Linda Varjo

Henkilötietojen suojan turvaaminen NIS2-direktiivin mukaisessa organisaation kyberturvallisuuspoikkeaman raportointiprosessissa

Johtamisen akateeminen yksikkö
Julkisoikeus, Pro Gradu-tutkielma
Hallintotieteiden maisteri

Vaasa 2026

VAASAN YLIOPISTO
Johtamisen akateeminen yksikkö
Tekijä: Linda Varjo
Tutkielman nimi: Henkilötietojen suojan turvaaminen NIS2-direktiivin mukaisessa organisaation kyberturvallisuuspoikkeaman raportointiprosessissa
Tutkinto: Hallintotieteiden maisteri
Oppiaine: Julkisoikeus
Työn ohjaaja: Niina Mäntylä
Valmistumisvuosi: 2026 **Sivumäärä:** 66

TIIVISTELMÄ:
Tutkimuksen tarkoituksena on selvittää, miten henkilötietojen suojan turvaaminen on NIS2-direktiivin mukaisessa organisaation kyberturvallisuuspoikkeaman raportointiprosessissa huomioitu. Lisäksi käsitellään, miten NIS2-direktiivin ja yleisen tietosuoja-asetuksen raportointivelvoitteet eroavat toisistaan ja kuinka organisaation tulee lain mukaan toimia tilanteessa, jossa kyberturvallisuuspoikkeama vaikuttaa myös henkilötietoihin sekä niiden käsittelyyn. Tutkielmassa käsitellään henkilötietojen käsittelyä ja kyberturvallisuuspoikkeamien raportointia pääasiassa julkishallinnollisen toimijan näkökulmasta.

Suomen perustuslain (731/1999) 10 pykälän mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Myös Euroopan unionin perusoikeuskirjan 8. artikla sekä Sopimus Euroopan unionin toiminnasta takaavat, että jokaisella on oikeus henkilötietojensa suojaan kansalaisuudesta tai asuinpaikasta riippumatta. Yleisen tietosuoja-asetuksen useat säädökset takaavat, että henkilötietojen suojan on toteuduttava myös verkkoympäristöissä, ja henkilötietojen käsittelylle tulee aina olla henkilötietojen omistajan suostumus tai jokin laillinen peruste.

NIS2-direktiivin vaatimusten on tarkoitus asettaa Euroopan unionin alueella vähimmäisvelvoitteet kyberturvallisuudelle. Direktiivissä on määritelty organisaation riskienhallintavelvoitteista kyberturvallisuuden tason takaamiseksi. Toimijat on velvoitettu NIS2-direktiivillä ja kansallisella kyberturvallisuuslailla (124/2025) ilmoittamaan valvoville viranomaisille havaitsemistaan kyberturvallisuuspoikkeamista kolmiportaisen raportointiprosessin kautta, joissa jokaisessa vaiheessa on ilmoituksen antamisessa noudatettavat aikamääreet. Yleisessä tietosuoja-asetuksessa on määritelty oma raportointiprosessi henkilötietojen tietosuojaloukkausten ilmoittamiseksi valvovalle viranomaiselle. Keskeinen havainto on, että NIS2-direktiivi ja yleinen tietosuoja-asetus asettavat erilaiset ilmoitusvelvollisuudet, vaikka samassa tapauksessa saatetaan tehdä ilmoitus sekä kyberturvallisuuspoikkeamasta että tietoturvaloukkauksesta. Käsittelyssä on myös tietojenkäsittelyssä tapahtuvista rikkomuksista tai laiminlyönneistä seuraavan hallinnollisen seuraamusmaksun määräytymisestä erityisesti julkishallinnon toimialaan kuuluvalle ja siihen liittyvän lakiuudistuksen valmistelu.

Tutkielman johtopäätöksissä todetaan, että sääntelyn kehityksessä korostuu erityisesti tarve selkeyttää vastuunjakoa sekä yhdenmukaistaa raportointiprosesseja, jotta sääntely ei olisi organisaatioille liian hajanaista ja raskasta soveltaa. Johtopäätöksissä todetaan myös hallinnollisten seuraamusmaksujen määräämisessä olevan tarvetta uudistukselle. Keskeisenä haasteena säädösten yhteensovittamisessa havaittiin poikkeamien tunnistamisen ja vastuiden epäselvyydet sekä säädösten asettamat eri aikamääreet ilmoituksille sekä eri valvovat viranomaiset.

AVAINSANAT: tietosuoja, tietoturva, henkilötieto, kyberturvallisuus, poikkeama, perusoikeudet

Sisällys

Lyhenteet

ENISA	Euroopan kyberturvallisuusvirasto
ETN	Euroopan tietosuojaneuvosto
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
GDPR	General Data Protection Regulation, Yleinen tietosuoja-asetus, Asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta
Julkisuuslaki	Laki viranomaisen toiminnan julkisuudesta (621/1999)
KHO	Korkein hallinto-oikeus
KKO	Korkein oikeus
NIS2-direktiivi	Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta
Tiedonhallintalaki	Laki julkisen hallinnon tiedonhallinnasta (906/2019)
Yleinen tietosuoja-asetus	Asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta

1 Johdanto

Suomen perustuslain (731/1999) 10 pykälän mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Myös Euroopan unionin perusoikeuskirjan 8. artikla sekä Sopimus Euroopan unionin toiminnasta takaavat, että jokaisella on oikeus henkilötietojensa suojaan kansalaisuudesta tai asuinpaikasta riippumatta. Yleisen tietosuoja-asetuksen useat säädökset takaavat, että henkilötietojen suojan on toteuduttava myös verkkoympäristöissä, ja henkilötietojen käsittelylle tulee aina olla henkilötietojen omistajan suostumus tai jokin laillinen peruste.

1.1 Tutkimuksen tausta ja tarkoitus

Digitalisaation myötä yhteiskunnan eri toiminnot ja palvelut ovat muuttuneet yhä enenevissä määrin digitaaliseen muotoon ja useat toiminnot toimivat aiempaa automatisoidummin yleisessä tietoverkossa[1]. Nyky-yhteiskunta toimii siis käytännössä suoraan tai välillisesti tietotekniikan varassa, joka väistämättä aiheuttaa myös uudenlaisia oikeudellisia haasteita ja ongelmia, sillä verkko- ja tietojärjestelmien merkittävä kehitys on samalla laajentanut myös kyberuhkaympäristöä (Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 [2]). Tietotekniikka mahdollistaa yhteiskunnassa monenlaista toimintaa ja sujuvoittaa sekä nopeuttaa parhaimmillaan tiedonkulkua ja sen käsittelyyn liittyviä prosesseja[3]. Myös hyvin merkittävä osa kriittisestä infrastruktuurista tarvitsee toimiakseen tietotekniikkaa tai tietoverkkoja[4]. Toisaalta tietotekniikan kehitys mahdollistaa myös rikollisen toiminnan, sillä lainsäädäntö tai siihen tarvittavien muutosten toteuttaminen ei pysy tietoteknisen kehityksen vauhdissa[5].

[1] Voutilainen 2023, s.17.
[2] EYVL N:o L 333, 27.12.2022, s.1–2.
[3] HE 57/2024 vp, s.7.
[4] Saarenpää & Riekkinen 2023, s.73.
[5] Saarenpää & Riekkinen 2023, s.29.

Kyberturvallisuus on noussut keskeiseen asemaan nyky-yhteiskunnassa, sillä sen avulla voidaan turvata paitsi organisaatioiden toiminta ja kilpailukyky myös yksityisten kansalaisten perusoikeuksien, kuten yksityisyyden suojan toteutuminen[6]. Käytännössä kyberturvallisuus vaikuttaa nykypäivänä kaikkeen tietoverkkojen ja tietojärjestelmien kautta tapahtuvaan toimintaan, jonka vuoksi sitä ei voida enää pitää muusta erillisenä asiana, vaan se tulee ottaa lähes kaikessa toiminnassa huomioon[7]. Tietojärjestelmien sekä tietoverkkojen kehityksen myötä myös erilaiset kyberuhat, kuten tietomurrot, haittaohjelmat sekä verkkohyökkäykset luonnollisesti kehittyvät ja muuttavat muotoaan samaa tahtia entistä vaikeammiksi tunnistaa tai estää[8]. Kyberturvallisuudella pyritään estämään, jotta tietoverkkorikollisilla ei olisi pääsyä kenenkään luottamuksellisiin tietoihin, joiden kautta voitaisiin aiheuttaa paitsi taloudellista haittaa myös vakavia häiriöitä koko yhteiskunnan tasolla[9]. Lainsäädännön avulla pyritään turvaamaan muun muassa ihmisten perusoikeuksien, yhdenvertaisuuden, sananvapauden, omaisuuden suojan, turvallisuuden sekä hyvän hallinnon toteutuminen digitaalisten palveluiden toteutuksessa[10].

Viime vuosina mediassa on uutisoitu runsaasti maailmallista kyberturvallisuustilannetta koskevista tapauksista. Kyberturvallisuuden merkitys on kasvanut runsaasti, sillä useisiin keskeisiin yhteiskunnan turvallisuutta tukeviin tai tuottaviin toimintoihin on mahdollista vaikuttaa tietoverkkojen kautta osana hybridivaikuttamista. Hybridiuhalla tarkoitetaan dynaamisia ja muuntuvia uhkia, jotka vaikuttavat koko yhteiskuntaan. Esimerkkinä hybridivaikuttamisesta ovat muun muassa vaalituloksiin vaikuttaminen, sosiaalisen median manipulointi sekä erilaiset kyberhyökkäykset julkisia palveluita kohtaan.[11] Hybridivaikuttamisen keinoihin kuuluvat poliittisten, taloudellisten ja sotilaallisten keinojen lisäksi in-

[6] HE 57/2024 vp, s.7. Myös Saarenpää & Riekkinen 2023, s.180.
[7] Saarenpää & Riekkinen 2023, s.26.
[8] Saarenpää & Riekkinen 2023, s.29.
[9] HE 57/2024 vp, s.7.
[10] Voutilainen 2023, s. 18.
[11] Ferm 2018, s.404.

formaatio- ja kybervaikuttamisen keinot, joilla pyritään pahantahtoisesti ulkoisesti vaikuttamaan valtiolliseen toimijaan tämän haavoittuvuuksia hyödyntäen systemaattisesti[12].

Venäjän hyökkäys Ukrainaan sai aikaan Suomen ja Euroopan turvallisuus- ja toimintaympäristössä pitkän rauhallisemman ajan jälkeen merkittäviä muutoksia, joilla on kauaskantoisia vaikutuksia[13]. Venäjä on toteuttanut hyökkäystoimissaan Ukrainaan monitahoista hybridivaikuttamista muun muassa kyberoperaatioilla, joissa on hyödynnetty vakoiluohjelmia, palvelunestohyökkäyksiä sekä sähköverkon häirintää[14]. Venäjän toimien myötä myös Suomessa on pyritty varautumaan laaja-alaiseen ja monitahoiseen hybridi- ja informaatiovaikuttamiseen[15]. Muutokset turvallisuuspoliittisissa toimintaympäristöissä näkyvät myös kyberympäristöissä, joissa valtio- ja kuntatasoon kohdistuvat uhat ovat monimutkaistuneet ja lisääntyneet merkittävästi, jonka vuoksi kriittisten toimien kuten vesi- ja energiahuollon turvaamiseksi kriisitilanteessa on varauduttava[16]. Kyberympäristöissä pystytään siis käytännössä vaikuttamaan nykypäivänä hyvin laaja-alaisesti myös yhteiskunnan kriittisiin toimintoihin.

Ulkoministeriö kertoi tiedotteessaan[17] suomalaisiin diplomaatteihin kohdistuneen kybervakoilua israelilaisen NSO Groupin Pegasus-vakoiluhaittaohjelmalla ainakin vuosien 2021–2022 aikana, mahdollisesti jopa pidempään. Tiedotteen tietojen mukaan kyseessä on kehittynyt haittaohjelma, joka voidaan asentaa puhelimeen huomaamatta sekä ilman käyttäjän toimenpiteitä. Ohjelman avulla voi lukea puhelimessa olevia viestejä, tallentaa puheluita, aktivoida mikrofonin salakuuntelua varten, tallentaa salasanoja ja jopa seurata, missä paikoissa käyttäjä on liikkunut[18]. Ulkoministeriö totesi kyseessä olleen laiton tiedustelu ja piti tapausta hyvin vakavana. Ylen mukaan[19] samaisen ohjelman avulla on

[12] Valtioneuvosto 2020, s.10.
[13] Valtioneuvosto 2022, s.7.
[14] Valtioneuvosto 2022, s.8.
[15] Sisäministeriö 2025, s.86.
[16] Sisäministeriö 2025, s.88.
[17] Ulkoministeriö 2022.
[18] Ulkoministeriö 2022 sekä KHO:2024:115.
[19] Pilke 2022.

vakoiltu myös muun muassa Ranskan presidentin sekä useiden muiden valtioiden päämiesten puhelimia. Tämä tapaus toimii hyvänä esimerkkinä siitä, miten kehittyneitä sekä laaja-alaisia tietoverkkojen ja digitaalisten väylien kautta toteutuvat kyberuhat tänä päivänä ovat ja miten arkaluontoisiin asioihin voidaan päästä käsiksi.

Saarenpään ja Riekkisen mukaan tietoturvallisuutta koskeva lainsäädäntö on jo pitkään ollut riittämättömästi säädeltyä sekä varsin hajanaista[20]. Sääntelyn tarkoituksena on ollut taata tietoverkkojen käyttäjien kuluttajansuoja, tietosuoja sekä oikeusturva, mutta viimeisen 20 vuoden aikana sääntely on lisääntynyt niin valtavasti, että niiden tyhjentävästä tulkinnasta on tullut haastavaa[21]. Euroopan parlamentti ja komissio ovat antaneet direktiivin (2022/2555) 14.12.2022 koskien toimenpiteitä kyberturvallisuuden yhteisen korkeamman tason varmistamiseksi koko unionissa. Kyseessä on niin sanottu NIS2-direktiivi, jonka tavoitteena on yhtenäistää kyberturvallisuutta koskevaa lainsäädäntöä, kehittää kyberturvallisuusvalmiuksia ja lieventää keskeisimpiä uhkia, asettaa vähimmäistaso kyberturvallisuusvaatimuksille koko unionin alueella sekä varmistaa keskeisten palveluiden jatkuvuus myös poikkeustilanteissa.[22] NIS2-direktiivi on pitänyt implementoida osaksi kansallista lainsäädäntöä 17.10.2024 mennessä. NIS2-direktiivi on tarkoitus ottaa osaksi Suomen lainsäädäntöä uuden kyberturvallisuuslain muodossa, joka kokoaisi yhteen NIS2-direktiivin mukaiset vähimmäisvelvoitteet kyberturvallisuuden riskienhallinnasta sekä poikkeamaraportoinnista direktiivin soveltamisalaan kuuluville toimijoille.[23] Kyseessä on siis verrattain tuore sekä ajankohtainen laki, joka on hallituksen esityksen mukaan[24] tullut Suomessa sovellettavaksi 18.10.2024 lähtien.

Kyberturvallisuuden merkitys on siis kasvanut vuosi vuodelta digitalisoitumisen ja teknologian kehityksen myötä, ja se tulee ottaa nykyään kaikessa toiminnassa niin yhteiskunnan kuin yritysten sekä yksityishenkilöiden toiminnassa huomioon. Kehityksen myötä

[20] Saarenpää & Riekkinen 2023, s.29.
[21] Voutilainen 2023, s.18–19.
[22] HE 57/2024 vp, s.7–8.
[23] HE 57/2024 vp, s.58.
[24] HE 57/2024 vp, s.1.

myös lainsäädännöllisen kehityksen pitäisi vähintäänkin yrittää pysyä mukana vauhdissa. Digitalisaatio sekä teknologian kehitys ovat osaltaan pakottaneet tietosuojaa koskevan lainsäädännön uudistamiseen, jotta perusoikeuksien toteutuminen voidaan taata myös jatkossa[25]. Kyberturvallisuuden yhtäläisen tason turvaamiseksi säädetty NIS2-direktiivi antaa organisaatiolle tietyt vaatimukset, joiden mukaan tulee toimia kyberturvallisuuspoikkeaman tullessa ilmi. Organisaation turvallisuutta ja etua tavoiteltaessa yksilön etu voi jäädä herkästi huomiotta. Tässä tutkielmassa otetaan selvää, onko organisaatioille annetuissa vaatimuksissa otettu huomioon myös yksilöiden oikeus henkilötietojensa suojaan ja miten sen turvaaminen toteutuu kyberturvallisuuspoikkeaman ilmentyessä.

Tutkimuksen tarkoituksena on selvittää organisaatioiden velvoitteita koskien kyberturvallisuutta ja tietosuojaa sekä niiden toteutumista oikeudellisesta näkökulmasta. Tarkoituksena on syventyä siihen, minkälaisia vaatimuksia organisaatioilla on NIS2-direktiivin, kyberturvallisuuslain, yleisen tietosuoja-asetuksen sekä muun ajantasaisen lainsäädännön puitteissa asetettu kyberturvallisuuspoikkeamien raportointiin liittyen, ja kuinka nämä vaatimukset vaikuttavat tietosuojaan liittyviin käytäntöihin.

