaamiselle, mutta lisää entisestään työnantajien vastuita. Työnantajan on myös osattava hankkia tietotaitoa teknisellä tasolla.

# 6 TIETOTURVALOUKKAUS, VAHINGONKORVAUS JA VALVONTA

## 6.1 Tietoturvaloukkaus

Tietosuoja-asetus määrittää, että tietoturvaloukkauksella viitataan tilanteeseen, kun henkilötietoja vahingossa tai vastoin lakia tuhotaan, muutetaan tai ilman valtuuksia luovutetaan. [123] Tietoturvaloukkaukset voivat johtua erilaisista asioista; tietoturvaloukkaus voi olla muun muassa teknisestä viasta johtuva liian laaja pääsy rekisteröidyn tietoihin tai muu järjestelmän aiheuttama virhe. Tietoturvaloukkaus voi tulla kyseeseen myös huolimattomuudesta, esimerkiksi jos työntekijä lähettää henkilötietoja sisältävän sähköpostin väärälle vastaanottajalle.[124]

Rekisterinpitäjän, kuten työnantajan, on selvitettävä mahdolliset uhat tietoturvaan liittyen sekä estettävä mahdollisten tietoturvauhkien tapahtuminen kohtalaisuuden nimissä. [125] Työnantajan on dokumentoiva kaikki tietoturvaloukkaukset tietosuoja-asetuksen mukaisesti. [126] Dokumentaatiossa on hyvä kirjata ylös muun muassa tarkka kuvaus siitä, mitä on tapahtunut, montako rekisteröityä loukkaus on koskenut sekä mitä työnantaja on tehnyt, jotta vastaavaa ei tapahtuisi uudestaan tulevaisuudessa. Tietosuojavaltuutetun toimiston mukaan dokumentaatiovelvollisuuteen kuuluu myös järjestelmien lokitietojen dokumentointi, mikäli kyseessä on tietoturvaloukkaus järjestelmään. Työnantajan on tämän nojalla säilytettävä tarkat lokitiedot loukkauksen ajalta.[127]

Työnantaja voi esimerkiksi säännöllisin väliajoin järjestää koko henkilöstölle koulutusta ja opetusta tietoturvaloukkauksien ehkäisemiseksi sekä oikeaoppisesta henkilötietojen käsittelystä. Hyvä käytäntö on, että työnantaja järjestää aina uusille työntekijöille kattavan perehdytyksen tietosuojaan sekä järjestää säännöllisin väliajoin myös kertauskoulutusta.

---

[123] Hanninen ym. 2017: 23.
[124] Wennäkoski 2016: 74.
[125] Hanninen ym. 2017: 23.
[126] EU:n yleinen tietosuoja-asetus artikla 33.
[127] Tietosuojavaltuutetun toimisto: https://www-edilex-fi.proxy.uwasa.fi/uutiset/72522?allWords=tietoturvaloukkaus&offset=1&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=1292292.

Tietosuoja-asetuksen 33 artiklan mukaisesti rekisterinpitäjän on ilmoitettava valvontaviranomaiselle tietoturvaloukkauksesta 72 tunnin sisällä siitä, kun loukkaus on todettu. Suomessa valvontaviranomaisena toimii Tietosuojavaltuutetun toimisto. Mikäli tietoturvaloukkauksesta ei koidu luonnolliselle henkilölle riskiä, ei ilmoitusta valvontaviranomaiselle tarvitse tehdä. Mikäli loukkaus on vakava ja siitä arvioidaan koituvan riskiä henkilön oikeuksiin liittyen, tulee työnantajan antaa viranomaisilmoituksessaan tarkka kuvaus siitä, mitä loukkauksessa on tapahtunut, kuinka monta luonnollista henkilöä henkilötietojen loukkaus on koskenut sekä mihin ryhmään henkilöt kuuluvat. Lisäksi työnantajan tulee ilmoituksessa kertoa tietosuojavastaavan tiedot, mitkä ovat tietoturvaloukkauksen mahdolliset seuraamukset sekä minkälaisia toimia rekisterinpitäjä on tehnyt, jotta se ehkäisee tietoturvaloukkauksia tulevaisuudessa. [128]

Rekisterinpitäjällä on tosiaan velvollisuus ilmoittaa loukkauksista valvontaviranomaiselle, henkilötietojen käsittelijällä on myös vastaava ilmoitusvelvollisuus mutta rekisterinpitäjälle. Näin ollen asetuksen 33 artikla asettaa ilmoitusvelvollisuuden myös henkilötietojen käsittelijälle. Koska organisaatiot ulkoistavat yhä enemmän palvelujaan, on myös henkilötietojen käsittelijälle asetettu ilmoitusvelvollisuus. Henkilötietojen käsittelijän ilmoituksen jälkeen rekisterinpitäjän on tehtävä oma arvionsa loukkauksen vakavuudesta. Joka tapauksessa myös näissä tilanteissa on rekisterinpitäjän vastuulla ilmoittaa loukkauksesta tarvittaessa sekä rekisteröidylle että valvontaviranomaiselle. [129]

Jos kyseessä on tietoturvaloukkaus, jonka arvioidaan aiheuttavan vakavaa haittaa rekisteröidylle, on rekisterinpitäjän ilmoitettava tästä valvontaviranomaisen lisäksi myös itse rekisteröidylle 34 artiklan mukaisesti. Vakavalla haitalla viitataan muun muassa tilanteeseen, jos loukkaus aiheuttaisi suuren uhan rekisteröidyn oikeuksille tai vapauksille. Uhan määritelmän voidaan katsoa olevan monikäsitteisempi ja yleensä onkin niin, että loukkauksesta ilmoitetaan harvemmin itse rekisteröidylle ja useammin

[128] EU:n yleinen tietosuoja-asetus artikla 33.
[129] Parkkamäki 2018: 147–148.

valvontaviranomaiselle. Merkittävän uhan voidaan katsoa muodostuvan esimerkiksi silloin, jos loukkaus mahdollistaisi identiteettivarkauden tai maineen kärsimisen. Jos asetus ei määrittäisi tällaista käytäntöä, olisi rekisteröidyn vaikeampi varmistua siitä, kuinka organisaatio hänen henkilötietojaan käsittelee. Rekisteröidyn ilmoitusvelvollisuus koskee vain rekisterinpitäjää. [130] Jos työnantaja esimerkiksi lähettäisi sähköpostin, joka pitäisi sisällään toisen työntekijän tai hakijan henkilötietoja, kuten nimen, ei tästä aiheutuisi vielä vakavaa haittaa rekisteröidylle. Jos puolestaan esimerkiksi työntekijöillä olisi pääsy toistensa järjestelmäprofiileihin teknisestä viasta johtuen, olisi loukkaus jo vakava ja rekisterinpitäjä olisi ilmoitusvelvollinen sekä rekisteröidylle että valvontaviranomaiselle.

Toki vakavasta tietoturvaloukkauksesta on kyse myös silloin, jos esimerkiksi henkilöiden arkaluontoisia tietoja päätyy kolmansille osapuolille. Hyvä esimerkki hyvin vakavasta tietoturvaloukkauksesta on paljon esillä ollut Psykoterapiakeskus Vastaamon tapaus. Tietosuojavaltuutettu sai Vastaamolta syksyllä 2020 tiedonannon, jossa se ilmoitti, että sen potilastietojärjestelmä on ollut iskun kohteena, ja ulkopuolinen taho oli päässyt sisälle potilastietojärjestelmään. Vastaamolla oli apulaistietosuojavaltuutetun selvityksen perusteella huomattavia tietoturvahaittoja, eikä se ole varmentunut potilastietojen turvallisesta käsittelystä. Vastaamo määrättiin rekisterinpitäjänä ilmoittamaan loukkauksesta ja henkilötietojen vuodosta suoraan rekisteröidyille. Lisäksi Vastaamolle langetettiin 608 000 euron suuruinen hallinnollinen sanktio.[131]

Tietosuojavaltuutetun toimisto toimii Suomessa valvontaviranomaisena ja huolehtii tietoturvaloukkauksien oikeasta käsittelystä. Tietosuojavaltuutetun antamassa päätöksessä 2437/161/22, työnantaja oli laiminlyönyt työntekijöihinsä kohdistuneen tietoturvaloukkauksen ilmoittamisen valvontaviranomaiselle. Ilmoitus on tietosuoja-asetuksen artiklan 33 mukaisesti tehtävä ilman aiheetonta viivästystä.

> Rekisterinpitäjä, Ulkoministeriö teki ilmoituksen henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle 24.1.2022. Ulkoministeriön antamien tietojen mukaan

[130] Parkkamäki 2018: 147–148.
[131] TSV 1150 /161/ 2021.

> loukkauksen kohteena olivat Ulkoministeriön työntekijät, jotka työskentelivät ulkomailla. Ilmoituksen mukaan Ulkoministeriö on tiedottanut asianomaisia tietoturvaloukkauksesta sekä ilmoittanut sen johtuvan vakoiluhaittaohjelmasta. Ulkoministeriön antaman selvityksen mukaan myöhässä ilmoittaminen johtui siitä, että se selvitti tietoturvaloukkausta. Syynä myöhästymiselle oli lisäksi kansallinen turvallisuus sekä tiedotusvastuiden jakautumisten epäselvyyteen. Apulaistietosuojavaltuutetun näkemyksen mukaan, Ulkoministeriö ei ollut noudattanut tietosuoja-asetuksen 33 artiklan 1 kohtaa. Artiklan 1 kohta määrittää tietosuojaloukkauksen 72 tunnin ilmoitus aikarajan, tietosuojaloukkauksesta on ilmoitettava ilman aiheetonta viivästystä 72 tunnin aikarajassa tietosuojavaltuutetun toimistolle. Tietosuoja-asetuksen mukaan rekisteröidylle voi aiheutua huomattavaa haittaa, jos rekisterinpitäjä ei puutu loukkaukseen tarpeeksi tehokkaasti. Ilmoituksen mukaan Ulkoministeriö oli antanut tietoturvaloukkauksen tiedoksi rekisteröidyille mutta tietosuojavaltuutettu katsoi, että sitäkään ei ollut tehty ilman aiheetonta viivästystä.[132]

Tietosuojavaltuutettu katsoi päätöksessään, että Ulkoministeriö oli toiminut tietosuoja-asetuksen vastaisesti artiklojen 33 ja 34 osalta. Rekisterinpitäjä ei ollut ilmoittanut loukkauksesta ilman aiheetonta viivästystä valvontaviranomaiselle, eikä rekisteröidyille. Tietosuojavaltuutettu antoi tapauksesta rekisterinpitäjälle asetuksen 58 artiklan mukaisen huomautuksen.

On huomattavan tärkeää, että tietoturvaloukkaukset käsitellään heti niiden tultua ilmi, myös mahdollisten viikonloppujen aikana. Tämä siis väistämättä vaatii organisaation tietosuojavastaavalta tarvittaessa työntekoa myös esimerkiksi viikonloppuisin tai pitkien pyhien aikana. Toki päätöksistä voidaan päätellä, että ilmoitusten myöhästyminen loukkauksesta rekisteröidylle ja valvontaviranomaiselle ei ole niin vakava rike. Kun verrataan esimerkiksi tietosuojalainsäädännön vastaiseen henkilötietojen käsittelyyn tai puutteelliseen tietoturvaan, ilmoitusvelvollisuudesta ei ole määrätty hallinnollisia seuraamusmaksuja. Ulkoministeriön tapauksessa rekisterinpitäjä sai ainoastaan huomautuksen, kun puolestaan tietosuojalainsäädännön vastainen henkilötietojen käsittely on johtanut huomattaviin sakkoihin.

Kuten edellä on todettu, organisaatiot ulkoistavat entistä enemmän palvelujaan ja on tilanteita, jolloin tietoturvaloukkaus ei ole suoraan rekisterinpitäjästä johtuva, mutta rekisterinpitäjä on kuitenkin perimmäisenä vastuussa velvoitteiden hoitamisesta.

---

[132] TSV 2437/161/22.

Tietosuojavaltuutetun käsittelemässä tapauksessa 2691/171/19 henkilötietoja sisältäviä asiakirjoja hävisi kolmannen osapuolen toimesta.

> Kelan asiakkaiden asiakirjoja sisältämä paketti hävisi Postin käsittelyssä. Asiakirjat sisälsivät arkaluontoisia tietoja asiakkaista, kuten terveydentilaa ja taloudellista tilannetta koskevia tietoja. Asiakirjat huomioiden, rekisteröidyille voi mahdollisesti koitua huomattavaa haittaa, kuten henkilöllisyyden varastaminen tai taloudellinen vaurio. Tietosuojavaltuutetun toimisto määräsi rekisterinpitäjän ilmoittamaan asiasta rekisteröidyille kenen tietoja oli hävinnyt sekä tekemään tarvittava dokumentaatio. [133]

Tapauksesta voidaan päätellä, että Kela rekisterinpitäjänä ei ole vastuussa huolimattomuudesta, eikä se ole voinut vaikuttaa henkilötietojen katoamiseen, eikä ole siitä johtuen aiheuttanut tietoturvaloukkausta. Näin ollen tietosuojavaltuutetun toimisto ei määrännyt rekisterinpitäjälle seuraamusmaksua tai edes antanut huomautusta asiasta. Vaikka tietosuojalainsäädäntö asettaa työnantajille huomattavia velvoitteita, on tapausten tarkastelussa myös inhimillinen puoli. Jos rekisterinpitäjä ei aidosti olisi voinut tehdä henkilötietojen käsittelyssä mitään toisin, ei sille määrätä tapauksesta rangaistusta, vaikkakin rekisterinpitäjä on loppukädessä vastuussa kaikesta henkilötietojen käsittelystä.

### 6.2 Tietosuoja-asetuksen asettama korvausvastuu

EU:n tietosuoja-asetus asettaa korvausvastuukäytännöt henkilötietojen lainvastaiselle käsittelylle. Perustana asetuksessa toimii se, että kyse on täyden korvauksen periaatteesta tarkoittaen sekä aineellisia että aineettomia vahinkoja. [134] Asetuksen mukaan väärinkäytöstä syntyvä vastuu ilmenee rekisterinpitäjälle tai tietoja käsittelevälle hallinnollisena sakkona tai vahingonkorvausvastuuna.[135] Asetus on myös laajentanut vahingonkorvausvastuuta pelkästä rekisterinpitäjästä myös henkilötietojen käsittelijään.[136] Tietosuojaviranomaiset huolehtivat väärinkäyttötilanteista, tietoturvaloukkauksista ja vahingonkorvausvastuista. Erityisesti mahdollisissa tietomurtotilanteissa, korvausvastuu voi nousta isoiksikin, sillä nämä voivat huonoimmissa tilanteissa synnyttää petoksia toisten

[133] TSV 2691/171/19.
[134] Wennäkoski 2017:71.
[135] Heiskala ym. 2018: 8.
[136] Heiskala ym. 2018: 25–26.

nimissä tai identiteettivarkauksia. [137] Asetus määrittää tietoturvaloukkauksen tapahtuneen silloin, kun henkilötietoja muun muassa luovutetaan, muutetaan tai hävitetään joko vahingossa tai lainvastaisesti. Tietoturvaloukkauksesta on kyse myös silloin, kun henkilötietoihin on pääsy jollakin luvattomalla henkilöllä. [138]