1.2 Tutkimusongelma ja tutkimustehtävän rajaus

Tarkastelen tutkielmassani organisaatioihin kohdistuvia kyberturvallisuusvaatimuksia, ja tarkemmin organisaation velvollisuutta raportoida kyberturvallisuuspoikkeamista. Tarkoituksenani on tutkia, ***miten uuden NIS2-direktiivin myötä on pyritty reagoimaan kyberturvallisuusuhkiin ja, millaisia vaatimuksia se asettaa organisaatioille kyberturvallisuuspoikkeaman ilmentyessä.*** Aion tarkastella kyberturvallisuusvaatimuksia niin yksityisten yritysten kuin myös julkisten organisaatioiden näkökulmasta, kuitenkin keskittyen enemmän julkishallinnon toimialaan. Tarkoituksena on keskittyä NIS2-direktiivin asettamiin ja yleisessä tietosuoja-asetuksessa asetettuihin raportointivelvoitteisiin, ja ***miten***

[25] Ojajärvi 2022, s.104.

henkilötietojen suoja turvataan näiden säädösten puitteissa kyberturvallisuus-poikkeamista raportoidessa*.** Tutkin, millaisia tekijöitä uudessa direktiivissä on nimetty kyberturvallisuuteen vaikuttaviksi tekijöiksi. Erityisesti tietosuojaan liittyvät vaatimukset kiinnostavat, sillä tutkin kandidaatin tutkielmassani henkilötietojen suojan turvaamista verkkoympäristöissä ja tietosuoja-asiat ovat myös organisaatioissa hyvin merkittävässä asemassa kyberturvallisuuden toteutuksessa. Tarkoituksenani on siis tutkia ***miten NIS2-direktiivin ja yleisen tietosuoja-asetuksen raportointivelvoitteet eroavat toisistaan ja kuinka organisaation tulee lain mukaan toimia tilanteessa, jossa kyberturvallisuus-poikkeama vaikuttaa myös henkilötietoihin sekä niiden käsittelyyn.

Tarkoituksena on käsitellä aihetta voimassa olevan kansallisen lainsäädännön sekä kansainvälisen EU-lainsäädännön puitteissa. NIS2-direktiivin lisäksi käsittelyssä on muun muassa Euroopan unionin yleinen tietosuoja-asetus. Tutkin, miten direktiivi on onnistuttu ottamaan osaksi kansallista lainsäädäntöä kyberturvallisuuslain muodossa ja onko direktiivin uudistamisessa onnistuttu vai onko jäänyt jotakin selkeitä puutteita tai onko direktiivi jo valmiiksi joiltakin osin vanhentunut astuessaan voimaan. Koska keskityn erityisesti julkishallinnon toimialaan, joka on lisätty NIS2-direktiivissä uutena erittäin kriittisenä toimialana osaksi soveltamisalaa[26], käsittelen myös tiedonhallintalakia, jonka tietoturvallisuussääntelyä sovelletaan julkishallinnossa.

1.3 Keskeiset käsitteet

Tutkimuksessani keskeisimpinä käsitteinä ovat kyberturvallisuus, tietosuoja sekä henkilötietojen suoja. Käsitteet ovat hyvin lähellä toisiaan ja kytkeytyvät toisiinsa, mutta jokaista käsitettä koskee omat säädökset ja jokaisella käsitteellä on oma määritelmänsä. Kyberturvallisuus on yksi tietoturvallisuuden osa, jolla pyritään osaltaan varmistamaan kansallinen turvallisuus sekä maanpuolustuksen, huoltovarmuuden, elinkeinoelämän ja kansalaisyhteiskunnan toimintaedellytykset. Suomen kyberturvallisuusstrategian mukaan yleisesti määrittäen kyberturvallisuus kattaa ne toimet, joiden avulla suojataan

[26] HE 57/2024 vp, s.52–53.

viestintä- ja tietojärjestelmiä sekä muita sähköisiä järjestelmiä. Kyberturvallisuuden tarkoituksena on suojata kyberuhilta paitsi näihin järjestelmiin tallennettavia, siirrettäviä tai niissä käsiteltäviä tietoja myös järjestelmien käyttäjiä, niitä hyödyntäviä ja muita asiaan osallistuvia tahoja.[27] Käsitteenä kyberturvallisuus ulottuu siis hyvin laajalle alalle yhteiskuntatasolta aina yksilöihin asti. Kyberturvallisuudesta säännellään Euroopan unionin tasolla NIS2-direktiivissä sekä siitä kansallisella tasolla säädetyssä kyberturvallisuuslaissa. Lisäksi NIS2-direktiivin 7 artikla velvoittaa jäsenvaltiot hyväksymään oman kansallisen kyberturvallisuusstrategian, jossa on määritelty kybertoimintaympäristöä kohtaavien haasteiden käsittelyyn keskeisimmät tavoitteet sekä toimintamallit, joiden avulla voidaan varmistaa ja mahdollistaa kyberturvallisuuden korkea taso. [28]

Yleisen tietosuoja-asetuksen ((EU) 2016/679) 4 artiklan määritelmän mukaan henkilötiedolla viitataan kaikkiin tunnistettuihin tai tunnistettavissa oleviin luonnollista henkilöä koskeviin tietoihin. Näiden tietojen perusteella luonnollinen henkilö on siis tunnistettavissa joko suoraan tai epäsuorasti tietoja yhdistellen[29]. Tietoihin lukeutuu muun muassa nimi, henkilötunnus, sijaintitieto, verkkotunnistetieto sekä henkilölle tunnusomaiset fyysiset, fysiologiset, geneettiset, psyykkiset, taloudelliset, kulttuuriset tai sosiaaliset tekijät. Henkilötietoja käsiteltäessä luonnollista henkilöä koskevat tiedot pyritään pitämään suojassa vahingolliselta tai rikolliselta toiminnalta, jotta perustuslain 10 pykälän yksityiselämän suoja toteutuu. Tietosuojalla viitataan siis nimensä mukaisesti toimiin ja tapoihin, joiden avulla muun muassa yksityisyys ja henkilötiedot pyritään pitämään suojattuna.

Yleisen tietosuoja-asetuksen 4 artiklan 12 kohdassa on annettu määritelmä henkilötietojen tietoturvaloukkaukselle. Henkilötietojen tietoturvaloukkauksen takia käsiteltäviin henkilötietoihin on kohdistunut vahingossa tai lainvastaisesti henkilötietojen tuhoamista, häviämistä, muuttamista, luvatonta luovuttamista tai tietoihin on päästy käsiksi sellaisen

[27] Suomen kyberturvallisuusstrategia, 2024, s.10.
[28] HE 57/2024 vp, s.21 ja s.56.
[29] Neuvonen 2019, s.233.

tahon toimesta, joka ei niiden käsittelyyn ole oikeutettu. Henkilötietojen tietoturvaloukkaus katsotaan tapahtuneen esimerkiksi onnistuneen palvelunestohyökkäyksen tai tietomurron tapahtuessa, henkilötietoja sisältävän dokumentin tai teknisen laitteen kadotessa, kun ulkopuolisella taholla on pääsy tietoihin tai kun henkilötietoja sisältävä kirje on postitettu väärälle henkilölle.[30]

1.4 Tutkimuksen rakenne ja metodi

Aineistona käytän tutkimuksessani oikeuskirjallisuutta, artikkeleita, hallituksen esityksiä sekä lain valmistelussa annettuja muita valmisteluaineistoja ja oikeuskäytäntönä kansallisten tuomioistuinten ratkaisuja. Tutkimusmetodinani käytän lainoppia eli oikeusdogmatiikkaa. Oikeusdogmatiikka tutkii voimassa olevaa oikeutta eli sitä, mikä on velvoittavaa ja pätevää.[31] Voimassa olevia oikeusnormeja systematisoidaan ja tulkitaan eli järjestetään voimassa olevia oikeusnormeja niin, että niiden sisällön tulkinnasta tulee mahdollista.[32] Lainopin tarkoituksena on tuottaa perusteltuja kannanottoja voimassa olevasta oikeudesta. Kannanotot voivat olla tulkinnallisia, punnitsevia tai systematisoivia.[33] Tunnusomaista lainopilliselle metodille on toistettavissa ja perusteltavissa olevat ajatukselliset siirtymät oikeudelliseen tulkintalauseeseen, joka ei saa perustua vain henkilökohtaiseen mielipiteeseen. Tulkinnan tulee olla laadukkaasti perusteltavissa, jotta ne ovat vakuuttavia.[34] Lainopillinen tulkinta pohjautuu oikeuslähteisiin, joilla tarkoitetaan eritasoisia lähteitä, joista oikeudelliset säännöt ovat löydettävissä. Oikeuslähteitä ovat muun muassa EU:n oikeusjärjestyksen perustan luovat periaatteet, perustamissopimukset, kansainväliset sopimukset, direktiivit, asetukset sekä tuomioistuinten ratkaisut.[35]

---

[30] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.80–81.
[31] Hirvonen 2011, s.22–23.
[32] Husa & Pohjolainen 2014, s.37.
[33] Kolehmainen 2016, s.107.
[34] Kolehmainen 2016, s.115.
[35] Talus & Penttinen 2016, s.224–225.

Tutkielmassani käyn läpi aiheeseen liittyvää lainsäädäntöä sekä lainsäädännön valmisteluaineistoa, joiden avulla pyrin selvittämään tutkimusaihettani. Tarkoituksenani on systematisoida voimassa olevia lakeja. Tutkimukseni on tarkoitus keskittyä tarkastelemaan syntynyttä kotimaista oikeustilaa kansallisen oikeuden näkökulmasta, mutta väistämättä tulen tarkastelemaan aihetta myös EU-oikeuden kannalta, sillä se on merkittävässä roolissa aiheeni kannalta.

Oikeustieteen näkökulmasta organisaatioiden kyberturvallisuusvaatimusten tutkiminen sijoittuu useammalle oikeustieteen alalle. Yleisesti aiheena kyberturvallisuuteen linkittyy paitsi lakien ja muun oikeuskäytännön ja -lähteiden määrittämiä vastuita ja velvollisuuksia myös runsaasti tietotekniikkaan liittyviä seikkoja. Kyberturvallisuutta voidaan pitää aiheena perusoikeudellisena, sillä tietosuoja on siinä hyvin merkittävässä roolissa. Tietosuoja puolestaan linkittyy perusoikeuksiin, sillä tietosuojaan sisältyy muun muassa henkilötietojen suoja, joka osana yksityisyyden suojaa on osa perusoikeuksia. Toisaalta henkilötietojen suoja on poikkeus julkisuusperiaatteeseen, joka puoltaa aiheen julkisoikeudellisuutta. Hieman ympäripyöreästi todeten kyberturvallisuus voidaan katsoa kuuluvan oikeusinformatiikan oikeudenalaan, sillä sen tutkimusalalla yhdistyy useat tieteenalat oikeustieteen kanssa.[36]

Kyberturvallisuuteen sisältyy kuitenkin tarkemmassa tarkastelussa myös informaatio-oikeutta[37] sekä teknologiaoikeutta. Toisaalta organisaatioiden kyberturvallisuuteen linkittyy myös hyvin kiinteästi sopimusoikeus, kun organisaatiot tekevät keskenään sopimuksia, joissa myös kyberturvallisuus on otettava huomioon. Toisaalta nykypäivänä oikeastaan kaikissa organisaatioiden toiminnassa kyberturvallisuus on merkittävästi läsnä. Oikeudenalaan vaikuttaa merkittävästi se, minkä organisaation näkökulmasta asiaa tarkastellaan; yritysten, julkisen sektorin tai yksityishenkilöiden tietosuojan.

[36] Saarenpää & Riekkinen 2023, s.19.
[37] Neuvonen 2019, s.17.

Tutkielmani koostuu johdantoluvun lisäksi kolmesta pääluvusta sekä johtopäätöksistä. Ensimmäisessä pääluvussa tarkastelen kyberturvallisuutta käsitteenä sekä NIS2-direktiivin asettamia vaatimuksia kyberturvallisuuspoikkeamista ilmoittamisesta sekä raportoinnista. Perehdyn aihetta koskevaan lainsäädäntöön ja sen vaikutuksiin. Pääasiassa käsiteltävät lait ovat kyberturvallisuuslaki, tiedonhallintalaki, NIS 2-direktiivi ja siitä säädetty kansallinen kyberturvallisuuslaki sekä Euroopan unionin yleinen tietosuoja-asetus eli GDPR. Toisessa pääluvussa selvitän tarkemmin tietosuojan ja yksityisyydensuoja tai tarkemmin henkilötietojen suojaa suhteessa kyberturvallisuuteen. Toisessa pääluvussa tarkoituksenani on perehtyä, mitä yleisessä tietosuoja-asetuksessa säädetään tietosuojapoikkeamien raportoinnista. Toisen pääluvun loppupuolella käsittelen oikeustapauksia, joilla havainnollistan käytännön tasolla käsittelyssä olevan lainsäädännön soveltamista ja toimeenpanoa.

Kolmannessa pääluvussa syvennytään tarkemmin vielä NIS2-direktiivin ja GDPR:n asettamien vaatimusten väliseen suhteeseen ja jännitteisiin. Tarkoituksena on selvittää, miten vaatimukset eroavat toisistaan ja miten niitä tulisi soveltaa suhteessa toisiinsa. Kolmannessa pääluvussa käsittelen myös, mitä seuraa, jos NIS2-direktiivin ja GDPR:n mukaisia vaatimuksia ei täytetä tai prosesseissa ei toimita säännösten asettamien puitteiden mukaisesti. Tarkoituksenani on syventyä rikkeistä seuraaviin hallinnollisiin seuraamuksiin ja sanktioihin.

2 Kyberturvallisuus ja sen haasteet organisaatiossa

2.1 Kyberturvallisuus käsitteenä

Kyberturvallisuudella viitataan toimiin, joilla pyritään suojaamaan verkko- ja tietojärjestelmiä, näiden käyttäjiä sekä muita asianosaisia kyberuhilta[38]. Suomen kyberturvallisuusstrategiassa on määritelty kyberturvallisuuden olevan osa Suomen kokonaisturvallisuutta ja digitalisoituvaa yhteiskuntaa ja sen avulla voidaan varmistaa kansallisen turvallisuuden, maanpuolustuksen, huoltovarmuuden, elinkeinoelämän ja kansalaisyhteiskunnan toimintaedellytykset[39]. Kyberturvallisuus on ulottuvuuksiltaan hyvin laaja-alainen, ja se vaikuttaakin käsitteenä aina yhteiskuntatasolta kansalaisiin asti.

Kyberturvallisuus käsitteenä viittaa tavoiteltavaan tilaan, jossa luotettava ja turvallinen toiminta kybertoimintaympäristössä on turvattu. Kybertoimintaympäristöllä viitataan sähköiseen ympäristöön, jossa monialainen tietojenkäsittely tapahtuu. Kybertoimintaympäristössä toiminnan kannalta on välttämätöntä, että tietojärjestelmät ja tietoverkot ovat toiminnassa ja tieto kulkee niiden välillä ilman ongelmia. [40] Kyberturvallisuus on yksi osa laajempaa tietoturvan käsitettä, jolla tarkoitetaan yleisesti tietojen turvaamista. Kyberturvallisuus keskittyy nimenomaisesti sähköisten tietojen turvaamiseen erilaisissa järjestelmissä sekä pyrkii takaamaan verkko- ja järjestelmäriippuvaisten organisaatioiden ja yhteiskunnan toiminnan kybertoimintaympäristössä[41].

Kyberturvallisuus nähdään nykyään oikeudellisena käsitteenä, ja siitä säännelläänkin muun muassa Euroopan unionin NIS2-direktiivissä eli kyberturvallisuusdirektiivissä, joka

[38] HE 57/2024 vp., s.53.
[39] Valtioneuvosto, 2024, s.10.
[40] Andersson 2024, s.56.
[41] Andersson 2024, s.56–57.

pyrkii määrittämään unionin alueella yhteisen ja yhtäläisen kyberturvallisuuden vähimmäistason[42]. Kyberturvallisuuteen liittyy vahvasti käsitteet kyberuhka sekä kyberriski. Kyberuhan on määritelty NIS2-direktiivissä tarkoittavan potentiaalista tilannetta, tapahtumaa tai toimintaa, joka voi aiheuttaa vahinkoa tai häiritä verkko- ja tietojärjestelmiä, niiden käyttäjiä ja muita henkilöitä tai vaikuttaa muulla tavalla haitallisesti näihin[43]. Käsitteellä uhka tarkoitetaan jotakin sellaista, jolla on epätoivottuja vaikutuksia organisaatioon eikä tapahtumassa ole positiivista mahdollisuutta[44]. NIS2-direktiivissä puhutaan vielä tarkemmin merkittävästä kyberuhasta, jolla viitataan uhkaan, jonka teknisten ominaisuuksien perusteella voidaan olettaa aiheuttavan tai vaikuttavan vakavasti verkko- ja tietojärjestelmiin tai niiden käyttäjiin aiheuttaen huomattavaa aineellista tai aineetonta haittaa[45].