Asetuksen 83 artikla määrittelee henkilötietojen väärinkäytöstä aiheutuvat seuraukset sekä vahingonkorvausvastuut. Asetus määrittää rekisterinpitäjille ja henkilötietojen käsittelijöille ankaran vastuun, eli sakko ei edellytä syyllisyyttä. Korvauksen tai sakon määrään vaikuttaa kuitenkin huomattavasti tahallisuus ja tuottamuksellisuus, jotka otetaan huomioon. Asetus määrittää huomattavan korkeat enimmäismäärät sakoille. Tulkintojen mukaan merkittävän korkeat enimmäismäärät on lähtökohtaisesti säädetty suuria internetyhtiöitä, kuten Googlea ja Facebookia varten.[139] Alkuvuodesta 2019, Ranskan kansallinen valvontaviranomainen, CNIL, on määrännyt huomattavan suuren seuraamusmaksun Googlelle. Hallinnollinen seuraamusmaksu oli suuruudeltaan 50 miljoonaa euroa.[140] Tietosuoja-asetuksen asettama hallinnollinen sanktio määräytyy koko organisaation maailmanlaajuisen liikevaihdon pohjalta.[141]

Mikäli henkilölle aiheutuu tietosuoja-asetusrikkeestä vahinkoa, henkilö on tällöin oikeutettu korvaukseen joko rekisterinpitäjältä tai tietojen käsittelijältä. Kyseessä voi olla aineellinen tai aineeton vahinko. Jotta henkilölle syntyy korvausoikeus, vahingon ja käsittelyn rikkeen välillä tulee olla selvä syy-yhteys. Vahingonkorvauksessa pätee asetuksen mukaan sama ankara vastuu kuin sakkojen määräämisessä. Eli vahingonkorvaus syntyy jo pelkällä henkilötietojen väärinkäsitellyllä, joka aiheuttaa henkilölle vahinkoa. Korvaus tarkoittaa täyttä ja tuntuvaa korvausta aiheutuneesta vahingosta. EU:n lainsäätäjän mukaan vahinko asetuksen vastaisesta käsittelystä voi olla aineellisen ja aineettoman vahingon lisäksi myös fyysinen. Lainsäätäjä on lisäksi painottanut, että vahinko voi johtaa

[137] Heiskala ym. 2018: 21–22.
[138] Hanninen ym. 2017: 23.
[139] Heiskala ym. 2018: 22.
[140] Läng & Taka 2018: 61.
[141] Parkkamäki 2018: 128.

huomattaviin taloudellisiin menetyksiin, luottamuksen kärsimiseen tai maineen menettämiseen sekä muihin sosiaalisiin haittoihin.[142]

Rekisterinpitäjällä ja henkilötietojen käsittelijällä on asetuksen mukainen yhteisvastuu rikkeen korvauksesta. Jos rekisterinpitäjä ja henkilötietojen käsittelijä ovat ottaneet osaa samaan käsittelyyn, he ovat kaikki vastuussa tapahtuneesta vahingosta. Henkilötietojen käsittelijälle vastuu syntyy vasta siinä vaiheessa, kun se on toiminut asetuksen vastaisesti käsittelijälle osoitetuissa vastuissa tai se ei ole toiminut rekisteripitäjän asettamien ohjeiden mukaisesti. Kun he ovat suorittaneet täyden korvausmaksun tapahtuneesta vahingosta, heillä on oikeus nostaa takautumiskanne myöhemmin. Takautumiskanne voidaan siis nostaa muita rekisterinpitäjiä tai käsittelijöitä vastaan, jotka ovat ottaneet osaa samaan käsittelyyn.  Luonnollisesti, jos he molemmat pystyvät osoittamaan, että heillä ei kummallakaan ole vastuuta aiheutuneesta vahingosta, he vapautuvat yhteisvastuusta.[143] Toki loppukädessä perimmäinen vastuu ja osoitusvelvollisuus on aina rekisterinpitäjällä. Siksi on tärkeää, että rekisterinpitäjä pystyy osoittamaan, että se on henkilötietojen käsittelijää valitessa selvittänyt sen asianmukaisen tietosuojan tason. [144]

Kuten aikaisemmin on mainittu korvausta arvioidessa, otetaan huomioon rekisterinpitäjän tai käsittelijän tahallisuus ja tuottamuksellisuus. Tietosuojarikkeet voivat tulla järjestelmävioista tai teknisten varotoimien puuttumisesta. Rike voi siis perustua laiminlyöntiin ja huolehtimattomuuteen. Jos yritys joutuu ulkopuolelta tulevan tietosuojariskin kohteeksi, yrityksen varotoimilla voi olla suurikin arvo, kun arvioidaan vahingonkorvauksia. [145]

[142] Heiskala ym. 2018: 25–26.
[143] Heiskala ym. 2018: 26–27.
[144] Parkkamäki 2018: 127.
[145] Korpisaari 2017: 74.

### 6.3 Ryhmäkanteet

Tietosuojarikkeen vahinko voi olla todella suuri, mutta yksittäiselle henkilölle korvausten hakeminen ei ole välttämättä oikeusteitse kovin realistista.[146] Ryhmäkanteella tarkoitetaan sitä, että monella henkilöllä on samanlainen vaatimus jotakin tahoa kohtaan.[147] Tällaisessa tilanteessa tietosuoja-asetuksen mukaan henkilöllä on oikeus nimittää voittoa tavoittelematon yhdistys ajamaan asiaa hänen puolestaan ryhmäkanteen kautta. Yhdistyksen tulee olla asianmukainen ja sen toiminnan tulee noudattaa jäsenmaan lainsäädäntöä.[148] Kansallisesti ryhmäkanteen ajajana toimii kuluttaja-asiamies, joka nostaa tahoa vastaan ryhmäkanteen sekä edustaa ryhmäkanteen muodostamaa ryhmää.[149] Yhdysvaltoihin verrattuna ryhmäkanne on tämä uusi mahdollisuus EU:ssa.[150] Toki itse tietosuoja-asetus ei aloittanut keskustelua ryhmäkanteista, vaan EU:n osalta keskustelu ryhmäkanteista on noussut esiin jo kilpailuoikeuden mietinnän kohdalla. [151] Ryhmäkanteiden oikeudenkäyntikulut eivät aiheudu ryhmäkanteen osapuolten maksettaviksi, vaan ne ovat joko kuluttaja-asiamiehen tai kannetta vastaan nostetun tahon vastuulla.[152]

Ryhmäkanteiden mahdollistamisessa on toki organisaatioille jälleen taloudellista painetta. Asetuksen mukaan organisaatiolle voidaan suurimmillaan määrätä hallinnollinen seuraamusmaksu, joka on 4 % sen liikevaihdosta. Hallinnollisen seuraamusmaksun lisäksi luonnollinen henkilö voi nostaa myös ryhmäkanteen organisaatiota vastaan. Nämä kaksi yhdistettynä voivat olla todellinen taloudellinen rasite yritykselle, eikä sen maksukyky välttämättä ole riittävä molempiin varsinkaan odottamattomissa tapauksissa. Toki tässä voi tulla eteen myös rekisteröidyn oikeusturvan toteutuminen. On mahdollista, että näin kovissa mahdollisissa sanktioissa organisaatio ei ole maksukykyinen ja rekisteröity ei saa korvauksia, joihin olisi oikeutettu. [153]

---

[146] Wennäkoski 2017: 81–82.
[147] Tuomioistuinlaitos: https://oikeus.fi/tuomioistuimet/fi/index/asiat/riita-asiat/ryhmakanne.html.
[148] Wennäkoski 2017: 81–82.
[149] Tuomioistuinlaitos https://oikeus.fi/tuomioistuimet/fi/index/asiat/riita-asiat/ryhmakanne.html.
[150] Wennäkoski 2017: 81–82.
[151] Wikberg 2011: 226.
[152] Tuomioistuinlaitos: https://oikeus.fi/tuomioistuimet/fi/index/asiat/riita-asiat/ryhmakanne.html.
[153] Wennäkoski 2017: 81–82.

Toki yleensä ryhmäkanteiden vaatimukset eivät ole olleet järin suuria. Facebookia vastaan on nostettu ryhmäkanne, jossa vaatimuksena oli 500 euron rahallinen korvaus henkilöä kohden. Ryhmäkanteiden osalta on kuitenkin syytä varautua siihen, että ryhmäkanteiden yhteenlaskettu korvaussumma voi nopeasti noustakin merkittäväksi. [154]

### 6.4 Kansallinen sääntely ja korvausvastuu

Kansallisesti lainsäädäntö turvaa henkilöitä henkilötietojen väärinkäytöstä ja luo vahingonkorvausvastuun rikkomuksille. Laki yksityisyydensuojasta työelämässä ja rikoslaki toimivat keskeisimpänä kansallisena lainsäädäntönä, kun puhutaan tietosuojarikkeiden rangaistus- ja korvausvastuusta. [155] Lain yksityisyyden suojasta työelämässä 24 § asettaa työnantajalle perusteet, milloin työnantaja voidaan tuomita rangaistukseen, jos se tahallisesti tai törkeästi laiminlyö laissa asetettuja määräyksiä. Lain asettama rangaistusvaatimus väistyy, jos toiminta katsotaan ankarammaksi tuomituksi jossakin muussa laissa.[156] Rikoslain mukainen rikosoikeudellinen vastuu tulee käytäntöön vain niissä tilanteissa, kun tietosuojalain vastaista menettelyä ei ole asetettu hallinnollisten seuraamusmaksujen ulottuvuuteen.[157]

Tässä vastuu on myös työntekijöillä, sillä rikoslainsäädäntö pätee myös niissä tilanteissa, kun työnantajan palveluksessa oleva työntekijä toimii lainvastaisesti. Näin voi käydä, jos esimerkiksi työntekijä hävittäisi tai poistaisi tietoja ilman, että huolehtisi niiden tietoturvallisesta hävittämisestä. [158] Näin ollen on tärkeää, että työnantaja järjestää säännöllisin väliajoin koulutuksia koko henkilöstölle tietosuojaprosesseista. Vakavasta tietosuojalainsäädännön vastaisesta henkilötietojen käsittelystä voidaan rekisterinpitäjä tai henkilötietojen käsittelijä tuomita jopa yhdeksi vuodeksi vankeuteen.[159]

---

[154] Wennäkoski 2017: 81.
[155] Syrjänen 2006: 143.
[156] Syrjänen 2006: 143.
[157] Paasonen ym. 2021: 971.
[158] Paasonen ym. 2021: 979.
[159] Paasonen ym. 2021: 979.

Äärimmäisen tärkeä huomio rikosoikeudellisessa vastuussa on kuitenkin se, että se tulee kysymykseen vain tilanteissa, joissa tietosuojalainsäädännön vastainen henkilötietojen käsittely ei ole asetuksen hallinnollisten sakkojen soveltamisalassa. Käytännössä siis rekisterinpitäjä ja henkilötietojen käsittelijä ovat aina tietosuoja-asetuksen hallinnollisten seuraamusmaksujen soveltamisalassa, kyse voisi siis olla yksittäisestä työntekijästä. Jos esimerkiksi sairaanhoitajalla on pääsy potilastietojärjestelmään ja jos hän ainoastaan uteliaisuudestaan käsittelisi ja katsoisi muiden kuiden omien potilaiden tietoja, olisi tämä lainvastaista ja sairaanhoitaja kuuluisi rikosoikeudellisen vastuun piiriin. [160]

Suomessa tietosuojavaltuutetun toimisto on määritellyt, että tietosuojalain vastainen henkilötietojen käsittely voi johtaa seuraamusmaksuun, sakkoon, joka voi enimmillään olla 4% koko organisaation liikevaihdosta tai enintään 20 miljoonaa euroa. [161] Päätökset hallinnollisista seuraamusmaksuista tekee tietosuojavaltuutetun toimiston seuraamuskollegio. Seuraamuskollegion antamat päätökset eivät ole lainvoimaisia, rekisterinpitäjillä on mahdollisuus valittaa annetuista päätöksistä hallinto-oikeuteen. Seuraamuskollegiolla tarkoitetaan tietosuojavaltuutetuntoimiston ja apulaistietosuojavaltuutetuntoimiston yhdessä tekemää päätöstä.[162]

Tietosuojavaltuutetun toimisto on syyskuussa 2019 ottanut käsittelyyn tapauksen 4282/ 161/ 21, jossa tarkasteltiin kantelua koskien turvallista henkilötietojen käsittelyä. Henkilötietojen turvallisen käsittelyn lisäksi kantelu koski rekisteröidyn oikeutta pyytää yritystä poistamaan häntä koskevat henkilötiedot, eli oikeus tulla unohdetuksi. Tapaus tuli tietosuojavaltuutetun käsiteltäväksi, kun rekisteröity ilmaisi epäilynsä siitä, että rekisterinpitäjä, Matkatoimisto, ei toimisi tietosuojalain mukaisesti sähköisen viisumilomakkeen tiedoissa. Rekisterinpitäjä on käsittelyn aikana hakeutunut konkurssiin, tammikuussa 2021.

[160] Paasonen ym. 2021: 979.
[161] TSV 2477/161/21.
[162] TSV 2477/161/21.

> Rekisteröidyn antamien tietojen mukaan sähköinen viisumilomake on avoimessa verkossa sekä yhteys on salaamattoman HTTP-yhteyden takana. Lomake sisältää rekisteröidyn henkilötietoja. Rekisteröity on lisäksi vedonnut oikeuteensa tulla unohdetuksi, mutta ei ole saanut pyyntöön vastausta rekisterinpitäjältä. Tietosuojavaltuutetun toimisto on pyytänyt rekisterinpitäjältä kaksi kertaa selvitystä asiaan, joulukuussa 2019 ja toukokuussa 2020, mutta rekisteripitäjä ei ole vastannut pyyntöihin. Matkatoimisto vastasi toiseen hallintolain (434/2003) mukaiseen kuulemispyyntöön. Vastauksessaan se perusteli asiaa niin, että se on omistanut vain 40%. Matkatoimiston mukaan sillä on ollut erilliset järjestelmät ja asiakasluottelut eikä se näin ole käsitellyt henkilötietoja. Matkatoimisto vetosi siihen, että tietosuoja-asetuksen mukaan konsernisuhdetta ei voitaisi katsoa tapahtuneen tässä tapauksessa, sillä yrityksillä on osoitetusti eri järjestelmät. Matkatoimisto on kuitenkin kuulemiseen mennessä käsitellyt rekisteröidyn tietojen poistopyynnön. Tietosuojavaltuutetun toimisto tarkastelu onko seuraavat vaatimukset huomioitu; tietosuoja-asetuksen 5 artiklaa, luottamuksellisuuden periaatetta, tietosuoja-asetuksen 17 artiklaa, jonka mukaisesti rekisterinpitäjä on velvollinen poistamaan rekisteröidyn henkilötiedot, tietosuoja-asetuksen 25 artiklaa asianmukaisista teknisistä toimista sekä tietosuoja-asetuksen 32 artiklaa asianmukaisesta turvallisuustasosta. Tietosuojavaltuutetun toimisto ei antanut rekisterinpitäjälle käskyä poistaa turvattomat henkilötiedot, koska matkatoimistoa ei enää ollut. Tietosuojavaltuutetun toimisto nosti kuitenkin esiin tietosuojalain 24§ mukaisen hallinnollisen sakkorangaistuksen. Sakko annettiin edelleen päätettäväksi seuraamuskollegiolle.[163]

Seuraamuskollegio antoi päätöksen 6500 euron sakkorangaistuksesta. Sakon summa-arvioi perustui konsernin liikevaihdolle.