Kyberriski on vahinkomahdollisuus tai haavoittuvuus, joka kohdistuu kybertoimintaympäristöön, ja voi toteutuessaan tai sitä hyödyntäen aiheuttaa kyberympäristön toiminnasta riippuvalle toiminnolle haittaa, vahinkoa tai häiriötä[46]. Kyberriskiä ei kuitenkaan esimerkiksi NIS2-direktiivissä ole määritelty ollenkaan erikseen käsitteenä. Henkilötietojen suojassa riskillä voidaan tarkoittaa henkilötietojen käsittelyn aiheuttamaan fyysisen, aineellisen tai aineettoman vahingon tapahtumisen mahdollisuutta. Riskin realisoituessa syntyy vahinko, joka voi käydä ilmi esimerkiksi identiteettivarkautena, petoksena, maineen vahingoittumisena tai aiheuttaa muuta merkittävää taloudellista tai sosiaalista vahinkoa.[47]

Riskiä ja uhkaa saatetaan käyttää joissakin tilanteissa ikään kuin toistensa synonyymeinä, mutta käsitteiden välillä on kuitenkin olemassa keskeinen ero. Uhkalla tarkoitetaan potentiaalista negatiivista tapahtumaa. Riskillä viitataan tarkemmin arvioituihin seuraamuksiin, joita tästä tapahtumasta seuraa sekä todennäköisyyttä, jonka mukaan uhka voi

[42] Andersson 2024, s.57. Myös HE 57/2024 vp, s.1.
[43] HE 57/2024 vp., s.53.
[44] Andersson 2024, s.51–52.
[45] Andersson 2024, s.57–58. Myös HE 57/2024 vp., s.17.
[46] Andersson 2024, s.58.
[47] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.302.

toteutua. Riski on siis tietyn uhan aiheuttaman menetyksen tai vahingon todennäköisyys.[48]

Organisaatioiden tulee toiminnassaan arvioida tietojenkäsittelyynsä liittyviä riskejä[49]. Tätä toimintatapaa kutsutaan riskiperustaiseksi lähestymistavaksi. Riskiperustaisessa lähestymistavassa keskeistä on riskien arviointi sekä mahdollisten ongelmien ennaltaehkäisy.[50] Yleisen tietosuoja-asetuksen 25 artiklan mukaan tietojärjestelmien suunnittelussa sekä henkilötietojen käsittelyssä tulisi ottaa tietosuoja huomioon prosessin alusta alkaen eikä vasta jälkikäteisesti. Tällä tarkoitetaan, että jo suunnitteluvaiheessa tietosuojan toteutuminen otetaan huomioon ennakoivasti ottamalla huomioon yksityisyyden vaatimukset sekä riskienhallinta.[51]

NIS2-direktiivin 20 ja 21 artikloissa on määritelty vähimmäistason riskienhallintavelvoitteita, joita toimijoiden tulee noudattaa. Velvoitteet on pyritty muotoilemaan teknologianeutraalisti soveltuen erilaisille toimijoille ja, jotta ne olisivat mahdollisimman ajattomia eivätkä vanhetuisi termistöltään ja toimiltaan heti. Kyseessä on vähimmäistason vaatimukset, joka tarkoittaa, että jokainen toimija voi niin halutessaan tai jäsenvaltiot voivat kansallisessa lainsäädännössään säätää myös tiukempia riskienhallintavelvoitteita.[52] Direktiivin 20 artiklan mukaan keskeisten ja tärkeiden toimijoiden hallintoelinten tulee hyväksyä toimijoidensa toteuttamansa kyberturvallisuusriskien hallintatoimenpiteet, joiden avulla toteutetaan 21 artiklan vaatimuksia. Riskienhallintatoimenpiteiden täytäntöönpanon valvonta on myös hallintoelinten vastuulla, ja heidät voidaankin saattaa vastuuseen 21 artiklan vaatimusten rikkomisista. Direktiivi velvoittaa hallintoelinten jäseniä osallistumaan koulutukseen ja jäsenmaita kannustumaan hallintoelinten jäseniä järjestämään koulutusta myös työntekijöilleen.[53]

---

[48] Andersson 2024, s.52.
[49] Seppänen 2024, s.2.
[50] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.30.
[51] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.311.
[52] HE 57/2024 vp., s.14.
[53] HE 57/2024 vp., s.15.

Myös yleisen tietosuoja-asetuksen 32 artiklassa on säädetty käsittelyn tietoturvallisuudesta, jossa keskiössä on henkilötietojen suojaan liittyvät riskit. Rekisterinpitäjän sekä henkilötietojen käsittelijän tulee toiminnassaan toteuttaa riskin taso huomioiden oikeasuhtaiset ja asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta riskin vaatima turvallisuustaso voidaan säilyttää käsittelyssä. Organisatorisilla toimenpiteillä viitataan kaikenlaisiin toimintalinjauksiin, periaatteisiin, organisaatiojärjestelyihin sekä henkilöstöä koskeviin ohjeistuksiin, koulutuksiin ja valvontaan. Myös henkilöstön tehtävien ja vastuualueiden määrittely ovat keskeisiä organisatorisia toimia.[54] Riskin huomioivat toimenpiteet tulee suhteuttaa vallitseviin olosuhteisiin, joihin kuuluvat uusin teknologia ja toimenpiteiden toteuttamiskustannukset sekä käsittelyn luonne, laajuus ja konteksti. Toimenpiteiden toteutuksessa tulee tietysti ottaa huomioon myös luonnollisten henkilöiden oikeudet ja vapaudet sekä niihin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit. Tällä tarkoitetaan käytännössä sitä, että kaikki riskit eivät vaadi samantasoisia toimenpiteitä, vaan niin sanotusti vähäpätöisempien riskien torjuntaan riittää kevyemmätkin ja edullisemmatkin toimenpiteet kun taas vakavammat riskit vaativat kaikki mahdolliset saatavissa olevat turvamekanismit.[55]

2.2 Kyberkestävyys ja kybersolidaarisuus

Euroopan unionissa on pyritty edistämään kyberuhkiin varautumista, niiden sietokykyä sekä turvaamaan niiden toteutuessa turvallisuus sekä yhteiskunnan toimintakyky. Digitaalisia elementtejä sisältäville tuotteille, kuten ohjelmistoille ja laitteille asetettiin yhteiset standardit 10.12.2024 voimaan astuneella kyberresilienssi- eli kyberkestävyyssäädöksellä ((EU) 2024/2847). Kyberresilienssisäädöksen tarkoituksena on tietyt vähimmäisedellytykset luomalla varmistaa, että markkinoille saatettavat laitteisto- ja ohjelmistotuotteet sisältävät alun alkaen markkinoille tullessaan vähemmän haavoittuvuuksia, ja että tietoturvaan suhtaudutaan valmistajien toimesta vakavasti koko tuotteen elinkaaren

[54] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.304.
[55] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.370–373.

ajan.[56] Kyberresilienssisäädöksen tavoitteena on siis 1 artiklan mukaan osaltaan yhtenäistää EU:n alueella digitaalisia tuotteita koskevia kyberturvallisuusvaatimuksia, ja siten parantaa kybertuvallisuuden tasoa. Yleisen tietosuoja-asetuksen 25 artikla vaatii, että tietosuoja huomioitaisiin keskeisesti jo heti tietojärjestelmien suunnittelun sekä henkilötietojen käsittelyn alussa eikä vasta valmiin olemassa olevan tuotteen kohdalla niin sanotusti jälkikäteisesti päälle liimattuna. Artiklalla viitataan siihen, että heti alusta alkaen teknisten tuotteiden tai tietojärjestelmien suunnittelussa toimittaisiin tietosuojan toteuttaminen edellä, jotta lopullisesta tuotteesta saataisiin varmasti tietoturvallinen kokonaisuus[57]. Kyberresilienssi- eli kyberkestävyyssäädöksen 2 artiklassa määritellään soveltamisala, jonka mukaan säädös koskee ohjelmistoja, laitteita, IoT-tuotteita sekä erikseen myytäviä digitaalisia komponentteja.

Kyberkestävyyssäädöksen 13 artiklassa on määritelty olennaisimmat kyberturvallisuusvaatimukset, jotka säädös asettaa tuotteiden valmistajille. Olennaista on, että digitaalisen tuotteen valmistajan tulee arvioida tuotteen turvallisuutta koko sen kehityksen ja elinkaaren ajan ja, että sen jokaisessa vaiheessa on menetelty kyberturvallisuusvaatimusten mukaisesti. Valmistajan tulee kyseisen artiklan mukaan tehdä kyberturvallisuusriskien arvioinnit sekä ottaa arviointien tulokset huomioon kehittelyssä, suunnittelussa ja toteutuksessa. Valmistajan tulee dokumentoida kaikki tuotetta koskevat turvallisuusratkaisut sekä siihen liittyvät mahdolliset haavoittuvuudet. Valmistajan vastuulla on myös ylläpitää tuotetta ja toimittaa siihen tietoturvapäivityksiä pitääkseen tuotteen kyberturvallisuuden tason ajan tasalla.

Kyberkestävyyssäädöksen 14 artiklan mukaan valmistajia koskee raportointivelvoite havaituista hyödynnetyistä haavoittuvuuksista tai vakavista tietoturvapoikkeamista tuotteessaan. Valmistajan on annettava ennakkoilmoitus ilman aiheetonta viivytystä, kuitenkin 24 tunnin kuluessa CSIRT-yksikölle ja ENISA:lle havaittuaan haavoittuvuuden tai va-

[56] EUVL L 2024/2847, 20.11.2024, s.1.
[57] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.311.

kavan tietoturvapoikkeaman tuotteessaan. Lisäksi on toimitettava haavoittuvuusilmoitus 72 tunnin sisällä poikkeaman havaitsemisesta sekä loppuraportti viimeistään 14 päivän kuluttua havainnosta.

Myös maahantuojille on määritelty velvoitteet 19 artiklassa, jonka mukaan maahantuoja voi tuoda markkinoille vain sellaisia digitaalisia tuotteita tai elementtejä, jotka täyttävät säädöksen liitteessä 1 mainitut olennaiset kyberturvallisuusvaatimukset. Olennaisilla kyberturvallisuusvaatimuksilla tarkoitetaan muun muassa laitteen riskienhallinnan tasoa, riittäviä päivityksiä sekä laitteen suojaamista luvattomalta käytöltä esimerkiksi pääsynhallinnan tai muun todennusjärjestelmän avulla. Kyberkestävyyssäädöksen avulla pyritään siis luomaan laitteille ja järjestelmille kyberturvallisuuden vähimmäistaso, jotta tietoturvallisuus voitaisiin taata kaikin mahdollisin keinoin. Vaatimusten mukaisuutta valvotaan ja säädös antaa kansallisen liikkumavaran säätää rikkeistä koituvien seuraamusten määräämisestä ja toteuttamisesta.

Euroopan unionin kybersolidaarisuussäädöksen ((EU) 2025/38) avulla on tarkoitus parantaa kyberturvallisuuspoikkeamiin varautumista sekä niiden havaitsemista ja niihin reagoimista koko Euroopan unionin alueella.[58] Säädöksen avulla on tavoitteena vahvistaa Euroopan unionin yhteisiä havaitsemis-, tilannetietoisuus- ja reagointivalmiuksia merkittävien ja laajamittaisten kyberturvallisuusuhkien varalta.[59] Kybersolidaarisuussäännöksellä on tarkoitus luoda niin sanottu eurooppalainen suojakilpi, jolla tarkoitetaan Euroopan kyberturvallisuuden hälytysjärjestelmää. Järjestelmässä hyödynnetään kansallisia ja rajat ylittäviä turvallisuusoperaatiokeskuksia ympäri unionin alueen. Keskukset hyödyntävät muun muassa tekoälyä ja data-analytiikkaa havaitakseen mahdollisia kyberturvallisuusuhkia ja jakaakseen niistä varoituksia viranomaisille yli kansallisten rajojen.[60] NIS2-direktiivi tukee osaltaan kybersolidaarisuussäädöksen toteutumista, sillä direktiivin

[58] EUVL L 2025/38, 15.1.2025, s.3.
[59] EUVL L, 2025/38, 15.1.2025, s.2.
[60] EUVL L 2025/38, 15.1.2025, s.2.

tavoitteena on kehittää yhteistyötä EU:n jäsenvaltioiden kansallisten viranomaisten välillä parantaakseen kyberturvallisuuden tasoa.[61]

Kybersolidaarisuussäädöksen keskeinen tavoite on mahdollistaa kyberuhkien ja poikkeamien nopeampi havaitseminen ja niihin reagoiminen. Tarkoituksena on tiivistää jäsenvaltioiden yhteistyötä kyberturvallisuuspoikkeamien havaitsemiseksi, jotta niistä voitaisiin myös palautua nopeammin, ja jotta niistä voitaisiin oppia ja estää samankaltaiset poikkeamat jatkossa.[62] Kybersolidaarisuussäädöksen myötä perustetaan jäsenmaiden yhteinen rajat ylittävä valvontaverkosto, jonka toiminnassa hyödynnetään tekoälypohjaista uhkien tunnistusta. Tarkoituksena on myös luoda yhteinen varoitusjärjestelmä, jossa havaituista uhista ja poikkeamista voidaan varoittaa myös muita verkoston jäseniä helposti ja nopeasti[63]. Tämä mahdollistaa muun muassa asiantuntija-avun hyödyntämisen yli kansallisten rajojen poikkeamatilanteissa ja niiden selvittelyssä. Verkostossa voidaan myös järjestää yhteisiä harjoituksia poikkeamatilanteiden varalle[64].

2.3 Kyberturvallisuuspoikkeaman raportointi ja sen haasteet

Uuden NIS2-direktiivin tavoitteena on yleisesti vahvistaa ja luoda Euroopan unionin alueella yhteinen kyberturvallisuuden taso. Direktiivin tarkoituksena on pyrkiä poistamaan jäsenvaltioiden välisiä eroavaisuuksia aiemman NIS1-direktiivin täytäntöönpanossa vahvistamalla tietty kyberturvallisuuden vähimmäistaso. Vähimmäistaso pyritään saavuttamaan toiminnalle asetetun koordinoidun sääntelykehyksen, jäsenvaltiokohtaisten vastuuviranomaisten vahvistamisen sekä ajantasaisten luetteloiden laatimisen avulla kyberturvallisuusvelvoitteita noudattavista aloista sekä toiminnoista. Myös tehokkaista oikeussuojakeinoista ja täytäntöönpanotoimenpiteistä säätämällä on pyritty edistämään

[61] HE 57/2024 vp, s.10.
[62] EUVL L 2025/38, 15.1.2025, s.2.
[63] EUVL L 2025/38, 15.1.2025, s.10.
[64] EUVL L 2025/38, 15.1.2025, s.5.

vähimmäistason saavuttamista.[65] Uudessa NIS2-direktiivissä pyritään myös laajentamaan soveltamisalaa ottamalla uusia oleellisia toimialoja riskienhallintavelvoitteiden ja poikkeamien ilmoittamisvastuiden piiriin, ja näin ollen parantamaan mahdollisuuksia kyberturvallisuuden vähimmäistason määrittämiseksi yhä useammalla toimialalla.[66] Direktiivin tarkoituksena on siis saada unionin jäsenvaltiot parantamaan kyberturvallisuusvalmiuksiaan direktiivin määrittämien keinojen avulla.

NIS2-direktiivin soveltamisala määritellään direktiivin 2 artiklassa, jonka mukaan direktiiviä sovelletaan sellaisiin Euroopan unionissa toimiviin julkisiin ja yksityisiin toimijoihin, jotka täyttävät suosituksen 2003/361/EY 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset tai ylittävät samaisen artiklan 1 kohdan keskisuurten yritysten määrittelyn kynnysarvot. Direktiiviä sovelletaan erityisesti yleisiin sähköisten viestintäverkkojen tai yleisesti saatavilla olevien viestintäpalvelujen tarjoajiin, luottamuspalveluiden tarjoajiin sekä toimijoihin, jotka tarjoavat jäsenvaltiossa ainoana toimijana palvelua, joka on keskeinen yhteiskunnan tai talouden kriittisten toimintojen järjestämisen kannalta. Soveltamisala kattaa myös toimijat, joiden palveluihin kohdistuva häiriö saattaa vaikuttaa merkittävästi yleiseen turvallisuuteen, järjestykseen tai kansanterveyteen sekä toimijoihin, joiden palveluissa tapahtuva häiriö saattaisi aiheuttaa hyvin merkittävän systeemisen riskin, jolla olisi rajat ylittäviä vaikutuksia. Myös julkishallinnon toimijat, jonka jäsenvaltio on kansallisen lainsäädännön tasolla määritellyt keskustason julkishallinnon toimijaksi tai aluetason julkishallinnon toimijaksi ja, joka riskiperusteisen arvion perusteella tarjoaa sellaisia palveluita, joiden häiriintymisestä voisi koitua merkittäviä vaikutuksia yhteiskunnan tai talouden kriittisiin toimijoihin, sovelletaan direktiivin vaatimuksia. Näitä edellä mainittuja toimijoita kutsutaan NIS2-direktiivissä keskeisiksi toimijoiksi.