Tietosuojavaltuutetun seuraamuskollegio on antanut sakkorangaistuksen huhtikuussa 2021 tapaukselle 2477/161/21. ParkkiPate Oy ei ollut käsitellyt henkilötietoja voimassa olevan tietosuojalainsäädännön mukaisesti. Tietosuojalainsäädännön vastainen menettely on koskenut muun muassa sitä, että yritys ei ole toteuttanut rekisteröityjen oikeuksia, kuten oikeutta tulla unohdetuksi, myöskään henkilötietojen säilytysajat eivät ole olleet lainsäädännön mukaisia. Lisäksi rekisterinpitäjän menetelmät rekisteröityjen tunnistamiseen eivät ole olleet lainmukaisia. Tietosuojavaltuutetun seuraamuskollegio langetti rekisterinpitäjälle 75 000 euron sakkorangaistuksen. [164]

Erityisesti suurien työnantajien on suositeltavaa olla tietoisia seuraamusmaksun enimmäismääristä. Työnantajalle voi pahimmillaan tulla todella suuret sakkorangaistukset

[163] TSV 4282/ 161/ 21.
[164] TSV 2477/161/21.

maksettaviksi, jos se ei käsittele työntekijöiden henkilötietoja lainsäädännön velvoittamalla tavalla.

Vahingonkorvausvastuun ja hallinnollisten seuraamusmaksujen osalta on tiettyjä eroja yksityisten yritysten ja julkisten organisaatioiden osalta. Hallinnollisten sakkorangaistuksien määrääminen viranomaisille tarkoittaisi sitä, että seuraukset suuntautuisivat asiakkaisiin. Julkisten organisaatioiden asiakkaat kärsisivät siis tästä syyttöminä sen myötä, että hallinnollinen sakko laskisi julkisten organisaatioiden kykyä suorittaa julkisia tehtäviä. [165] Asetus antaa kansallisesti joustoa hallinnollisten seuraamusmaksujen määrittämiselle. Suomessa onkin tehty kansallisesti päätös, että hallinnollista sakkorangaistusta ei kohdenneta julkihallinnon elimille. Päätöstä on puollettu sillä, että julkisella puolella on käytössä jo virkavastuu. Virkavastuu ulottuu tietosuojalainsäädännön lainmukaisuuden noudattamiseen.[166]

## 6.5 Valvonta

### 6.5.1 Kansallinen valvontaviranomainen

Tietosuoja-asetus velvoittaa jokaista EU:n jäsenmaata nimittämään oman kansallisen valvontaviranomaisen, joka valvoo kansallista tietosuojalainsäädäntöä. [167] Kansallisesti tietosuojalainsäädännön valvonta kuuluu tietosuojavaltuutetun toimistolle. Tietosuojavaltuutetun toimisto on virallinen valvontaviranomainen Suomessa oikeusministeriön yhteydessä. [168] Yhdessä tietosuojavaltuutetun kanssa tietosuojalainsäädäntöä valvoo kansallisesti apulaistietosuojavaltuutetun toimisto. Tietosuoja-asetuksen mukaisesti kansallisten valvontaviranomaisten on toimittava tiiviissä sekä vilpittömässä yhteistyössä. Virallisella valvontaviranomaisella on ensisijainen valta tehdä päätöksiä. Tästä

[165] Mäntylä ym. 2022: 35–36.
[166] Mäntylä ym. 2022: 94–95.
[167] EUT lehdistötiedote 103/21.
[168] Tietosuojavaltuutetun toimisto, https://tietosuoja.fi/tietosuojavaltuutetun-toimisto.

huolimatta tietosuojavaltuutetun toimisto ei voi jättää muita valvontaviranomaisia huomiotta, vaan näiden on toimittava jatkuvassa yhteistyössä. [169]

Jos siis esimerkiksi työntekijä epäilee työnantajan henkilötietojen käsittelyn olevan tietosuojalainsäädännön vastaista, on työntekijällä mahdollisuus saattaa asia tietosuojavaltuutetun toimiston tietoisuuteen. Olisi myös suotavaa, että työnantaja saattaa tämän työntekijöiden oikeuden heidän tietoisuuteensa.

### 6.5.2 Kansainvälinen ja rajat ylittävä valvonta

Kansainvälisesti Unionin tietosuojavalvonnasta vastaa Euroopan tietosuojaneuvosto ja EU:n tietosuojavaltuutettu. Euroopan tietosuojaneuvosto koostuu eri jäsenmaiden valvontaviranomaisten johdosta.[170] Kuten myös kansallisesti tietosuojavaltuutetun tehtäviin kuuluu valvonnan lisäksi myös ohjeiden ja suosituksien antaminen. Näin myös yksi Euroopan tietosuojaneuvoston tehtävistä on valvonnan lisäksi tulkita tietosuoja-asetus ja antaa jäsenmaille tästä tulkintoja ja suosituksia. Sen lisäksi, että Euroopan tietosuojaneuvosto valvoo tietosuojalainsäädännön toteutumista eri jäsenvaltioissa, on sen tehtävänä valvoa myös henkilötietojen käsittelyä ja tiedonsiirtoa kolmansiin maihin. Neuvosto muun muassa valvoo ja antaa ohjeet sille, että kolmannen maan tietosuojan laadun on oltava vähintään EU:n tietosuoja-asetuksen standardien mukainen. [171] Tietosuojaneuvoston yksi tärkeimmistä tehtävistä on varmistaa, että asetuksen tulkinta ja soveltaminen on yhdenmukaista kaikkien jäsenvaltioiden välillä. [172]

On myös mahdollista, että valvonta ja tietosuojalainsäädännön lainvastaisen käsittelyn tarkastelu tapahtuu yli jäsenmaiden rajojen. Tällöin kyse on rajat ylittävästä tietosuojalainsäädännön valvonnasta. Jos siis esimerkiksi työnantaja toimii kansainvälisesti, monessa Euroopan maassa, on mahdollista, että toisen jäsenmaan valvontaviranomainen

[169] EUT lehdistötiedote 103/21.
[170] Lång & Taka 2018: 66.
[171] Kurvinen 2021: 993–996.
[172] Lång & Taka 2018: 66.

aloittaa tietosuojalainsäädännön vastaisen henkilötietokäsittelyn tapauksen käsittelyn. EU:n tuomioistuin on antanut lausunnon ja tulkintansa tietosuoja-asetuksen määrittämistä valvontaviranomaisten oikeuksista ja valtuuksista. EU:n tuomioistuimen suuren jaoston lausunnon mukaan, tietosuoja-asetus, tiettyjen edellytyksien täyttyessä, antaa mahdollisuuksia toisen jäsenmaan valvontaviranomaiselle. Jäsenvaltion valvontaviranomaisella on näin ollen tietyissä tilanteissa oikeus tuoda tietosuoja-asetuksen vastaiset menettelyt ja toimet kyseisen jäsenvaltion tuomioistuimen tietoisuuteen. Suuren jaoston tulkinnan mukaan tällä on oikeus lisäksi tarpeen mukaan aloittaa oikeudelliset prosessit, vaikka se ei toimi johtavana valvontaviranomaisena. Vaikka lainvastaisen toiminnan tietoon saattava valvontaviranomainen ei toimi johtavana osapuolena tapauksessa, on tietosuoja-asetuksen mukaisesti valvontaviranomaisten tehtävä yhteistyötä ja jaettava tietoja. [173]

Asetuksen mukaan, rekisterinpitäjältä ei kuitenkaan velvoiteta sitä, että sen tulisi olla tietoinen eri jäsenmaiden välisistä valvontaviranomaisista. Rajat ylittävässä tapauksen käsittelyssä rekisterinpitäjälle siis riittää, että se toimii vain yhden valvontaviranomaisen kanssa, yhdessä jäsenvaltiossa. Käytännössä siis rekisterinpitäjän tarvitsee asioida vain johtavan valvontaviranomaisen kanssa kaikissa tapaukseen liittyvissä kyselyissä ja asioissa. [174]

Työnantajan toimiessa useassa Euroopan jäsenvaltiossa pätee yllä mainittu sääntö ja riittää, että rekisterinpitäjä toimii vain yhden jäsenmaan valvontaviranomaisen kanssa. Yleisesti valvontaviranomainen muotoutuu sen mukaan, missä maassa rekisterinpitäjän tai henkilötietojen käsittelijän päätoimipaikka sijaitsee. Päätoimipaikka ei välttämättä ja automaattisesti tarkoita vain työnantajan suurinta toimistoa. Tietosuojan yhteydessä päätoimipaikka määrittyy muun muassa sen perusteella, kuinka henkilötietojen käsittely on organisaation sisällä järjestetty. [175]

---

[173] EUT lehdistötiedote 103/21.
[174] Talus ym. 2012: 29.
[175] Talus ym. 2012: 29.

Kyseistä menettelyä, jossa valvonta keskitetään ainoastaan yhdelle jäsenmaalle ja valvontaviranomaiselle, kutsutaan nimellä One-stop-shop. Huomiota saanut rajat ylittävä tapahtuma on Googlen tapaus, jossa Ranskan valvontaviranomainen, CNIL, tuomitsi organisaation 50 miljoonan euron hallinnolliseen seuraamusmaksuun. Googlen ollessa alun alkujaan yhdysvaltalainen yritys, tietosuojalainsäädäntö luonnollisesti velvoittaa myös tätä Euroopassa toimiessa. Kyseisessä tapauksessa organisaation päätoimipaikaksi katsotaan sen keskushallinnon paikka. Googlen antaman selvityksen mukaan Irlanti toimii sen EU:n keskuksena ja päätoimipaikkana. CNIL kuitenkin katsoi, että Irlannilla ei ollut päätösvaltaa kyseisessä asiassa, joten sitä ei ollut mahdollista määrittää organisaation päätoimipaikaksi. Näin ollen Ranskan valvontaviranomainen otti tapauksen käsittelyyn ja langetti organisaatiolle yhden suurimmista hallinnollisista seuraamusmaksuista tietosuojalainsäädännön vastaisesta toiminnasta. [176]

[176] Lång & Taka 2018: 62.

# 7 YHTEENVETO JA JOHTOPÄÄTÖKSET

Tietosuoja-asetus mahdollistaa työntekijöille laajan oikeuden omiin henkilötietoihinsa sekä myös paremman tiedonsaannin niiden käsittelystä. Vaikkakin asetus on tuonut rekisteröidylle laajemmat oikeudet omiin henkilötietoihin, on se tuonut myös tavallisille työntekijöille enemmän velvollisuuksia työelämään. Myös työntekijöiden on jokapäiväisessä työssään ja toiminnassaan huomioitava vallitseva tietosuojalainsäädäntö ja osallistuttava työnantajan koulutuksiin, joita työnantajat toivon mukaan järjestävät useammin asetuksen voimaan tulon jälkeen. Myös yksilön, työntekijän on oltava tarkempi omassa toiminnassaan, sillä myös yksittäinen työntekijä voi kohdata seuraamuksia, jos hän tahallisesti tai törkeästä huolimattomuudesta toimii tietosuojalainsäädännön vastaisesti henkilötietojen käsittelyssä. Vaikka työntekijällä olisikin laaja pääsy järjestelmiin, ei työntekijä esimerkiksi saa käydä katsomassa muiden henkilöstöön kuuluvien henkilötietoja ilman, että sillä on tälle työn velvoittama tarve. Työntekijöidenkin on oltava enemmän valveilla tietosuojalainsäädännön suhteen.

Tietosuoja-asetuksen säädös- ja voimaantulovaiheessa asetuksesta puhuttaessa on aina korostettu rekisteröityjen oikeuksia. Asetus on alusta alkaen ikään kuin brändätty niin, että se suojaa rekisteröityjen oikeuksia. Esimerkiksi paljon on puhuttu ja korostettu sitä, että rekisteröidyillä on oikeus saada omat henkilötiedot poistetuiksi organisaation järjestelmistä. Ongelmallista tästä tekee se, että asia ei ole näin yksiselitteinen organisaation, eikä työnantajan näkökulmasta, mutta se on tarjoiltu rekisteröidyille näin yksinkertaistettuna. Tämä aiheuttaa ristiriitaa rekisterinpitäjän ja rekisteröidyn välillä. Esimerkiksi työnantajalla on lakisääteisiä velvollisuuksia, jonka myötä se ei voi poistaa kaikkia rekisteröidyn tietoja, ei edes pyydettäessä. Työnantajan on toiminnassaan seurattava lainmukaisia kanneaikoja. Jos työnhakija epäilisi tulleensa syrjityksi rekrytointiprosessissa, on hakijalla mahdollisuus nostaa kahden vuoden määräajassa kanne työnantajaa kohtaan. Jos työnantaja olisi poistanut kaikki kyseisen hakijan tiedot, kuinka työnantaja voisi osoittaa, että hakijaa ei ole syrjitty rekrytointiprosessissa?

### 7.1 Oikeus henkilötietojen käsittelyyn

Työnantaja on lakisääteisesti velvoitettu keräämään tiettyjä henkilötietoja omista työntekijöistään. Esimerkiksi palkanmaksu työntekijälle ei onnistu ilman tietoa tilinumerosta tai ilman, että työntekijä on toimittanut verokortin. Työnantaja on myös tietyissä tilanteissa oikeutettu keräämään työntekijöistä arkaluontoisia henkilötietoja, kuten terveystietoja. Lääkärintodistuksen pyytäminen työntekijältä on väistämätön esimerkiksi sairauspäivärahan hakemista varten. Lähtökohtaisesti arkaluontoisten tietojen käsittely ja kerääminen on kuitenkin lain mukaan kielletty. Vaikka työnantajalla olisi hyvä tarkoitusperä arkaluontoisten tietojen keräämiselle, ei tämä tietosuojalainsäädännön näkökulmasta ole riittävä peruste. Jos työnantaja haluaisi esimerkiksi tietää lähtötason henkilöstön diversiteetistä ja tätä kautta miettisi kuinka parantaa työpaikan monimuotoisuutta, joutuisi se keräämään todella arkaluontoisia tietoja työntekijöistään. Lähtökohtana kaikessa henkilötietojen keräämisessä toimii tarpeellisuusvaatimus, erityisesti myös arkaluontoisten tietojen keräämisessä. Erityisesti arkaluontoisten henkilötietojen käsittely ja kerääminen ei saisi ainoastaan perustua työntekijöiden suostumukseen.

Työntekijän suostumuskin tiettyjen henkilötietojen käsittelyyn nähdään ongelmallisena, jos työnantajalla ei ole lakisääteistä tarvetta näiden tietojen keräämiselle ja käsittelylle. Ongelmallisuuden asiaan tuo se, että työnantajan nähdään aina olevan vahvempi osapuoli työntekijään verrattuna. Tämän perusteella voidaan katsoa, onko työntekijän suostumus todellinen suostumus ilman, että työnantajan tarpeellisuusvaatimus täyttyy. Työnantaja ei näin ollen voi vedota siihen, että se on saanut työntekijän suostumuksen tiettyjen henkilötietojen keräämiselle.