Keskeisten toimijoiden lisäksi NIS2-direktiivin 3 artiklassa on määritelty direktiivin soveltamisen kannalta keskeiset sekä tärkeät toimijat, jotka koosta riippumatta kuuluvat direktiivin soveltamisalaan. Jaottelu keskeisiin ja tärkeisiin toimijoihin määrittää toimijaa

[65] HE 57/2024 vp, s.10–11.
[66] Andersson 2024, s.307.

koskevat valvontatoimivaltuudet. Pääpiirteissään keskeisten toimijoiden tulee valvonnassaan kattaa etukäteis- sekä jälkikäteisvalvontaa, kun taas tärkeiden toimijoiden kohdalla direktiivin nojalla riittää pelkkä jälkikäteisvalvonta.[67] Keskeisiä toimijoita ovat muun muassa keskisuuren yrityksen kynnysarvot ylittävät yritykset, luottamuspalveluiden tarjoajat ja aluetunnusrekisterit sekä yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalveluiden tarjoajat. Myös keskustason julkishallinnon toimijat katsotaan keskeisiksi toimijoiksi. Tärkeinä toimijoina pidetään direktiivin 3 artiklan 2 kohdan mukaan toimijoita, jotka eivät täytä keskeisen toimijan määritelmää, mutta ovat direktiivin soveltamisalan piirissä. Tärkeitä ja keskeisiä toimijoita koskevat direktiivin tarkoittamat riskienhallinta- ja raportointivelvoitteet.[68]

NIS2-direktiivissä on määritelty vähimmäistason, mahdollisimman teknologianeutraaleja riskienhallintavelvoitteita, jotka toimijoiden on otettava käyttöön toiminnassaan. Koska kyseessä on vähimmäistason velvoitteet, voivat toimijat halutessaan ottaa käyttöön myös tiukempia toimia tai kansallisesti voidaan säätää tiukemmista velvoitteista. [69] Artiklan 20 mukaisesti tärkeiden ja keskeisten toimijoiden hallintoelinten tulee hyväksyä toteuttamansa kyberturvallisuusriskien hallintatoimenpiteet sekä valvoa niiden täytäntöönpanoa noudattaakseen artiklaa 21. Mikäli hyväksyttyjä hallintatoimenpiteitä ei noudateta, voidaan hallintaelinten toimijat saattaa vastuuseen. Lisäksi hallintoelinten jäsenet on velvoitettu osallistumaan koulutukseen sekä tarjota työntekijöilleen koulutusta jäsenmaiden kannustuksella. [70]

NIS2-direktiivin 23 artiklassa on määritelty merkittävien kyberturvallisuuspoikkeamien raportointivelvoitteesta. Merkittävällä kyberturvallisuuspoikkeamalla tarkoitetaan NIS2-direktiivin 23 artiklan 1 kohdan mukaan poikkeamaa, joka vaikuttaa merkittävästi palvelujen tarjoamiseen. Poikkeama katsotaan merkittäväksi, jos se aiheuttaa tai voi aiheuttaa

[67] HE 57/2024 vp., s.13.
[68] HE 57/2024 vp., s.14.
[69] HE 57/2024 vp., s.14.
[70] HE 57/2024 vp., s.15.

vakavan toimintahäiriön palvelujen tuottamiselle tai asianomaiselle toimijalle taloudellista tappiota tai jos poikkeamalla on vaikutusta luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttaen huomattavaa aineellista tai aineetonta haittaa.[71] Mikäli toimija kohtaa merkittävän kyberturvallisuuspoikkeaman, on poikkeamasta ilmoitettava NIS2-direktiivissä säädetyn raportointivelvoitteen mukaisesti CSIRT-yksikölle tai toimivaltaiselle valvontaviranomaiselle[72]. Kyberturvallisuuslain (124/2025) 4 luvun 26 pykälän mukaan Suomessa NIS2-direktiivin valvonta on hajautettu toimialan mukaan eri viranomaisille, mutta kansallinen koordinoiva valvova viranomainen on Liikenne- ja viestintävirasto Traficom, jonka alaisuudessa toimii Kyberturvallisuuskeskus.

Toimijoiden raportointivelvoite merkittävästä kyberturvallisuuspoikkeamasta on NIS2-direktiivin 23 artiklan 4 kohdan mukaan kolmiportainen. Kun toimija havaitsee merkittävän poikkeaman, tulee siitä antaa ensi-ilmoitus ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluessa poikkeaman havaitsemisesta. Ensi-ilmoituksessa toimijan tulee kertoa, epäilläänkö poikkeaman taustalla olevan lainvastaisia tai vihamielisiä toimia sekä onko poikkeamalla rajat ylittäviä vaikutuksia. Mikäli poikkeamalla todetaan olevan rajat ylittäviä vaikutuksia, tiedotetaan poikkeamasta myös poikkeamaan liittyviä jäsenvaltioita sekä Euroopan unionin kyberturvallisuusvirastoa ENISA:a.

Ensi-ilmoituksen jälkeen viranomaiselle tulee toimittaa varsinainen poikkeamailmoitus, jossa ensi-ilmoituksen tiedot tulee päivittää ja antaa alustavat arviot poikkeamasta, sen laajuudesta, vakavuudesta sekä sen vaikutuksista. Poikkeamailmoitukseen tulee liittää mahdolliset saatavilla olevat vaarantumisindikaattorit eli poikkeamaa koskevat lokitiedot, joiden perusteella voidaan päätellä, milloin poikkeama on tapahtunut ja onko se edelleen käynnissä[73]. Poikkeamailmoitus tulee jättää 72 tunnin kuluessa merkittävän poik-

[71] HE 57/2024 vp., s.17.
[72] HE 57/2024 vp., s.16.
[73] HE 57/2024 vp., s.187.

keaman havaitsemisesta. Mikäli toimija on luottamuspalvelun, kuten sähköisten allekirjoitusten tai varmenteiden tarjoaja, tulee palveluun tai sen tarjontaan vaikuttavasta poikkeamasta jättää poikkeamailmoitus 24 tunnin kuluessa poikkeaman havaitsemisesta.

Viimeistään kuukauden kuluttua poikkeamailmoituksen jättämisestä kolmantena vaiheena tulee laatia loppuraportti, jossa käydään tarkasti läpi poikkeaman kuvailu, vakavuus sekä sen vaikutukset. Loppuraporttiin kirjataan myös, mikä uhka tai juurisyy poikkeaman todennäköisesti aiheutti sekä tehdyt toimenpiteet tai suunnitellut toimet vaikutusten lieventämiseksi. Mikäli poikkeama ei ole vielä kuukauden kuluttua poikkeamailmoituksen jättämisestä päättynyt, toimijan on toimitettava edistymisraportti tilanteen käsittelystä. Kuukauden kuluttua poikkeaman käsittelyn päättymisestä on toimitettava vielä lopullinen raportti.[74]

Niin sanotusta vapaaehtoisesta ilmoittamisesta säädetään NIS2-direktiivin 30 artiklassa. Vapaaehtoisella ilmoittamisella tarkoitetaan muita ilmoituksia kuin, joihin toimijalla on esimerkiksi merkittävän poikkeaman kohdalla direktiivin määräämä velvoite. Toimija voi siis vapaaehtoisesti ilmoittaa kyseisen artiklan nojalla valvovalle viranomaiselle poikkeamista, kyberuhkista sekä mahdollisista läheltä piti-tilanteista. Valvova viranomainen on velvoitettu ottamaan myös vapaaehtoisia ilmoituksia vastaan sekä käsittelemään niitä kuten velvoittavia ilmoituksia.[75]

Erityisesti direktiivin asettamat tiukat aikarajat, joiden aikana havaituista poikkeamista tulee ilmoittaa, voivat olla organisaation näkökulmasta haastavia. Ensi-ilmoitus poikkeamasta tulisi antaa 24 tunnin kuluessa poikkeaman havaitsemisesta. Haasteena voi olla tunnistaa poikkeama ja varmistua, että kyseessä on todella poikkeama. On myös tulkinnanvaraista, milloin kyseessä todella on merkittävän poikkeaman määritelmän täyttävä poikkeama, jolloin ilmoitusvelvollisuuden kriteeristö täyttyy. Mikäli organisaatiossa ei toteuteta riittävän laajaa valvontaa tai riskienhallintatoimet eivät ole riittävällä tasolla,

[74] HE 57/2024 vp., s.17.
[75] HE 57/2024 vp., s.18.

voi poikkeaman havaitseminen olla itsessään jo haaste. Kun poikkeama on havaittu, 24 tuntia on äärimmäisen lyhyt aika kerätä kaikki ensi-ilmoitukseen tarvittavat tiedot.

Raportoinnin kolmiportaisuus lisää myös organisaatioissa seurannan ja vastuuttamisen tarvetta. Kuka organisaatiossa on vastuussa raportoinnista ja sen seurannasta, jossa ensi-ilmoituksen jättämisen jälkeen poikkeamailmoitus sekä loppuraportti tai mahdollinen edistymisraportti jätetään määräajassa ja riittävän laadukkaasti täytettynä?

3 Tietosuoja ja yksityisyyden suoja raportoinnissa

3.1 Tietosuoja ja henkilötietojen suojaaminen käsitteenä

Lähtökohtaisesti julkisuusperiaatteen mukaisesti viranomaisten asiakirjat ovat julkisia ja julkisesta vallankäytöstä sekä viranomaisten muusta toiminnasta on jokaisella tasavertainen oikeus saada tietoa niin halutessaan. Perustuslain (731/1999) 12 §:n 2 momentissa säädetyn julkisuusperiaatteen mukaan viranomaisen asiakirjat ja tallenteet ovat julkisia, ellei niiden julkisuutta ole erikseen lailla välttämättömien syiden takia rajoitettu.[76] Viranomaisen menettelyn tulisi julkisuusperiaatteen mukaan olla avointa, joka merkitsee, että viranomaisella olevat tiedot tulee olla avoimesti kaikkien saatavilla ja käytettävissä. Viranomaisten tulisi myös tiedottaa toiminnastaan julkisuusperiaatteen mukaisesti.[77] Julkisuusperiaatteen pääasiallisena tarkoituksena on mahdollistaa hallintotoimintaan ja hallinnolliseen päätöksentekoon vaikuttamisen sekä osallistumisen yhteiskunnalliseen toimintaan ja päätöksenteon valmisteluun avoimen hallintotoiminnan kautta[78].

Julkisuusperiaatteen soveltamiseen liittyy muiden perusoikeuksien asettamia poikkeuksia muun muassa tilanteessa, jossa viranomaisen julkiset asiakirjat sisältävät henkilötietoja.[79] Näiden muiden perusoikeussäännösten julkisuutta tukevat, julkisuuteen rajoituksia asettavat tai mahdollisesti jopa ristiriidassa olevat oikeudet eivät sinällään tee julkisuusperiaatetta merkityksettömäksi, vaan muiden perusoikeussäännösten vaatimat suojan tarpeet otetaan julkisuutta soveltaessa huomioon joko nimenomaisella lainsäädännöllä tai muun oikeudellisen tulkinnan avulla[80]. Yksi näistä poikkeuksista on perustuslain

[76] Mäenpää 2020, s.5.
[77] Mäenpää 2020, s.1–2.
[78] Mäenpää 2017, s.334–335.
[79] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.17.
[80] Mäenpää 2017, s.330.

10 pykälän takaama perusoikeus yksityiselämän suojaan. Yksityiselämän suojan mukaisesti jokaisella on oikeus yksityiselämän, kunnian sekä kotirauhan turvaamiseen ja yksityiselämää koskevien tietojen ja luottamuksellisten viestien salaisuus on loukkaamaton. Myös Euroopan ihmisoikeussopimuksen 8 artiklassa taataan jokaisen oikeus nauttia yksityis- ja perhe-elämää, kotia sekä kirjeenvaihtoa koskevaa kunnioitusta.[81] Lisäksi Euroopan unionin perusoikeuskirjan 7 artiklassa on turvattu yksityiselämän suoja[82].

Henkilötiedot voidaan katsoa osaksi yksityiselämän suojaa, mikäli ne ovat yksityiselämää koskevia tietoja, mutta kaikki henkilötiedot eivät aina suoraan kuulu yksityiselämän suojan piiriin. Toisaalta yksityiselämää koskevat tiedot luetaan aina henkilötiedoiksi, mikäli tiedot kyetään yhdistämään tiettyyn henkilöön.[83] Näin ollen henkilötiedot voidaan siis tietyissä tilanteissa katsoa osaksi perustuslain 10 §:n mukaista yksityisyyden suojaa, joka asettaa poikkeuksen julkisuusperiaatteelle. Henkilötietojen suoja on osana yksityisyyden suojaa siis turvattu perusoikeutena perustuslain 10 §:n 1 momentissa sekä perusoikeuskirjan 8 artiklassa. Henkilötietojen käsittelystä säännellään tarkemmin Euroopan unionin yleisessä tietosuoja-asetuksessa (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679[84]) sekä sitä täsmentävässä kansallisessa tietosuojalaissa (1050/2018).[85] Lisäksi henkilötietojen suojaa on melko vakiintuneesti sovellettu Euroopan unionissa osana yksityiselämän suojaa[86].

Yleisen tietosuoja-asetuksen 4 artiklassa on määritelty, että henkilötiedolla tarkoitetaan kaikkia niitä tietoja, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Henkilötietoja voivat olla siis esimerkiksi nimi, henkilötunnus, sijaintitieto tai jokin kyseiselle henkilölle tunnusomainen fyysinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä, jonka perusteella henkilö ja sitä koskeva

[81] Mäenpää 2020, s.31.
[82] Mäenpää 2020, s.38.
[83] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.16.
[84] EYVL N:o L 119, 4.5.2016.
[85] Mäenpää 2020, s.39.
[86] Ojajärvi 2022, s.108.

tieto voidaan yhdistää toisiinsa. Yleisen tietosuoja-asetuksen antama määritelmä henkilötiedolle on laajempi, mitä ennen asetuksen antamista, eikä määritelmää voi kansallisella lainsäädännöllä kaventaa.[87]

Tietosuojalla tarkoitetaan siis tiivistetysti yksityisyyden suojaamista henkilötietoja käsiteltäessä[88]. Käsitteellä tarkoitetaan ihmisten yksityiselämän suojaamista, sisältäen jokaisen oikeuden henkilötietoihinsa. Tietosuojan perusajatuksena on taata henkilötiedoille suoja tietojen vahingoittavalta käytöltä.[89] Tietoturva on yksi tietosuojan osa, jonka tavoitteena on suojata järjestelmät, tietoaineistot sekä palvelut teknisin ja organisatorisin toimin ottaen tietojen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat riskit huomioon[90]. Luottamuksellisuudella tarkoitetaan, että varmistetaan tietojen olevan vain niiden käyttöön oikeutettujen saatavilla eikä tietoihin ole muilla mahdollisuutta päästä käsiksi. Eheydellä tarkoitetaan tietojen virheettömyyden ja luotettavuuden takaamista ja sitä, että tietojen muuttaminen voi tapahtua vain siihen oikeutettujen tahojen toimesta ja, että tiedot säilyvät suunnitellulla tavalla. Saatavuudella tarkoitetaan, että tietoja ja tietojärjestelmiä voi hyödyntää tarvittaessa kaikki niihin oikeutetut.[91] Tietoturvatoimenpiteiden avulla siis toteutetaan tietosuojaa eli suojataan henkilötietoja[92].

3.2 Yksityisyydensuoja ja sen merkitys poikkeamatilanteessa

3.2.1 Yksityisyydensuojan periaatteet

Yleisen tietosuoja-asetuksen toisessa luvussa on säädetty periaatteet, joiden mukaan henkilötietojen käsittelyä tulisi toteuttaa. Tietosuoja-asetuksen 5 artiklan mukaan hen-

[87] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.58–61.
[88] Valtiovarainministeriö 2016, s.12.
[89] Valtiovarainministeriö 2016, s.13.
[90] Andersson 2024, s.43. Myös Korpisaari, Pitkänen ja Warma-Lehtinen 2022, s.371.
[91] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.371.
[92] Andersson 2024, s.50.

kilötietojen käsittelyä koskevat periaatteet ovat lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus. Henkilötietojen käsittelylle on oltava lainmukainen peruste, joka voi yleisen tietosuoja-asetuksen 6 artiklan mukaan olla suostumus käsittelylle, jonkin sopimuksen täytäntöönpano, rekisterinpitäjän lakisääteisen velvoitteen noudattaminen, elintärkeiden etujen suojaaminen, yleistä etua koskevan tehtävän suorittaminen tai rekisterin pitäjälle kuuluvan julkisen vallan käyttäminen ja oikeutettujen etujen toteuttaminen.