### 7.2 Työnantajan velvollisuudet

Jo ennen tietosuoja-asetuksen voimaan tuloa Suomessa on kansallisesti ollut jo kattava tietosuojalainsäädäntö, joka on määrittänyt työnantajien velvollisuuksia ja vastuita. Laki yksityisyyden suojasta työelämässä ja entinen henkilötietolaki ovatkin asettaneet velvollisuuksia työnantajia kohtaan sekä turvanneet työntekijöiden oikeuksia

yksityisyydensuojaan. Asetus on kuitenkin tuonut mukanaan entistä enemmän velvoitteita henkilötietojen käsittelyyn työnantajille. Asetuksen myötä myös organisaatioiden korvausvastuu on korostunut huimasti. Pahimmillaan työnantaja voi kohdata todella suuretkin sanktiot tietosuojalainsäädännön vastaisesta menettelystä. Voi olla, että juuri suurista sanktiomahdollisuuksista johtuen asetus velvoittaa organisaatioita nimittämään tietosuojavastaavan, jotta lainsäädännölliset vastuut eivät unohdu ja organisaation sisällä valvotaan henkilötietojen käsittelyä.

Erityisesti pienten työnantajien osalta tietosuojalainsäädännön laajat ja jokseenkin monitulkintaiset säännökset voivat olla kovin työläät ja tuoda jopa lisäkustannuksia organisaatiolle. Monitulkintaisuus saattaa kuulostaa erikoiselta tietotuoja-asetuksen sisältäessä 99 artiklaa. Asetuksessa on kuitenkin havaittavissa aukkoja sekä valvontaviranomaisten linjaukset eivät aina ole täysin kattavat. Organisaatiot ovat lisäksi huomauttaneet asetuksen vaikeaselkoisuudesta.[177] Kuitenkin monitulkintaisuus on noussut esiin esimerkiksi tietyissä asetuksen tulkintatilanteissa. Kuten minkälainen tietoturvaloukkaus katsotaan niin vakavaksi aiheuttavan huomattavaa haittaa rekisteröidylle, että työnantajan on ilmoitettava loukkauksesta sekä valvontaviranomaiselle että suoraan itse rekisteröidylle.

Kuten edellä on mainittu, työnantajan on jo lakisääteisistä velvoitteista kerättävä työntekijöidensä henkilötietoja. Jos pienikin työnantaja käsittelee laajaa määrää henkilötietoja tai erityisten henkilöryhmien tietoja, on sen nimitettävä tai palkattava tietosuojavastaava. Pienenkin työnantajan on äärimmäisen tärkeää kiinnittää huomiota jo toiminnan alusta asti juuri teknisiin asetuksiin ja tietoturva-aspekteihin. Pienempi työnantaja voi nähdä velvoitteet enemmänkin rasitteena, mutta on myös organisaation edun mukaista, että sen tietojärjestelmät ovat tietoturva ystävälliset sekä ajantasaisen tietosuojalainsäädännön mukaiset.

[177] Lång & Taka: 56–57.

Jokaisella EU:n jäsenmaalla on oma nimetty valvontaviranomainen, jonka tulisi valvoa kansallista tietosuojalainsäädännön toteutumista sekä antaa neuvoja ja tulkintoja tietosuoja-asetuksesta. Useammat organisaatiot ovatkin luottaneet siihen, että tietosuojavaltuutettu olisi ollut aktiivisempi ohjeiden ja tulkintojen antamisessa. [178] Asetuksen voimaan tulosta on jo neljä vuotta, joten tietosuojavaltuutetun toimisto on onnistunut antamaan enenevissä määrin linjauksia ja ohjeita organisaatioille. Myös organisaatioille on tarjolla laajempaa tietosuojalainsäädännön koulutusta.

Lisäksi organisaatioiden ja työnantajien tietosuojaloukkauksissa ja rikkeissäkin on nähtävissä yhtäläisyyksiä. Voidaan ajatella tutkimuksen oikeustapausten sekä tietosuojavaltuutetun ratkaisujen perusteella, että kaikilla organisaatioilla ei ole tarvittavaa tietotaitoa tietosuojalainsäädännöstä ja asetuksen tuomista velvotteista. Jossain määrin on sinänsä ymmärrettävää, että työnantajilla ei ole kaiken kattavaa tietoa, koska tietosuoja-asetuksen myötä työnantajan velvollisuudet ovat kasvaneet merkittävästi. Työnantaja on rekisterinpitäjän vastuussa kaikesta henkilötietojen käsittelystä, vaikka se olisi ulkoistanut palvelunsa. Asetuksen myötä työnantajien teknisen tietotaidon vaatimukset ovat lisääntyneet merkittävästi. Työnantaja ei voi luottaa esimerkiksi tietokoneiden teknisten asetusten, kuten sijaintitietojen olevan automaattisesti oikein. Työnantaja on rekisterinpitäjänä aina loppukädessä vastuussa kaikesta henkilötietojen käsittelystä ja keräämisestä.

Kaiken kaikkiaan asetus on tuonut mukanaan paljon hyvää työntekijöiden yksityisyydensuojaan mutta myös paljon uusia velvollisuuksia työnantajille. On äärimmäisen tärkeää huomioida, että maailman digitalisoituessa entistä enemmän ja data siirron laajentuvan yhä enemmän, on yksityisyydensuojalla ja tietoturvalla aikaisempaa suurempi merkitys. Sinänsä vaikka asetus on tuonut tiukemmat säännökset organisaatioiden tietoturvaan, ei sitä välttämättä kannata nähdä vain velvoittavan asian. On myös organisaation etu, että tietoturvasta on huolehdittu riittävässä määrin. Erityisesti kansainvälistyneessä maailmassa ja epävarmassakin maailman tilanteessa, on hyvä, että organisaatio on

[178] Lång & Taka: 57.

kiinnittänyt huomiota omaan tietoturva. Yhä enemmän ja taitavammin myös organisaatioihin kohdistuu huijaus ja kalasteluviestejä.

**LÄHDELUOTTELO**

Alén-Saavikko, Anette (2015) Pois hakutuloksista, pois mielestä? Lakimies 3-4/2015.

Andersson, Jenna (2018) Organisaation tietoturva- ja tietosuojariskienhallinta sekä lainsäädännön vaatimukset. Vaasan yliopisto. Saatavissa 4/2018.

Hanninen, Minna, Elli Laine, Kati Rantala, Mari Rusi, Markku Varhela (2017) Henkilötietojen käsittely. EU-tietosuoja-asetuksen vaatimukset. Helsingin Kamari Oy ja tekijät. Vantaa.

Heiskala, Sonja, Jenni Vinnari (2018) EU:n tietosuoja-asetuksen mukaisen vastuun jakautuminen EU:n ulkorajat ylittävässä henkilötietojen käsittelysuhteessa. Edilex. 2018/1.

Hirvonen, Ari (2011) Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja. Helsinki.

Huusko, Liisa (2006) Työoikeus on tärkeä elementti jo rekrytoinnissa. Joensuun yliopisto. Saatavissa 6/ 2006.

Härkönen, Heidi, Jenni Hokka, Henni Parviainen, Annamari Vänskä & Anne Alvesalo-Kuusi (2022) Puettava teknologia ja yksityisyydensuoja työelämässä. Referee artikkeli. Defensor Legis. 2/2022.

Korhonen, Rauno, Perusrekisterit ja tietosuoja. Edita Publishing Oy. Helsinki 2003.

Korpisaari, Päivi (2017) Viestinnän muuttuva sääntely. Viestintäoikeuden vuosikirja 2016. Helsinki. Helsingin yliopiston oikeustieteellinen tiedekunta.

Korpisaari, Päivi (2018) Miten henkilötietojen suoja rajoittaa paikkatietojen käyttämistä? Referee artikkeli 2018/1.