Suostumuksella tarkoitetaan yleisen tietosuoja-asetuksen 7 artiklan mukaan tahdonilmaisua, jonka on oltava vapaaehtoinen, yksilöity, tietoinen sekä yksiselitteinen[93]. Tahdonilmaisulla hyväksytään omien henkilötietojen käsittely.[94] Henkilötietojen käsittelyn näkökulmasta suostumus on rekisteröidylle ainoa omaa osallistumista edellyttävä oikeusperuste, jonka avulla rekisteröity voi vaikuttaa omien henkilötietojensa käsittelyn sallimiseen. Käytännössä tämä tarkoittaa, että rekisteröidyn tietoja on mahdollista käsitellä tietyissä tapauksissa vain, jos rekisteröity on itse antanut vapaaehtoisesti, yksilöidysti, tietoisesti sekä yksiselitteisesti oman suostumuksensa tietojen käsittelylle. Suostumus on oikeutettua myös peruuttaa milloin tahansa.[95] Suostumus siis edellyttää aktiivista toimintaa, jolla voidaan tarkoittaa esimerkiksi tietyn kohdan rastittamista tai kirjallisen suostumuslomakkeen täyttämistä. Verkkosivuilla ei voida rekisteröidyn puolesta valmiiksi rastittaa ruutua, jolla rekisteröity antaisi suostumuksensa henkilötietojen käsittelylle, sillä tällöin suostumuksen antamisen edellytykset vapaaehtoisesta, yksilöidystä, tietoisesta ja yksiselitteisestä tahdonilmaisusta eivät täyttyisi.[96]

Henkilötietojen käsittelyssä kohtuullisuudella tarkoitetaan reiluutta, jonka nimissä käsittelyssä tulee ottaa huomioon myös ihmisten edut ja odotukset. Kohtuullisuuden mukaan tietoja ei saa käyttää väärin ja se varmistaa, ettei rekisteröidyn tietoja kerätä tai muutoin

[93] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.79.
[94] Hanninen, Laine, Rantala, Rusi, Varhela 2017, s.23.
[95] Ojajärvi 2022, s.115.
[96] Hanninen, Laine, Rantala, Rusi, Varhela 2017, s.36.

käsitellä salassa.[97] Läpinäkyvyyden periaatteella pyritään takaamaan, että rekisteröity on aina tietoinen, miten hänen henkilötietojaan kerätään, käytetään sekä käsitellään. On pitkälti rekisterinpitäjän vastuulla, että henkilötietojen käsittelyyn liittyvät tiedot ja viestintä ovat läpinäkyvästi ja helposti rekisteröidyn saatavilla, riittävän selkeällä ja yksinkertaisella kielellä ilmaistuna.[98] Käyttötarkoitussidonnaisuuden tarkoituksena on rajoittaa rekisterinpitäjän mahdollisuuksia käyttää keräämiään tietoja. Käyttötarkoitussidonnaisuuden mukaan tietoja saa kerätä vain tiettyä laillista tarkoitusta varten, eikä tietojen käsittely saa myöhemmin olla näiden tarkoitusten kanssa yhteensopimatonta. Tavoitteena on siis taata, että rekisteröidyn odotukset tietojensa käsittelystä toteutuu, eikä rekisteröityä johdeta harhaan.[99]

Kerättyjen henkilötietojen tulee olla käsittelyn kannalta tarpeellisia ja olennaisia, ja niitä on käsiteltävä vain, jos tarkoitusta ei ole mahdollista toteuttaa muiden keinojen avulla kohtuullisesti. Tätä kutsutaan tietojen minimointiperiaatteeksi, jonka mukaan tiedot tulee myös poistaa, kun ne ovat muuttuneet tarpeettomiksi. Tietojen tarpeellisuutta voidaan arvioida, onko rekisterinpitäjällä enää toimintansa kannalta perusteltua syytä käsitellä tai säilyttää kyseisiä henkilötietoja.[100] Lisäksi rekisterinpitäjän on pidettävä huolta, että käsiteltävät tiedot ovat täsmällisiä ja ajantasaisia, ja että virheelliset tiedot joko korjataan tai poistetaan viipymättä[101]. Tarkoituksena on, että henkilötietoja säilytetään mahdollisimman lyhyen ajan. Joissakin tapauksissa säilytysaika saattaa olla lain määrittelemä velvollisuus, mutta rekisterinpitäjän on toimissaan varmistettava, ettei henkilötietoja säilytetä pidempään kuin on tarve tai perusteet.[102]

Euroopan unionin yleisen tietosuoja-asetuksen 32 artiklassa määritellään henkilötietojen turvallisesta käsittelystä. Kyseisen artiklan 1 kohdan mukaan henkilötietojen käsitte-

[97] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.102.
[98] Koivumäki & Häkkänen 2018, s.177. Myös Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.102.
[99] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.103.
[100] Koivumäki, Häkkänen 2018, s.180. Myös Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.104.
[101] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.107.
[102] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.107–108.

lyssä tulee ottaa huomioon kaikki riskit, jotka voivat vaikuttaa luonnollisen henkilön oikeuksiin ja vapauksiin, ja toimia riskiä vastaavan turvallisuustason mukaisesti toteuttaen tarvittavat ja asianmukaiset tekniset sekä organisatoriset toimenpiteet. Tällaisia toimenpiteitä voivat samaisen artiklan 1 kohdan alakohtien a-d mukaan olla henkilötietojen pseudonymisointi tai salaus, käsittelyjärjestelmien jatkuvan luottamuksellisuuden, eheyden, käytettävyyden ja vikasietoisuuden takaaminen, tietojen palauttaminen nopeasti saataville ja tietoihin pääsyn takaaminen fyysisen tai teknisen vian sattuessa sekä menettely, jolla voidaan tietojenkäsittelyn turvallisuuden varmistamiseksi testata, tutkia tai arvioida teknisten ja organisatoristen toimenpiteiden tehokkuutta. Yleistä tietosuoja-asetusta soveltaessa tulee ottaa huomioon lähtökohtana oleva riskiperusteisuus, jonka mukaan henkilötietojen käsittelyyn kohdistuvia riskejä tulee aina huomioida sen henkilön näkökulmasta, jonka tietoja käsittely koskee[103]. Henkilötietojen asianmukaisesta käsittelystä vastuu on rekisterinpitäjällä, jolla tarkoitetaan henkilötietojen käsittelystä vastaavaa henkilöä tai yritystä[104].

Henkilötietojen käsittelyllä tarkoitetaan kaikkia toimintoja, jotka kohdistuvat henkilötietoihin automaattisen tietojenkäsittelyn kautta tai manuaalisesti. Muun muassa henkilötietojen kerääminen, tallentaminen, järjestäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, yhdistäminen, saattaminen saataville, poistaminen sekä hävittäminen katsotaan kaikki henkilötietojen käsittelyksi.[105] Rekisteröidyn oikeudet ovat keskiössä yleisen tietosuoja-asetuksen toteuttamisessa[106]. Rekisteröidyllä tarkoitetaan henkilöä, jonka tietoja käsitellään[107]. Rekisteröity on oikeutettu saamaan tiedon hänen tietojensa käsittelystä, mihin tarkoitukseen tietoja kerätään ja käsitellään sekä kuinka kauan tietoja tullaan säilyttämään[108]. Lisäksi rekisteröidyllä on oikeus tarkistaa, mitä tietoja rekisterinpitäjällä on hänestä, tarvittaessa korjata virheelliset tiedot sekä tulla unohdetuksi, jolla tarkoitetaan, että tiedot tulee poistaa rekisteristä rekisteröidyn niin pyytäessä.

[103] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.33.
[104] Neuvonen 2019, s.234.
[105] Valtiovarainministeriö 2016, s.10.
[106] Neuvonen 2019, s.235.
[107] Koivumäki, Häkkänen 2018, s.173.
[108] Neuvonen 2019, s.235.

Rekisteröity voi myös tietyissä tilanteissa rajoittaa tietojensa käsittelyä sekä siirtää tiedot järjestelmästä toiseen niin halutessaan.[109] Rekisteröidyn oikeuksien toteutuminen on pääasiassa rekisterinpitäjän vastuulla, ja rekisterinpitäjän tuleekin toiminnassaan huolehtia näiden oikeuksien toteutumisesta. Tietosuojan toteutumista koskevan vastuunjaon pääsääntö määrää tietojen käsittelystä määräävän tahon olevan vastuussa myös tietosuojasääntelyn toteutumisesta, joka tarkoittaa rekisterinpitäjää[110].

3.2.2 Tietoturvaloukkauksista ilmoittaminen

Tietoturvariskillä viitataan yleensä ei-toivottuun tilanteeseen, joka uhkaa tietojen luottamuksellisuutta, eheyttä tai käytettävyyttä. Kun tietoturvariski realisoituu, tapahtuu tietoturvaloukkaus.[111] Tietoturvaloukkauksella tarkoitetaan lainvastaista tai vahingossa tapahtuvaa henkilötietojen tuhoamista, häviämistä, muuttamista tai luvatonta luovuttamista tai lainvastaista pääsyä henkilötietoihin, joka tapahtuu henkilötietojen käsittelyssä, siirrossa tai tallennuksessa. Tuhoamisen myötä tietoja ei enää ole saatavilla hyödynnettävässä muodossa, häviämisellä tarkoitetaan tilannetta, jossa tiedot ovat edelleen olemassa, mutta eivät kontrollissa tai niihin ei enää päästä käsiksi.[112] Tietoturvaloukkauksella voi olla merkittäviä vaikutuksia paitsi organisaation maineelle, myös varallisuudelle, toiminnalle tai mahdollisiin yhteiskumppanuus- ja sidosryhmäsuhteille[113]. Toisaalta luonnolliselle henkilölle saattaa koitua tietoturvaloukkauksen seurauksena laajaakin kärsimystä, mainehaittaa, varallisuuden menetyksiä sekä terveydellisiä ongelmia[114].

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tilannetta, jonka seurauksena rekisterinpitäjä ei ole enää kykeneväinen takaamaan tietosuoja-asetuksen 5 artiklan mukaisten henkilötietojen käsittelyn periaatteiden noudattamista. Tämän tiedon valossa kaikki

[109] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.191.
[110] Lindroos-Hovinheimo 2018, s.757–758.
[111] Andersson 2024, s.53.
[112] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.381. Myös Valtiovarainministeriö 2016, s.10.
[113] Andersson 2024, s.2.
[114] Andersson 2024, s.81.

tietoturvaloukkaukset eivät siis ole henkilötietojen tietoturvaloukkauksia, mutta kaikki henkilötietojen tietoturvaloukkaukset katsotaan tietoturvaongelmiksi.[115] Yleisen tietosuoja-asetuksen 32 artiklassa edellytetään henkilötietojen käsittelyssä toteutettavan riskiin nähden riittävän turvallisuustason takaamiseksi oikeasuhtaisia ja asianmukaisia teknisiä sekä organisatorisia toimenpiteitä. Mikäli näistä toimenpiteistä huolimatta riski realisoituu ja tietoturvaloukkaus pääsee tapahtumaan, on siitä ilmoitettava.[116]

Euroopan unionin yleisen tietosuoja-asetuksen 33 artiklassa säädetään henkilötietojen tietoturvaloukkauksesta ilmoittamisesta valvontaviranomaiselle. Artiklan sisällön mukaan henkilötietojen tietoturvaloukkauksesta tulee ilmoittaa ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta toimivaltaiselle kansalliselle valvontaviranomaiselle sekä tietyissä tapauksissa myös henkilölle, jonka tietoja loukkaus koskee. Jos henkilötietojen tietoturvaloukkauksesta ei aiheudu todennäköistä riskiä, joka kohdistuisi luonnollisten henkilöiden oikeuksiin tai vapauksiin, 72 tunnin määräaikaa tai ilmoitusta ei tarvitse toteuttaa. Mikäli 72 tunnin määräaika ei toteudu ilmoituksen jättämisessä, tulee rekisterinpitäjän toimittaa viranomaiselle perusteltu selitys viivästyksen syistä. Suomessa toimivaltainen valvontaviranomainen on tietosuojavaltuutettu.[117]

Henkilötietojen tietoturvaloukkauksesta valvovalle viranomaiselle annettavasta ilmoituksesta on 33 artiklan 3 kohdan mukaan käytävä ilmi kyseessä olevan loukkauksen kuvaus, joka sisältää mahdollisuuksien mukaan loukkauksen piirissä olevien asianosaisten rekisteröityjen ryhmät sekä niiden arvioidut lukumäärät ja kyseessä olevien henkilötietotyyppien ryhmät ja arviot lukumäärästä. Lisäksi on ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu lisätietoja antava yhteyspiste. Ilmoituksessa on kuvattava mahdolliset seuraukset, jotka henkilötietojen tietoturvaloukkauksesta on todennäköi-

[115] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.382.
[116] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.381.
[117] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.381.

sesti aiheutuneet. Rekisterinpitäjän on täytynyt ehdottaa tai toteuttaa toimenpiteitä tietoturvaloukkauksen vuoksi sekä myös lieventääkseen mahdollisia haittavaikutuksia. Organisaation tietosuojavastaava on hyvin keskeisessä roolissa tietoturvaloukkauksen tapahtumisen selvittämisessä sekä siitä tehtävän ilmoituksen laadinnassa ja mahdollisessa täydentämisessä[118].

Rekisterinpitäjän on toteutettava riskiarvio heti saadessaan tietoonsa tietoturvaloukkauksen. Euroopan tietosuojaneuvoston mukaan riskiarvio tulisi toteuttaa ilman yksityiskohtaisen teknisen tutkinnan alkamisen odottamista[119]. Voiko rekisterinpitäjä todellisuudessa tietää täysin, kuinka laajasta loukkauksesta on kyse ilman kunnollisia teknisiä selvityksiä, joissa voi kuitenkin kulua aikaa niin kauan, että 72 tunnin määräaika ehtii kulua umpeen? Onko tarkoituksenmukaista tehdä ilmoitus loukkauksesta, josta rekisterinpitäjällä ei todellisuudessa ole vielä riittävästi tietoa, ja voi pahimmillaan antaa tietosuojaviranomaiselle jopa virheellistä tietoa, jos myöhemmin tarkempien selvityksien yhteydessä selviääkin loukkauksen todellinen laajuus ja luonne? Yleisen tietosuoja-asetuksen 33 artiklan 4 kohta mahdollistaa kuitenkin loukkausta koskevien tietojen toimittamisen vaiheittain, mutta sekin tulee toteuttaa ilman aiheetonta viivytystä.

Yleisen tietosuoja-asetuksen 33 artiklan 5 kohdan mukaisesti rekisterinpitäjän tulee dokumentoida ja säilyttää henkilötietojen tietoturvaloukkauksia koskevat tiedot, vaikka loukkauksesta ei olisikaan tarvinnut ilmoittaa viranomaisille. Dokumentoinnin toteutuksesta rekisterinpitäjä saa päättää itse, mutta siihen on sisällytettävä tietoturvaloukkauksen kuvaus, sen vaikutukset sekä tilanteen korjaamiseksi tehdyt toimenpiteet. Osana dokumentointia rekisterinpitäjän tulee säilyttää myös loukkauksen tapahtuma-aikaan sijoittuvat lokitiedot. Toteutetun dokumentoinnin perusteella valvovalla viranomaisella on oltava mahdollisuus tarkistaa ja valvoa, että artiklaa ja sen määräämää ilmoitusvelvollisuutta on noudatettu.

[118] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.388.
[119] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.383.

Henkilötietojen tietoturvaloukkauksesta ilmoittamisesta rekisteröidylle säädetään yleisen tietosuoja-asetuksen 34 artiklassa. Artiklassa täydennetään artiklan 33 mukaista ilmoitusvelvollisuutta viranomaiselle säätämällä ilmoitusvelvollisuudesta myös niille henkilöille, jonka oikeuksille tai vapauksille kyseinen tietoturvaloukkaus aiheuttaa huomattavan riskin. Rekisteröidylle on yleisen tietosuoja-asetuksen 34 artiklan 2 kohdan mukaisesti annettava selkeällä ja yksikertaisella kielellä kuvaus sattuneesta henkilötietojen tietoturvaloukkauksesta, sen seurauksista sekä rekisterinpitäjän ehdottamista tai toteuttamista toimenpiteistä, joita loukkauksen vuoksi olisi toteutettava. Rekisteröidylle tulee myös ilmoittaa yhteystiedot tietosuojavastaavalle tai muulle yhteyspisteelle, josta voi pyytää lisätietoja. Käytännössä rekisteröidylle tehtävän ilmoituksen sisältö on samansisältöinen kuin valvovalle viranomaisellekin tehtävä ilmoitus, mutta rekisteröidyn ilmoituksessa vaatimuksena on, että siinä tulisi käyttää selkeää ja yksinkertaista kieltä.

Rekisteröidylle ei kuitenkaan tarvitse erikseen ilmoittaa sattuneesta loukkauksesta yleisen tietosuoja-asetuksen 34 artiklan 3 kohdan mukaan, mikäli rekisterinpitäjä on henkilötietojen käsittelyssään huolehtinut riittävistä teknisistä ja organisatorisista turvamekanismeista taatakseen riittävän turvallisuuden tason. Tämä pätee erityisesti, jos rekisterinpitäjä on hyödyntänyt salaustekniikoita, joiden avulla henkilötiedot on muutettu muotoon, jota ulkopuolisella tietoihin käsiksi pääsevällä taholla ei ole mahdollisuutta ymmärtää tai tulkita. Rekisteröidylle ei tarvitse ilmoittaa loukkauksesta, jos rekisteröidyn oikeuksiin ja vapauksiin kohdistuvaan korkeaan riskiin on reagoitu rekisterinpitäjän toimesta, ja on toteutettu jatkotoimenpiteitä, jotta riski ei olisi enää todennäköinen. Mikäli rekisteröidylle ilmoittamisesta koituisi rekisterinpitäjälle kohtuutonta vaivaa, voidaan rekisteröidylle jättää ilmoittamatta henkilökohtaisesti ja käyttää sen sijaan julkista tiedonantoa tai jotakin muuta yhtä tehokasta tiedonannon muotoa. Jokaisesta tietoturvaloukkauksesta ei tarvitse ilmoittaa erikseen rekisteröidylle, jotta voitaisiin taata, että oikeasti

merkittävät ilmoitukset huomioitaisiin, kun ilmoituksia ei tulisi jatkuvana tulvana[120]. Ilmoitus tulee antaa erillisenä viestinä, esimerkiksi sähköpostiviestinä tai tekstiviestinä rekisteröidylle, jotta ilmoitus varmasti huomataan[121].

Rekisteröidylle tehtävässä ilmoituksessa henkilötietojen tietoturvaloukkauksesta ei ole annettu erikseen tarkkaa aikamäärettä, jonka sisällä ilmoitus olisi tehtävä. Rekisteröidylle tulisi kuitenkin ilmoittaa kuitenkin ilman aiheetonta viivytystä. Yleensä ilmoitus tehdään tiiviissä yhteistyössä tietosuojavaltuutetun kanssa viranomaisten ohjeita noudattaen, sillä rekisterinpitäjän on ilmoitettava kuitenkin viranomaiselle kaikki loukkaukset, joista sen tulee ilmoittaa myös rekisteröidylle[122]. Rekisteröidylle on tarkoitus antaa mahdollisimman täsmällistä tietoa sattuneesta loukkauksesta, jotta rekisteröidyllä on mahdollisuus toteuttaa itseään ja tietojaan koskevat suojaavat toimet välttääkseen tai lieventääkseen mahdolliset lisähaittavaikutukset[123].

Toisaalta voi myös olla haastavaa tulkita, milloin ilmoitusvelvollisuus eli 72 tunnin aikaikkuna käynnistyy. Tähän vaikuttaa merkittävästi se, milloin tietoturvaloukkaus tulkitaan tulleen ilmi. Rekisterinpitäjän toteuttamien teknisten ja organisatoristen toimenpiteiden myötä loukkausten pitäisi tosin tulla ilmi heti, mikäli toimet ovat oikeasuhtaisia riskiin nähden ja toteutettu lain vaatimalla tavalla.[124]

Yleisen tietosuoja-asetuksen määrittämien ilmoitusta koskevien aikarajojen soveltaminen tai tulkinta siitä, mitä rekisterinpitäjänä toimivia tahoja ilmoittamisen velvoitteet koskevat, voivat olla varsin vaativaakin oikeudellista pohdintaa ja tulkintaa vaativia tapauskohtaisesti. Korkein hallinto-oikeus on antanut 1.11.2024 ratkaisun liittyen rekisterinpitäjän antamaa ilmoitusta tietoturvaloukkauksesta ja siitä, onko rekisterinpitäjä nou-

[120] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.393.
[121] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.395–396.
[122] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.395–396.
[123] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.394.
[124] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.385–386.

dattanut yleisen tietosuoja-asetuksen 33 ja 34 artiklojen mukaisia aikarajoja ilmoittaessaan loukkauksesta tietosuojavaltuutetulle sekä rekisteröidyille. Kyseessä oli suomalaisiin diplomaatteihin kohdistuneesta verkkovakoilusta, jossa käyttäjien puhelimiin oli asennettu heidän huomaamattaan ja ilman heidän toimenpiteitään NSO Groupin Pegasus -vakoiluhaittaohjelma, jolla päästiin käsiksi hyvin laajasti puhelimessa oleviin tietoihin sekä voitiin hyväksikäyttää puhelimen ominaisuuksia.[125]

Tapauksessa Ulkoministeriö on toiminut rekisterinpitäjänä ja tehnyt tietosuoja-asetuksen 33 artiklan mukaisesti tietosuojavaltuutetulle ilmoituksen 24.1.2022 havaitusta henkilötietojen tietoturvaloukkauksesta. Ministeriö on kuvannut ilmoituksessaan, että suomalaisten diplomaattien puhelimiin asennettu vakoiluhaittaohjelma on voitu asentaa ilman puhelimen omistajan suostumusta, ja sen avulla on voitu hyväksikäyttää hyvin laajasti puhelimessa olevia tietoja ja sen ominaisuuksia. Ministeriö on kertonut ilmoituksessa, että tapausta on selvitetty eri viranomaisten ja sidosryhmien kanssa syksyn 2021 ja talven 2022 aikana. Tietosuojavaltuutettu on vastaanottanut 16.3.2022 Ulkoministeriöltä selvityksen yleisen tietosuoja-asetuksen 33 ja 34 artikloissa tarkoitettujen ilmoitusten jättämisen ajankohdista.

Apulaistietosuojavaltuutettu on antanut päätöksen 23.3.2022, jossa se katsoo, ettei Ulkoministeriö ole rekisterinpitäjänä noudattanut yleisessä tietosuoja-asetuksen 33 artiklan 1 kohdassa määriteltyä valvontaviranomaiselle tehtävän ilmoituksen 72 tunnin aikarajaa. Ulkoministeriö ei ole myöskään toimittanut perusteltua selvitystä syystä, jonka vuoksi henkilötietojen tietoturvaloukkauksesta viranomaiselle toimitettava ilmoitus oli ollut myöhässä. Rekisterinpitäjänä toimineen Ulkoministeriön katsottiin lisäksi laiminlyöneen yleisen tietosuoja-asetuksen 34 artiklan 1 kohtaa, jonka mukaan rekisteröidylle tulisi ilmoittaa tietoturvaloukkauksesta ilman aiheetonta viivytystä.

[125] KHO: 2024:115.

Hallinto-oikeus katsoi tapauksessa, että yleisen tietosuoja-asetuksen 33 ja 34 artikloja sovellettiin myös kansalliseen ulko- ja turvallisuuspolitiikkaan sekä kansalliseen turvallisuuteen liittyvien henkilötietojen käsittelyyn, sillä tätä ei ollut Suomen kansallisessa sääntelyssä jätetty asetuksen soveltamisalan ulkopuolelle. Kuten yleisen tietosuoja-asetuksen 34 artiklan 1 kohdassa on säädetty, olisi rekisterinpitäjänä toimineen Ulkoministeriön pitänyt ilmoittaa sattuneesta loukkauksesta myös rekisteröidyille, sillä tapauksessa katsottiin kohdistuneen korkea riski henkilöiden oikeuksille ja vapauksille. Ulkoministeriö on kertonut myöhemmin tapauksen suullisessa käsittelyssä antaneensa henkilökohtaisesti tiedoksi verkkovakoilun kohteeksi joutuneille henkilöille sekä heidän lähipiirilleen ja edustustossa työskenteleville. Kuitenkaan henkilöille, joiden henkilötietoihin on voitu vakoiluhaittaohjelmalla päästä käsiksi mobiililaitteen tietosisällöissä, ei ole Ulkoministeriön toimesta ilmoitettu sattuneesta tietoturvaloukkauksesta, vaan tapahtuneesta on vain julkaistu tiedote ministeriön verkkosivustolla.

Apulaistietosuojavaltuutettu katsoo, ettei Ulkoministeriö ole toiminnassaan noudattanut velvollisuutta ilmoittaa rekisteröidyille tapahtuneesta ilman aiheetonta viivytystä, sillä ministeriön antaman lisäselvityksen perusteella tietoturvaloukkaus on sattunut jo vuoden 2021 aikana. Tapahtuneessa on siis kulunut loukkauksen havaitsemisen ja siitä rekisteröidyille ilmoittamisen välillä liian pitkä aika ottaen huomioon loukkauksen taustalla olevan haittaohjelman luonteen sekä rekisteröityjen aseman toimiessaan ulkomailla Ulkoministeriön virkamiehenä. Hallinto-oikeuden näkemyksen mukaan Ulkoministeriö on tapauksessa riittävän varmuuden loukkauksesta saatuaan ilmoittanut tapahtuneesta yleisen tietosuoja-asetuksen 34 artiklan 1 kohdan mukaisesti henkilöille, joiden laitteisiin kyseinen vakoilu oli kohdistunut.

Varsinainen yleisen tietosuoja-asetuksen ilmoitusvelvollisuuden laiminlyönti on tapahtunut, kun Ulkoministeriö on jättänyt ilmoittamatta ilman aiheetonta viivytystä tapahtuneesta loukkauksesta kaikille niille henkilöille, joiden henkilötietoihin verkkovakoiluhaittaohjelman avulla on ollut mahdollista päästä käsiksi mobiililaitteiden ominaisuuksia ja tietosisältöjä hyödyntäen. Myöskään yleisen tietosuoja-asetuksen 33 artiklan 1 kohdassa

määritelty valvovalle viranomaiselle 72 tunnin kuluessa ilmoittaminen ei ole toteutunut, eikä Ulkoministeriö ole antanut selitystä, jonka perusteella samaisen artiklan mahdollistama vaiheittainen ilmoittaminen ei olisi voinut tulla tapauksessa kysymykseen. Näiden edellä mainittujen laiminlyöntien ja rikkomusten perusteella hallinto-oikeus on antanut myönnytyksen apulaistietosuojavaltuutetun Ulkoministeriölle antamalle asetuksen 58 artiklan 2 kohdan b alakohdan mukaiselle huomautukselle.

Ulkoministeriö ei ollut tyytyväinen hallinto-oikeuden ratkaisuun, haki valituslupaa korkeimmasta hallinto-oikeudesta ja vaati hallinto-oikeuden ratkaisun ja apulaistietosuojavaltuutetun huomautuksen kumoamista. Ulkoministeriö katsoi, ettei ulko- ja turvallisuuspolitiikkaan voitu suoraan soveltaa yleisen tietosuoja-asetuksen 33 ja 34 artikloja, jolloin niissä säädetyt ilmoitusvelvollisuudet eivät olisi tässä tapauksessa olleet sovellettavissa. Ulkoministeriön perusteluiden mukaan tapauksessa muun muassa julkisuuslain tietyt kohdat ovat sellaista erityislainsäädäntö, jotka saavat etusijan suhteessa yleislaiksi luettavan tietosuojalain säännöksiin. Ulkoministeriö kokee, että yleisen tietosuoja-asetuksen 34 artiklan tarkoittama rekisteröidylle ilmoittaminen on toteutunut, sillä loukkauksen välittömänä kohteena oleville tapaus on saatettu tietoon heti ministeriön saatua asia tietoonsa.

Tapauksessa on katsottu olevan myös keskeistä löytää määritelmä varsin avoimelle ja tilannekohtaista tulkintaa sallivalle yleisen tietosuoja-asetuksen 34 artiklassa mainitulle ”ilman aiheetonta viivytystä”-aikamääreelle. On otettava huomioon Ulkoministeriö julkissektorilla toimivana ulko- ja turvallisuuspoliittisena elimenä, jonka toiminnassa julkiset tiedottamiset voivat vaarantaa Suomen ulko- ja turvallisuuspoliittisen tilan suhteessa vihamielisiin valtioihin, jotka voivat hyötyä liian aikaisessa vaiheessa julkisesta tiedottamisesta vakoiluyrityksiä koskien.

Korkeimman hallinto-oikeuden ratkaistavana oli siis lopulta kysymys, oliko Ulkoministeriö rekisterinpitäjänä noudattanut yleisen tietosuoja-asetuksen 33 ja 34 artikloissa säädettyjä aikarajoja ilmoittaessaan viranomaiselle ja rekisteröidyille vakoiluhaittaohjelman

avulla toteutetun verkkovakoilun aiheuttamasta henkilötietojen tietoturvaloukkauksesta. Asiassa oli otettava aluksi kantaa siihen, onko tapauksessa sovellettava mainittuja artikloja kuten unionin oikeutta tavallisesti vai sovelletaanko niitä kansallisen lainsäädännön tapaan. Korkein hallinto-oikeus katsoi, että Ulkoministeriön tapauksessa artikloja sovellettavan kansallisen lainsäädännön tapaan, joka merkitsisi, että julkisuuslain pykälät saavat etusijan suhteessa tietosuojalain soveltamiseen, ja tällä olisi merkittävä vaikutus tietosuoja-asetuksen määrittämän ilmoitusvelvollisuuden soveltamisen kannalta. Kansallisessa lainsäädännössä on laajennettu yleisen tietosuoja-asetuksen artiklojen soveltamista myös ulko- ja turvallisuuspolitiikkaan liittyvään henkilötietojen käsittelyyn, vaikka asetus ei sellaista laajennusta edellytä tehtävän. Siksi käsillä olevassa tapauksessa olisi tullut soveltaa yleisen tietosuoja-asetuksen 33 ja 34 pykäliä myös Ulkoministeriön toiminnassa. Ulkoministeriön jättämä ilmoitus henkilötietojen tietoturvaloukkauksesta katsotaan viivästyneen merkittävästi, eikä viivästykselle ole asiassa löydetty aiheellista perustetta. Tapauksessa on kuitenkin otettu huomioon julkisuuslain salassapitosäännökset, joita voidaan pitää erityissäännöksinä suhteessa tietosuoja-asetuksen 33 artiklan ilmoitusvelvollisuuteen viranomaiselle sekä 34 artiklan vaatimaan rekisteröidyille ilmoittamisvelvollisuuteen, ja jotka vaikuttivat ilmoituksen antamisajankohtaa. Tästä syystä korkein hallinto-oikeus katsoi, että Ulkoministeriö on antanut tapahtuneen tietoturvaloukkauksen rekisteröidyille tiedoksi ilman aiheetonta viivytystä, vaikka antoikin tiedoksiannon vasta huomattavasti tapauksen ilmitulon jälkeen.

Toinen tapaus koskien ilmoitusvelvollisuutta ja sitä, oliko tietosuojavaltuutettu oikeutettu antamaan rekisterinpitäjälle määräyksen ilmoittaa tapahtuneesta henkilötietojen suojan tietoturvaloukkauksesta rekisteröidyille. Korkeimman hallinto-oikeuden 23.11.2022 antamassaan ratkaisussa asianajotoimiston palveluksessa toimineen henkilön sähköpostitunnukset olivat päätyneet ulkopuolisen tahon haltuun kalastelusähköpostiviestin kautta. Tunnusten kautta ulkopuolisella taholla oli ollut noin kahden vuorokauden ajan pääsy arviolta 2000–2500 henkilön nimiin ja sähköpostiosoitetietoihin, 250–500 yksityishenkilön osoitetietoihin sekä 100–200 henkilön henkilötunnuksiin. Tapauksessa oli tietosuojavaltuutetun mukaan voitu varmistua, että hyökkääjällä oli ollut

pääsy tietoihin ja kaapattua sähköpostiosoitetta oli käytetty useissa operaatioissa, sillä sähköposti oli avautuessaan synkronoitunut hyökkääjälle. Tapauksessa ei voitu kuitenkaan täysin varmistua siitä, kuinka laajasti hyökkääjä oli käsillä olevia tietoja käyttänyt, mutta se oli varmaa, että tällä oli pääsy suureen joukkoon henkilötietoja, jotka olivat tunnistettavissa ja liitettävissä suoraan luonnollisiin henkilöihin. Lisäksi osa näistä tiedoista liittyi asianajotoimiston käsittelyssä oleviin luottamuksellisiin toimeksiantoihin.[126]

Asianajotoimisto oli tehnyt tietosuojavaltuutetun toimistolle ilmoituksen sattuneesta tietoturvaloukkauksesta, ja tietosuojavaltuutettu oli määrännyt rekisterinpitäjänä toimineen asianajotoimiston ilmoittamaan ilman aiheetonta viivytystä sattuneesta loukkauksesta rekisteröidyille, sillä loukkauksen katsottiin aiheuttavan todennäköisen korkean riskin rekisteröidyille. Rekisteröidyille oli katsottu aiheutuvan loukkauksesta merkittävä riski, sillä hyökkääjällä oli ollut pääsy yksityishenkilöiden henkilötunnuksiin ja joissain tapauksissa myös nimitietoihin, joiden samanaikaisesti käsiin saaminen mahdollistaa identiteettivarkauden toteuttamisen. Hyökkääjän saamat tiedot olivat asianajotoimiston mukaan luottamuksellisia eikä kaikki niihin liittyvä ollut julkisesti saatavilla olevaa tietoa. Siksi tietosuojavaltuutettu katsoi, että rekisterinpitäjällä oli ollut velvollisuus ilmoittaa tapahtuneesta mahdollisimman pian ainakin niille rekisteröidyille, joiden sekä henkilötietoihin että nimitietoihin hyökkääjällä oli ollut pääsy. Tietosuojavastaava ei kuitenkaan ollut antamassaan päätöksessä eritellyt, kenelle kaikille rekisteröidyille rekisterinpitäjän tulisi loukkauksesta ilmoittaa. Rekisterinpitäjänä toiminut asianajotoimisto oli valittanut tietosuojavaltuutetun antamasta päätöksestä, koska katsoi, ettei tietosuojavaltuutettu voinut määrätä rekisterinpitäjää ilmoittamaan rekisteröidyille tapahtuneesta henkilötietojen tietoturvaloukkauksesta.

Asian käsittelyssä arvioitiin loukkauksen vakavuutta ja sen aiheuttamaa riskiä erityisesti loukkauksen kohteeksi joutuneiden rekisteröityjen näkökulmasta. Hallinto-oikeus totesi, että hyökkäyksen toteuttanut osapuoli oli ollut pahantahtoinen ulkopuolinen taho eikä tapauksessa voitu varmistua mihin loukkauksessa vuotaneet tiedot olivat päätyneet.

---

[126] KHO: 2022:131.

Edellä mainittujen tietojen perusteella rekisteröityjen oikeuksiin ja vapauksiin kohdistuvaa riskiä, jonka tietoturvaloukkaus aiheutti, voitiin pitää korkeimman hallinto-oikeuden näkemyksen mukaan todennäköisenä sekä vakavana. Tuomioistuin katsoi, että erityisesti tapaukset, joissa hyökkääjällä oli pääsy identiteettivarkauden mahdollistaviin henkilötietoihin sekä tunnistettavissa oleviin luonnolliseen henkilöön liittyviin luottamuksellisiin tietoihin, voitiin katsoa aiheutuneen yleisen tietosuoja-asetuksen 34 artiklan 1 kohdan tarkoittama luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva todennäköinen korkea riski. Asiassa saadun selvityksen perusteella rekisteröidyille olisi pitänyt ilmoittaa henkilökohtaisesti yleisen tietosuoja-asetuksen 34 artiklan tarkoittamalla ilmoituksella sattuneesta henkilötietojen tietoturvaloukkauksesta, sillä mikään samaisen artiklan 3 kohdassa mainituista ilmoittamatta jättämistä perustelevista kohdista ei täyttynyt. Korkein hallinto-oikeus tuli ratkaisussaan tulokseen, että tietosuojavaltuutettu oli voinut yleisen tietosuoja-asetuksen 58 artiklan 2 kohdan e alakohdan nojalla antaa asianajotoimistolle määräyksen ilmoittaa sattuneesta tietoturvaloukkauksesta ilman aiheetonta viivytystä rekisteröidyille.

Ilmoittamisvelvollisuus ei siis aina ole rekisterinpitäjälle kovin yksiselitteinen ja helposti tulkittavissa. Rekisterinpitäjän oikeusturvan ja mahdollisimman lainmukaisen toimintatavan kannalta paras ratkaisu olisi siis aina ilmoittaa tietosuojavaltuutetulle sattuneista loukkauksista ja toimia viranomaisten antamien ohjeiden mukaan. Tietosuojavaltuutetulta voi kuitenkin aina pyytää myös tulkinta-apua ja toimintaohjeita, jos ei ole varma, miten tulisi lain näkökulmasta toimia oikein. Riskiperusteista lähestymistapaa mukaillen, parempi ilmoittaa pienellä kynnyksellä mahdollisista loukkausepäilyistä kuin jättää kokonaan ilmoittamatta.