Korpisaari, Päivi, Olli Pitkänen, Eija Warma-Lehtinen (2018) Uusi tietosuojalainsäädäntö. Alma Talent. Helsinki.

Korpisaari, Päivi, Olli Pitkänen, Eija Warma-Lehtinen (2022) Tietosuoja. Alma Talent. Helsinki.

Koskinen, Seppo (2004) Työhönotossa kerättävät tiedot ja työnhakijan yksityisyyden suoja. Lapin yliopisto. https://www-edilex-fi.proxy.uwasa.fi/artikkelit/2275.pdf

Koskinen, Kilpeläinen, Laakso (2007) Päihteet, Tupakka, alkoholi ja huumeet palvelusuhteen ongelmina. Edita. Helsinki. https://www-edilex-fi.proxy.uwasa.fi/kirjat/5529.pdf

Koskinen, Seppo, Nieminen Kimmo, Valkonen Mika (2008) Työhönotto ja työsopimuksen ehdot. Talentum Media Oy.

Koskinen, Seppo (2013) Verkkosurffailun valvonnasta. Edilex 3013/18.

Kuokkanen, Anna, Alvesalo-Kuusi Anne (2014) Työn elektroninen valvonta osana työntekijän hallinnan jatkumoa ja turvallistamista. Oikeus 2014 (43).

Kurvinen, Evgeniya (2021) Riittävän tietosuojan tason määrittelyn ja arvioinnin problematiikka. Referee artikkeli. Defensor Legis 4/2021.

Lamponen, Helena (2016) Yhteistoimintalaki kommentaari. Alma Talent.

Lehtonen, Asko (2005) Rikos, rangaistus ja prosessi. Juhlajulkaisu N:o 5. Turun Yliopisto. Oikeustieteellisen tiedekunnan julkaisuja.

Lång, Jukka, Anni-Maria Taka (2018). Tietosuoja-asetuksen soveltaminen käytännössä – katsaus ensimmäiseen vuoteen. Viestintäoikeuden vuosikirja 2018 s. 55–74.

Mäntylä, Niina, Karjalainen Ville, Korhonen Nora, Siikavirta Kristian, Wenander Henrik & Annola Vesa (2022). Virkavastuu julkishallinnon muuttuvassa toimintaympäristössä. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2022:14. Valtioneuvoston kanslia. Helsinki.

Neuvonen, Riku (2014) Yksityisyydensuoja Suomessa. Helsingin kauppakamari Oy / Helsingin seudun kauppakamari ja tekijä. Viro.

Nieminen, Kimmo (2017) Työpaikan lait ja työsuhdeopas 2018. Alma Talent.

Nieminen, Kimmo (2019) Työpaikan lait ja työsuhdeopas 2020. Alma Talent.

Nieminen, Liisa (2001) Perusoikeudet EU:ssa. Helsinki, Talentum.

Nyyssölä, Mikko (2020) Yksityisyydensuoja työsuhteessa. Alma Talent. Helsinki

Orasmaa, Pekka (2001) Luottamusmiehen työsuhdeturvasta. Edilex. Edita Ab.

Paasonen, Jyrki, Mikko Aaltonen ja Mikko Luomala (2021) Kyberrikokset tuomioistuimissa – tarkastelussa rikoslain 38 luvun mukaiset tieto- ja viestintärikokset. Referee artikkeli. Defensor Legis 4/2021.

Parkkamäki, Lasse (2018) EU:n yleinen tietosuoja-asetus ja tietojenkäsittelypalveluiden ulkoistaminen: Vastuiden jakautuminen rekisterinpitäjän ja henkilötietojen käsittelijän kesken. Acta Legis Turkuensia 1/2018.

Pesonen, Pirkko (2008) Lex Nokia ja työntekijän yksityiset viestit. Edilex 2008/16

Pitkänen, Olli, Päivi Tiilikka, Eija Warma (2013) Henkilötietojen suoja. Talentum

Saarinen, Mauri (2011) Työsuhteen pelisäännöt. Alma Talent.

Saraviita, Ilkka (2011) Perustuslaki. Talentum Media Oy.

Salokannel, Marjut (2016) Terveystiedot ja EU:n yleinen tietoasetus. Defensor Legis 4/2016. https://www-edilex-fi.proxy.uwasa.fi/defensor_legis/16902.pdf

Syrjänen, Pentti (2006) Yksityisyydensuoja ja henkilöarviointi. Akateeminen väitöskirja. Tampereen yliopisto. Oikeustieteen laitos. Tampere.

Telaranta Kari, Riku Neuvonen (2022) Oikeudesta kameravalvonnan tallenteisiin – empiirinen tarkastelu kansallisen ja EU oikeuden soveltamisessa. Lakimies 5/2022 s. 774–799. Referee artikkeli.

Vainio, Sonja (2017) Rekiterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa. 15 vuotta viestintäoikeutta – Viestintäoikeuden vuosikirja 2017 s. 45–77. Referee artikkeli.

Wennäkoski, Anna (2016) Tietosuojaoikeudellinen vahingonkorvaus murroksessa. Viestinnän muuttuva sääntely. Viestintäoikeuden vuosikirja 2016. Asiantuntija artikkeli.

Wikberg, Olli (2011) Onko Euroopan Unioni matkalla kohti EU- tason ryhmäkannetta? Defensor Legis 2/2011 s.226–238. Asiantuntija artikkeli.

Äimälä, Marku, Åström Johan & Nyyssölä Mikko (2012) Alma Talent. Talentum.

Internet lähteet

https://tietosuoja.fi/-/yritykselle-seuraamusmaksu-tietosuojarikkomuksista-pysakoinninvalvontamaksujen-yhteydessa. Noudettu 12.10.2022.

https://tietosuoja.fi/tietosuojavaltuutetun-toimisto Noudettu 4.10.2022.

https://oikeus.fi/tuomioistuimet/fi/index/asiat/riita-asiat/ryhmakanne.html Noudettu 18.9.2022.

https://european-union.europa.eu/institutions-law-budget/law/types-legislation_fi Noudettu 22.10.2022

https://www-edilex-fi.proxy.uwasa.fi/uutiset/72522?allWords=tietoturvaloukkaus&offset=1&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=1292292 Noudettu 22.10.2022

Tuomioistuinratkaisut

KKO 2010:60

HO 2020:6

TT 2016:124

TT 2018: 101

TT 2020: 74

EIT Bărbulescu v. Romania

EIT Niemietz v Saksa

EIT Drelon v France

Muut ratkaisut

Tietosuojavaltuutettu 87/41/2010

Tietosuojavaltuutettu 2691/171/19

Tietosuojavaltuutettu 3843/163/20

Tietosuojavaltuutettu 1150 /161/21

Tietosuojavaltuutettu 2477/161/21

Tietosuojavaltuutettu 4282/ 161/ 21

Tietosuojavaltuutettu 6813/ 171/21

Tietosuojavaltuutettu 2437/161/22

Virallislähteet

Oikeusministeriö (2017) Miten valmistautua EU:n tietosuoja-asetukseen. Helsinki. Tietosuojavaltuutetun toimisto. Saatavissa 4/2017.

Euroopan Unionin tuomioistuimen lehdistötiedote 103/21 (2021) Luxemburgissa 15.6.2021. Tuomio C-645/19. https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-06/cp210103fi.pdf

Talus Anu, Elina Autio, Anna Hänninen, Heljä-Tuuli Pihamaa ja Silja Kantonen (2017) Oikeusministeriön selvityksiä ja ohjeita 4/2017: Miten valmistautua EU:n tietosuoja-asetukseen. Tietosuojavaltuutetun toimisto. Oikeusministeriö. Helsinki.

Sopimuslähteet

Teknologiateollisuuden työehtosopimus

Teknologiateollisuuden toimihenkilöiden työehtosopimus, yhteistoimintasopimus