Nykyään useat yritykset ovat ulkoistaneet henkilötietojen käsittelyn ulkopuoliselle käsittelijälle tai jopa useammalle, jolloin vastuun jakaminen tai tulkinta voi olla varsin haastavaa toimijoiden kesken, varsinkin mahdollisen tietosuojaloukkauksen sattuessa[127]. Kun

[127] Lindroos-Hovinheimo 2018, s.757.

yritys on ulkoistanut henkilötietojen käsittelyn ulkopuoliselle taholle, kutsutaan tätä ulkopuolista tahoa yleisen tietosuoja-asetuksen 4 artiklan mukaan henkilötietojen käsittelijäksi, joka toimii rekisterinpitäjän lukuun. Rekisterinpitäjä on siis henkilötietojen käsittelystä määräävänä tahona vastuussa tietosuojan toteutumisesta ja muista henkilötietojen käsittelyä koskevien periaatteiden noudattamisesta, vaikkakin varsinaisen käsittelyn olisi ulkoistanut[128]. Henkilötietojen käsittelijästä voi kuitenkin tulla myös rekisterinpitäjä, mikäli käsittelijä toteuttaa keruuta, jonka on itse määritellyt, eikä toteuta enää rekisterinpitäjän toimeksiantoa[129]. Tämän kaltaisissa tilanteissa rajanveto vastuukysymyksissä voi olla varsin haastavaa, mikäli ei olla aivan perillä, kuka toimii tilanteessa rekisterinpitäjänä ja kuka käsittelijänä. Yleisen tietosuoja-asetuksen 33 artiklan 2 kohdassa henkilötietojen käsittelijä velvoitetaan ilmoittamaan ilmenneestä henkilötietojen tietoturvaloukkauksesta ilman aiheetonta viivytystä rekisterinpitäjälle.

Rekisterinpitäjän ja tietojen käsittelijän roolin ristiriitatilanteeseen liittyen Euroopan unionin tuomioistuin on antanut tuomion[130] ennakkoratkaisupyynnöstä, jossa saksalainen tietosuojaviranomainen oli antanut saksalaiselle Facebookin fanisivun kautta koulutusalan palveluita tarjoavalle yritykselle määräyksen poistaa kyseinen fanisivu. Tietosuojaviranomainen katsoi, ettei fanisivun käyttäjille ollut yrityksen eikä Facebookin toimesta ilmoitettu henkilötietojen keräämisestä ja käsittelystä evästeiden avulla. Yritys ei kuitenkaan katsonut olevansa vastuussa Facebookin toteuttamasta tietojenkäsittelystä tai sen asettamista evästeistä, jonka vuoksi yritys teki tietosuojaviranomaisen päätöksestä oikaisuvaatimuksen. Tietosuojaviranomainen hylkäsi oikaisuvaatimuksen, koska katsoi yrityksen hyötyvän Facebookin suorittamasta tietojen käsittelystä, sillä Facebook oli toimittanut yrityksen käyttöön tilastotietoja. Yritys nosti asiasta kanteen kansallisessa hallintotuomioistuimessa, sillä katsoi ettei ole vastuussa Facebookin suorittamasta tietojenkäsittelystä, koska ei ole antanut kyseistä toimeksiantoa Facebookin tehtäväksi, ja tietosuo-

[128] Lindroos-Hovinheimo 2018, s.757–758.
[129] Lindroos-Hovinheimo 2018, s.758.
[130] C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388.

javiranomaisen olisi pitänyt yrityksen mukaan toteuttaa toimenpiteet suoraan Facebookia kohtaan. Hallintotuomioistuin sekä ylempi hallintotuomioistuin totesivat yksimielisesti, ettei fanisivujen hallinnoija toimi tietojenkäsittelystä vastaavana elimenä. Tapauksessa Facebook päättää käytettävien ja kerättävien henkilötietojen käsittelyn tarkoituksen sekä keinot, ja fanisivun ylläpitäjälle päätyy pelkästään anonymisoituja tilastotietoja.

Tietosuojaviranomainen vei asian kuitenkin vielä eteenpäin Saksan liittovaltion ylimpään hallintotuomioistuimeen Bundesverwaltungsgerichtiin, sillä katsoi, että fanisivun ylläpitäjä oli perustanut koulutuspalvelunsa sille sopimattomalle alustalle ja soveltumattoman palveluntarjoajan hoidettavaksi. Tietosuojaviranomaisen mukaan palveluntarjoajana toimiva Facebook Ireland ei noudattanut tietosuojalainsäädäntöä toiminnassaan. Bundesverwaltungsgericht oli samaa mieltä hallintotuomioistuinten kanssa siitä, ettei yritystä voitu pitää rekisterinpitäjänä. Tapauksessa pohdittiin lisäksi, oliko tietosuojaviranomainen toimivaltainen puuttumaan Facebook Irelandin toimintaan, sillä kyseessä oli saksalainen tietosuojaviranomainen. Tämä pohdinta johti ennakkoratkaisukysymyksiin liittyen eurooppalaisten tietosuojaviranomaisten välisiin suhteisiin ja niiden määrittelyyn sekä rekisterinpitäjän toimeen ja muiden toimijoiden välisestä vastuunjaosta[131].

Julkisasiamiehen näkemyksen mukaan tapauksessa tuli selvittää, kuka toimi rekisterinpitäjänä ja voitiinko yritystä pitää sellaisena. Julkisasiamies katsoi aiempiin EUT:n julkaisuihin ja tietosuojatyöryhmien kannanottoihin nojaten, että fanisivua hallinnoimaa yritystä voitiin pitää yhteisvastuullisena rekisterinpitäjänä, sillä rekisterinpitäjänä pidetään ensisijaisesti sellaista tahoa, joka määrittelee henkilötietojen käsittelyn keinot ja tarkoituksen. Olennaista on, että koko henkilötietojen käsittelyä ei tapahtuisi, jos koko fanisivustoa ei olisi olemassa. Julkisasiamies muistuttaa, ettei Facebookin ja fanisivun hallinnoijan välisellä sopimuksella ole merkitystä rekisterinpitäjän roolin tulkinnassa oikeudellisesti. Tapauksessa on siis sovellettu rekisterinpitäjän käsitteen hyvin laajaa tulkintaa, sillä sen avulla pyritään välttämään väärinkäytösten tapahtuminen.[132]

---

[131] Lindroos-Hovinheimo 2018, s.760.
[132] Lindroos-Hovinheimo 2018, s.760–762.

4 Sanktioiden ja valvonnan merkitys

4.1 Valvonta ja hallinnolliset sanktiot

Yleisen tietosuoja-asetuksen sekä NIS2-direktiivin mukaisten vaatimusten laiminlyönnistä ja rikkeistä on säädetty seuraavan toimijalle määrättäviä hallinnollisia seuraamusmaksuja, jotta tietoturvallisuuden taso säilyisi. NIS2-direktiivin 34 artiklassa on vähimmäisvaatimukset hallinnollisista sakoista, jotka seuraavat direktiivin 21 artiklan mukaisen riskienhallintavelvoitteen ja 23 artiklan mukaisen raportointivelvoitteen laiminlyönnistä. Samaisessa artiklassa on myös määrätty vähimmäisvaatimus kansallisesti määrättäville hallinnollisille sakoille ja niiden enimmäismäärälle. Keskeiselle toimijalle kohdistuvan hallinnollisen sakon suuruuden määrittämiseen on kaksi tapaa; sakko voi olla enimmäismäärältään ”*vähintään 10 000 000 euroa tai 2 prosenttia sen yrityksen, johon keskeinen toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta.*” Sakon suuruuden laskutapa määräytyy sen mukaan, kumpi näillä kahdella tavalla määritettävistä summista on suurempi. Myös tärkeään toimijaan kohdistuvan sakon suuruuteen on kaksi määritystapaa ja niin ikään sakon määrä määräytyy sen perusteella, kumpi määristä on suurempi. Tärkeän toimijan hallinnollisen sakon enimmäismäärä on hallituksen esityksen mukaan ”*vähintään 7 000 000 euroa tai 1,4 prosenttia sen yrityksen, johon tärkeä toimija kuuluu, edellisen tilikauden maailmanlaajuisesta vuotuisesta kokonaisliikevaihdosta*”. [133] NIS2-direktiivin 34 artiklan 7 kohta antaa jäsenvaltioille mahdollisuuden säätää siitä, voiko julkishallinnon toimijalle määrätä hallinnollista sakkoa, ja jos voi, millä perusteilla ja kuinka suurista sakoista olisi kyse.

Tietosuojan toteutumisen turvaksi tietosuoja-asetuksessa on säädetty myös seuraamuksista, joita mahdollisista rikkeistä seuraa. Tietosuoja-asetuksen 83 artiklassa säädetään yleiset edellytykset hallinnollisten seuraamusmaksujen määräämiselle. Hallinnollisen

[133] HE 57/2024 vp., s.20.

seuraamusmaksun on tarkoitus olla tehokas, oikeasuhtainen ja varoittava yleisen tietosuoja-asetuksen 83 artiklan 1 kohdan mukaan. Sen on tarkoitus olla saman aikaisesti riittävän suuri pelote ja kannustin noudattaa tietosuojalainsäädäntöä, sillä todennäköisesti toimija pääsee halvemmalla noudattaessaan lakia kuin joutuessaan maksamaan rikkomuksistaan[134]. Hallinnollisen sakon suuruuteen vaikuttaa yleisen tietosuoja-asetuksen 83 artiklan 2 kohdan mukaan muun muassa rikkomuksen luonne, vakavuus ja kesto, tietojen käsittelyn luonne, laajuus ja tarkoitus, loukkauksen kohteeksi joutuneiden rekisteröityjen määrä ja heille aiheutuneen vahingon suuruus. Rikkomuksen tahallisuus tai tuottamuksellisuus ja rekisteröidylle koituneiden vahinkojen lieventämiseksi toteutetut toimenpiteet voivat vaikuttaa rekisterinpitäjään tai henkilötietojen käsittelijään kohdistuvan seuraamusmaksun suuruuteen. Myös muun muassa sillä on merkitystä, onko rekisterinpitäjä tai henkilötietojen käsittelijä aiemmin syyllistynyt vastaaviin rikkomuksiin.

Tietosuoja-asetuksessa on määritetty kaksi enimmäismäärää, jonka hallinnollinen seuraamusmaksu voi olla. Nämä enimmäismäärät ovat 10 ja 20 miljoonaa euroa. Sakon määrä voi määrittyä myös yrityksen liikevaihdon perusteella, jolloin sakko on 2 tai 4 prosenttia globaalista liikevaihdosta. Kaksi erisuuruista hallinnollisen sakon enimmäismäärää kertoo siitä, että joidenkin rikkomusten katsotaan olevan vakavampia kuin toisten. Sitä ei kuitenkaan ole määritelty, minkä rikkomusten hinta on 10 miljoonaa ja minkä 20 miljoonaa, vaan jokainen rikkomus tulkitaan tapauskohtaisesti.[135]

Tietoturvaloukkauksesta hallinnollisen seuraamusmaksun määrää tietosuojalain 24 pykälän mukaisesti tietosuojavaltuutetun ja apulaistietosuojavaltuutettujen muodostama seuraamuskollegio. Vireillä oleva asia esitellään kollegiolle ja enemmistön äänestämä kanta muodostuu päätökseksi. Mikäli äänet menevät äänestyksessä tasan, tuloksena se kanta, joka on lievempi osapuolelle, jolle seuraamus kohdistuu. Seuraamuskollegion toteuttamassa seuraamusmaksumenettelyssä on runsaasti huomioon otettavaa sattuneen rikkomuksen moitittavuutta harkitessa sekä maksun suuruutta määrittäessä, sillä yleisen

[134] EOAK/6681/2024, s.2.
[135] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.636–637.

tietosuoja-asetuksen 83 artiklan 2 kohta tarjoaa runsaasti seikkoja, jotka kyseiseen harkintaan vaikuttavat. Seuraamusmaksua ei voida määrätä, jos rikkomuksesta tai laiminlyönnistä on kulunut yli kymmenen vuotta. Tietosuojalain mukaan seuraamusmaksua ei voida määrätä valtion viranomaisille, valtion liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle eikä Suomen evankelisluterilaiselle kirkolle ja Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille ja muille elimille.

On huomionarvoista, että NIS2-direktiivi jättää jokaisen jäsenvaltion kansallisen päätäntävallan vastuulle, voiko julkishallinnolliselle toimijalle määrätä hallinnollista seuraamusmaksua, kun taas kansallinen tietosuojalaki suoraan kieltää, että hallinnollista seuraamusmaksua ei voida julkiselle toimijalle määrätä. Yleisen tietosuoja-asetuksen 83 artiklan 7 kohta on mahdollistanut kansallisen liikkumavaran seuraamusmaksujen määräämiselle julkisille toimijoille, ja kansallisessa tietosuojalain 24§:n 4 momentissa on säädetty, ettei maksua voi kyseisille tahoille määrätä[136]. Tähän on kuitenkin tulossa Suomessa kansallisella tasolla muutos, sillä hallitus on ehdottanut lakimuutosta, joka mahdollistaisi myös viranomaisille ja julkishallinnollisille toimijoille hallinnollisten seuraamusmaksujen määräämisen tietosuojalainsäädäntöä koskevista rikkomuksista[137]. Lakiuudistuksen tarkoituksena on yhtenäistää tietosuojaloukkauksista määrättävien hallinnollisten sakkojen määräytymistä koskemaan yhtäläisesti julkista sekä yksityistä sektoria[138].

Hallinnollisia seuraamusmaksujen uudistusta koskevassa keskustelussa on ollut keskiössä erityisesti oikeushenkilöoppi, ja se miten kukin julkishallinnollinen toimija tai viranomainen tulisi määritellä[139]. Julkisoikeudellisen oikeushenkilön rangaistus- ja vahingon-

[136] EOAK/6681/2024, s.2.
[137] HE 46/2026 vp., s.1.
[138] HE 46/2026 vp., s.4.
[139] EOAK/6681/2024, s.3.

korvausvastuuseen liittyy merkittäviä rajoituksia, jotka estävät muun muassa hallinnollisten seuraamusmaksujen määräämisen julkisoikeudelliselle oikeushenkilölle[140]. Suomessa virastoja ja viranomaisia ei kuitenkaan katsota itsenäisiksi oikeushenkilöiksi, joka tarkoittaa, ettei viranomainen voisi tehdä omissa nimissään oikeustoimia tai olla oikeuksien ja velvollisuuksien subjektina[141]. Käytännössä tämä tarkoittaa siis sitä, että virastot ja viranomaiset katsotaan osaksi valtiota, jolloin hallinnollisen seuraamusmaksun määrääminen tarkoittaisi käytännön tasolla vain varojen siirrosta valtion sisällä, ja sitä, että valtio määräisi rangaistuksia itselleen[142].

Keskustelussa hallinnollisten seuraamusmaksujen uudistuksesta keskeisenä ongelmana on oikeusasiamiehen lausunnon mukaan se, että käytännössä veronmaksajat joutuisivat maksajiksi julkishallintoon kohdistuvien seuraamusmaksujen kohdalla. Seuraamusmaksuihin käytettävät varat olisivat pois viranomaisen lakisääteisen tehtävän hoidosta, joka tarkoittaisi väistämättä esimerkiksi kuntatasolla veronkorotusten tarvetta tai palveluiden heikentämistä. Oikeusasiamies ehdottaa sen sijaan, että julkishallinnollisiin toimijoihin kohdistettaisiin hallinnollisia seuraamusmaksuja, että virkarikosoikeudelliseen vastuuseen tehtäisiin muutoksia ja parannuksia. Virkarikosoikeudelliseen vastuuseen tehtävillä muutoksilla voitaisiin tehostaa tietosuojalainsäädännön rikkomiseen liittyvää sanktiouhkaa sekä selkeyttää luonnollisten henkilöiden vastuuasemaa rekisterinpitäjän ja henkilötietojen käsittelijän tehtävissä. Käytännössä tämä tarkoittaisi, että organisaatioissa tulisi selkeästi määritellä, kuka toimii rekisterinpitäjänä ja kuka henkilötietojen käsittelijänä, jotta näitä toimijoita koskevat velvollisuudet ja vastuut voitaisiin rikosoikeudellisesta näkökulmastakin kohdentaa oikein.[143]

Uudistusta on perusteltu kuitenkin tarpeena yhtenäistää julkisen ja yksityisen sektorin seuraamusmenettelyä, sillä vaikka julkishallinnon henkilötietojen käsittelyn oikeuspe-

[140] Mäenpää 2023, s.226–227.
[141] EOAK/6681/2024, s.4. Myös Mäenpää 2023, s.230.
[142] EOAK/6681/2024, s.6.
[143] EOAK/6681/2024, s.6.

rusteet ovat rajallisempia kuin yksityissektorilla, toteutetaan käsittelyä silti julkissektorilla hyvin samankaltaisesti kuin yksityissektorilla. Lisäksi yleisessä tietosuoja-asetuksessa julkista sektoria ja yksityissektoria koskevat lähes samansisältöiset velvoitteet henkilötietojen käsittelijöinä. Julkisen sektorin ja yksityisen sektorin erilaisen aseman rekisterinpitäjän vastuusta suhteessa organisaatioon pelätään heikentävän merkittävästi rekisteröityjen luottamusta, varsinkin jos ilmenee, että julkissektorilla on tapahtunut tietosuojalainsäädännön rikkomuksia.[144]

Oikeusministeriön toteuttaman selvityksen perusteella julkissektorilla on tapahtunut yksityissektoriin verrattuna tietosuojalainsäädännön laiminlyöntejä melko usein, vaikka julkishallinnon rekisterinpitäjiä ja henkilötietojen käsittelijöitä on lukumäärällisesti vähemmän verrattuna yksityiseen sektoriin. Tietosuojavaltuutetun mukaan viranomaisille kohdistetuissa korjaavissa toimenpiteissä on selkeästi määrällisesti eniten annettu huomautuksia, vaikka kynnys sen määräämiseen on tietosuojavaltuutetun mukaan varsin korkea, kun kyseessä on viranomainen. Huomautukset ovat koskeneet muun muassa henkilötietojen tietoturvaloukkauksia koskevissa asioissa ja rekisteröidyn oikeuksien toteuttamiseen liittyvissä asioissa.[145] Näiden perustelujen perusteella voisi siis ajatella, että julkisyhteisöihin haluttaisiin kohdistaa jonkinlainen pelote, jotta tietosuojalainsäädäntöä noudatettaisiin tarkemmin ja paremmin, ja jotta tietoturvaloukkauksilta voitaisiin välttyä. Hallituksen esityksen sekä oikeusasiamiehen kommenttien perusteella jotakin muutoksia julkishallintoa koskeviin seuraamuksiin pitäisi tehdä, mutta hallinnollisen seuraamusmaksu ei välttämättä ole se kaikista paras ratkaisu ihan jo valtion talouden näkökulmasta.

[144] HE 46/2026 vp., s.5–6.
[145] HE 46/2026 vp., s.7.

4.2 Valvontaviranomaisten rooli ja toimivaltuudet

Yleisessä tietosuoja-asetuksessa ja NIS2-direktiivissä on määritelty omat valvontaviranomaiset, jotka valvovat asetuksen ja direktiivin sisällön soveltamista käytännössä. Yleisen tietosuoja-asetuksen 51 artiklassa säädetään, että jokaisessa jäsenvaltiossa on oltava yksi tai useampi riippumaton viranomainen, jonka vastuulla on valvoa kyseisen asetuksen soveltamista, jotta luonnollisten henkilöiden perusoikeudet sekä -vapaudet toteutuvat henkilötietojen käsittelyssä ja, jotta henkilötietojen vapaa liikkuvuus voidaan turvata unionissa[146]. Valvovia viranomaisia voi siis olla enemmän kuin yksi valtion toimesta nimettynä, mutta tällöin pitää valita, kuka viranomaisista edustaa jäsenvaltion viranomaisia Euroopan tietosuojaneuvostossa eli unionin jäsenvaltioiden viranomaisten yhteistyössä. Yleinen tietosuoja-asetus edellyttää, että valvovana viranomaisena toimivan on oltava täysin itsenäinen ja riippumaton toiminnassaan[147]. Kansallisessa tietosuojalaissa (1050/2018) on määritelty 8 pykälässä, että Suomessa yleisen tietosuoja-asetuksen mukaisena valvontaviranomaisena toimii Oikeusministeriön yhteydessä toimiva tietosuojavaltuutettu. Tietosuojavaltuutetun virkaan voidaan nimittää enintään viideksi vuodeksi kerrallaan[148]. Tietosuojalain 9 pykälässä on määritelty, että tietosuojavaltuutetun toimistolla työskentelee vähintään kaksi apulaistietosuojavaltuutettua sekä riittävästi tietosuojavaltuutetun tehtävänalaan perehtynyttä henkilöstöä.

Tietosuojavaltuutetun ensisijainen tehtävä on valvoa asetuksen soveltamista sekä myötävaikuttaa osaltaan asetuksen mahdollisimman yhdenmukaiseen soveltamiseen unionissa. Tietosuojavaltuutetun toimistossa työskentelevän asiantuntijalautakunnan tehtävänä on tietosuojalain 17 pykälän mukaan antaa pyynnöstä lausuntoja koskien henkilötietojen käsittelyyn liittyvän lainsäädännön soveltamisesta ja siihen liittyvistä kysymyksistä. Tietosuojalain 14 pykälässä määriteltyjen tietosuojavaltuutetun tehtävien mukaan tietosuojavaltuutettu edustaa Suomea Euroopan tietosuojaneuvostossa.

---

[146] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.514.
[147] HE 9/2018 vp., s.8.
[148] HE 9/2018 vp., s.9.

Tietosuojalain 4 luvun 21 pykälän mukaisesti rekisteröity on oikeutettu saattamaan asian tietosuojavaltuutetun käsittelyyn, jos rekisteröity kokee häntä koskevien henkilötietojen käsittelyssä rikotun tietosuojalainsäädäntöä. Tietosuojavaltuutetun on käsiteltävä vireille tullut asia kolmen kuukauden kuluessa tai ilmoittaa rekisteröidylle arvioitu päätöksen antamisajankohta, mikäli asia ei ole käsiteltävissä kolmen kuukauden määräajassa.

Yleisen tietosuoja-asetuksen 31 artiklan mukaisesti rekisterinpitäjää ja henkilötietojen käsittelijää koskee velvoite tehdä pyynnöstä yhteistyötä valvontaviranomaisten kanssa, jotta lakisääteiset valvontatehtävät saadaan suoritettua. Myös mahdollisen henkilötietojen käsittelijän edustajan on tehtävä pyydettäessä yhteistyötä valvontaviranomaisen kanssa, mutta yhteistyön laiminlyönnistä ei kuitenkaan koidu edustajataholle seuraamuksia toisin kuin rekisterinpitäjälle tai henkilötietojen käsittelijälle voi koitua[149].

Yleinen tietosuoja-asetus on asetuksena suoraan kaikilta osiltaan oikeudellisesti velvoittava[150] ja NIS2-direktiivi antaa direktiivinä jäsenvaltioille raamit, mitä pitää toteuttaa ja jäsenvaltio saa itse kansallisessa lainsäädännössään päättää, miten käytännössä direktiivin vaatimukset toteutetaan[151]. Siksi NIS2-direktiivissä valvonnasta ei ole säädetty aivan yhtä suoraviivaisesti kuten yleisessä tietosuoja-asetuksessa. NIS2-direktiivin toimijoiden jaottelu keskeisiin ja tärkeisiin toimijoihin vaikuttaa myös toimijoiden valvontaan. Keskeisten ja tärkeiden toimijoiden eri valvontajärjestelmää perustellaan direktiivissä mahdollisuutena varmistaa, että toimijoiden sekä toimivaltaisten viranomaisten velvoitteet olisivat oikeudenmukaisesti tasapainossa. Koska keskeiset toimijat on velvoitettu toteuttamaan sekä etukäteis- että jälkikäteisvalvontaa, kohdistuu heihin kattavampi valvontajärjestelmä. Tärkeiden toimijoiden vastuulla on vain jälkikäteisvalvonta, jonka vuoksi heihin sovelletaan kevyempää valvontajärjestelmää.[152] Jälkikäteisvalvonta tarkoittaa käytännössä viranomaisen valtuuksien kannalta, ettei valvovilla viranomaisilla ole mahdollisuutta kohdistaa tärkeisiin toimijoihin valvontatoimenpiteitä yhtä laajasti kuin keskeisiin

[149] Korpisaari, Pitkänen, Warma-Lehtinen 2022, s.369.
[150] Aalto 2025, s.226.
[151] Aalto 2025, s.302.
[152] HE 57/2024 vp., s.19.

toimijoihin. Mikäli tärkeän toimijan toiminnasta saadaan näyttöä tai muita viitteitä siitä, ettei se noudata NIS2-direktiivin 21 artiklan mukaista riskienhallintavelvoitetta ja 23 artiklan mukaista raportointivelvoitetta, voi viranomainen kohdistaa tähän valvontatoimenpiteitään, mutta vain jälkikäteisesti.[153]

NIS2-velvoittaa, että valvovilla viranomaisilla on oltava valtuus suorittaa keskeisten toimijoiden osalta muun muassa erilaisia tarkastuksia, auditointeja sekä valvontatehtävien suorittamiseksi pyynnöstä oltava pääsy valvontatehtävissä tarvittavaan dataan, asiakirjoihin ja muihin tietoihin. Valvovan viranomaisen tulee olla valtuutettu antamaan toimijoille varoituksia, sitovia ohjeita sekä määräämään direktiivin vastaisen toiminnan lopettamisesta. Valvovan viranomaisen toimivaltuuksiin tulee myös kuulua mahdollisuus määrätä tai pyytää muun muassa tuomioistuimia määräämään hallinnollisia sakkoja.[154] Valvovalla viranomaisella tulee olla myös toimivaltaa keskeyttää väliaikaisesti keskeisen toimijan tarjoamia palveluita tilanteessa, jossa toimija ei kehotuksista huolimatta tai määräaikoja laiminlyöden korjaa puutteita, joita sen toiminnassa on havaittu. Myös toimijan sertifiointi tai muu toiminnan jatkumisen edellyttämä lupa voidaan evätä puutteiden korjaamisen laiminlyönnin takia valvovan viranomaisen toimesta. Näitä edellä mainittuja seuraamuksia ei kuitenkaan voida soveltaa julkishallinnon toimijoihin.[155]

Jokaisen jäsenvaltion tulee nimetä yksi tai useampi CSIRT-yksikkö NIS2-direktiivin 10 artiklan mukaisesti. CSIRT-yksikön tehtäviin 11 artiklan mukaan kuuluu reagoida kyberturvaloukkauksiin ja tutkia niitä, seurata ja analysoida kyberuhkia, haavoittuvuuksia sekä poikkeamia ja antaa niihin liittyviä ennakkovaroituksia, hälytyksiä ja muita ilmoituksia. Yksikkö kerää ja analysoi tietoa poikkeamista, joiden avulla se ylläpitää tilannekuvaa kyberturvallisuudesta. Lisäksi yksikkö osallistuu CSIRT-verkoston toimintaan. CSIRT-yksikkö vastaanottaa toimijoilta ilmoituksia merkittävistä poikkeamista toimivaltaisen viranomaisen ohella.[156]

---

[153] HE 57/2024 vp., s.20.
[154] HE 57/2024 vp., s.19.
[155] HE 57/2024 vp., s.20.
[156] HE 57/2024 vp., s.20.

4.3 Tietoturvallisuuden koulutus ja osaaminen organisaatioissa ja johdon vastuu

Julkishallinnon toimialaa koskevassa tiedonhallintalain (906/2019) 4 a luvun 18 c pykälässä on määritetty toimenpiteet, joiden avulla kyberturvallisuuden riskien hallintaa tulisi hoitaa. Kyseinen lainkohta määrää, että ”*Tiedonhallintayksikön on toteuttava oikeasuhtaiset tekniset, operatiiviset ja organisatoriset kyberturvallisuutta koskevat riskienhallintatoimenpiteet käyttämiensä viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien kyberriskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi*”. Lisäksi tiedonhallintalain 2 luvun 4 pykälän mukaisesti on johdon vastuulla huolehtia, että kyseisessä tiedonhallintayksikössä on määritelty tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut, on olemassa ajantasaiset ohjeet tietojen käsittelystä ja siihen liittyvien tietojärjestelmien käytöstä. Johdon vastuulla on huolehtia tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä varautua mahdollisiin poikkeusoloihin. Johdon velvollisuus on myös tarjota henkilöstölle koulutusta, jonka avulla varmistetaan kaikilla tiedonhallintayksikössä työskentelevien riittävä tietotaito ja osaaminen ajantasaisesta tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen salassapitoa ja julkisuutta koskevista säädöksistä, määräyksistä ja kyseisen tiedonhallintayksikön toimintaan vaikuttavista ohjeista.

Tietosuojalainsäädännössä rekisterinpitäjällä on keskeinen vastuu huolehtia, että rekisteröidyn henkilötietojen suoja on turvattu, ja että henkilötietojen käsittely tapahtuu lainmukaisin edellytyksin. Organisaatiossa vastuu tietoturvan toteutumisesta ja kyberturvallisuutta koskevien riskienhallintatoimenpiteiden toteuttamisesta on pääasiassa johdolla.[157] Yksi merkittävimmistä tietoturvatoimenpiteistä, jolla tietoturvallisuutta voidaan parantaa ja ylläpitää, onkin siis kouluttaa organisaatiossa henkilöstöä. Henkilöstöä tulisi tietosuojalain 6 pykälän mukaan kaikkia organisaatiota velvoittavana tietoturvatoimenpiteenä ohjeistaa, kouluttaa tietoturva- ja tietosuojakoulutuksin sekä testata henkilöstön

[157] Andersson 2024, s.266.

osaamista.[158] NIS2-direktiivin 20 artikla velvoittaa keskeisten ja tärkeiden toimijoiden hallintoelinten jäseniä kouluttautumaan kyberturvallisuutta koskevista riskienhallinnasta ja sen toimenpiteistä. Lisäksi on suositeltavaa, että hallintoelinten jäsenet järjestävät koulutusta myös työntekijöilleen [159].

Pahimmillaan organisaation tietoturvallisuus voi vaarantua, jos organisaation henkilöstöllä ei ole riittävää tuntemusta ja osaamista siitä, miten tietosuojalainsäädäntöä ja kyberturvallisuutta koskevaa lainsäädäntöä tulisi soveltaa, saati jos henkilöstö ei ole edes tietoinen kyseisten lakien sisällöstä. Mikäli johto laiminlyö henkilöstönsä koulutusta, voi organisaatio syyllistyä vakaviin tietoturvaa koskevaan laiminlyöntiin, joka voi pahimmillaan johtaa merkittäviin riskien realisoitumisiin ja sitä kautta aiheutua vakavaa haittaa paitsi organisaatiolle myös henkilöille ja tahoille, joiden tietoja kyseisessä organisaatiossa käsitellään. Riskin realisoitumisen lisäksi myös valvova viranomainen on varmasti kiinnostunut mahdollisista puutteista kyberturvallisuuden toteuttamisessa, jolloin vakavammista rikkeistä organisaation toimintaa voidaan rajoittaa määräajaksi tai pahimmillaan organisaation maksettavaksi voi koitua mittavat hallinnolliset seuraamusmaksut. Mikäli kävisi ilmi, ettei organisaatiossa ole huolehdittu riskiperusteisen lähestymistavan mukaisesti siitä, että organisaation käytössä on riittävät ja ajantasaiset kyberturvallisuuden riskienhallinnan toimenpiteet, olisi vastuu sattuneesta tietoturvaloukkauksesta organisaation johdolla[160].

Organisaation tietoturvan kannalta on siis keskeistä, että huolehditaan työntekijöiden tietoturvaosaamisesta. Tietoturvaohjeistuksien antaminen, ylläpito sekä niiden jalkauttaminen käytännön tasolle koulutusten avulla kehittävät tietoturvaosaamista ja parantavat henkilöstön asennetta tietoturva-asioita kohtaan. Uuden työntekijän aloittaessa tietoturva-asioista kouluttamisen on oltava osana perehdytystä. Myös perehdytyksen jälkeen tulee huolehtia säännöllisestä osaamisen ylläpitämisestä ja kehittämisestä, jotta

[158] Andersson 2024, s.201–202.
[159] HE 57/2024 vp., s.15.
[160] Andersson 2024, s.267.

osaamisen taso säilyy. Lisäksi olisi hyvä testata henkilöstön osaamista käytännössä, jotta voidaan varmistua, että koulutukset ovat riittävän selkeitä ja täsmällisiä.[161] Osaamista ja poikkeamatilanteessa toimimista on hyvä myös harjoitella, jotta oikean tilanteen sattuessa henkilöstö osaa toimia, kuten pitää. Tietoturva- ja tietosuojaosaamisen vähimmäissääntely ei ole yksiselitteisesti saatavilla, vaan on hajaantunut usean eri säädöksen alaisuuteen. Siksi tietoturva- ja tietosuojakoulutusta ja osaamista koskevat vaatimukset voivat vaihdella siinä, mitä koulutuksissa painotetaan.[162]

Vastuukysymykset ovat tärkeitä tunnistaa, jotta henkilöstö tietää, mikä tehtävä kuuluu kenellekin. Päävastuu tietoturvallisuustoimenpiteistä ja niiden toteuttamisesta onkin siis organisaation johdolla, mutta jokaisen työntekijän vastuulla on myös työtehtäviään hoitaessa huolehtia, että tietoturvallisuus säilyy. On johdon vastuulla huolehtia, että jokainen työntekijä todella tietää vastuunsa ja osaa ottaa sen huomioon toiminnassaan. Selkeintä on, jos työntekijä ja työnantaja käyvät vastuut läpi jo heti työsopimuksessa, jolloin mahdollisten toistuvien rikkeiden sattuessa työnantajalla on myös mahdollisuus työsopimuksen sisältöön vedoten irtisanoa välinpitämättömästi tai huolimattomasti toimiva työntekijä ilman, että voitaisiin vedota tietämättömyyteen vastuustaan.[163]

[161] Andersson 2024, s.268.
[162] Andersson 2024, s.268.
[163] Andersson 2024, s.269.

5 Johtopäätökset

5.1 Keskeisimmät havainnot kyberturvallisuusvaatimusten täyttämisestä

Keskeisempänä havaintona kyberturvallisuusvaatimusten täyttämisestä nostaisin NIS2-direktiivin ja yleisen tietosuoja-asetuksen vaatimusten erilaisuudet. Molemmat säädökset velvoittavat ilmoittamaan havaitusta poikkeamasta tai loukkauksesta, mutta tahot, joille ilmoitus annetaan ovat eri ja myös ilmoitusvelvollisuutta koskevat aikamääreet ovat eri. NIS2-direktiivin mukaan kyberturvallisuuspoikkeamasta tulee ilmoittaa kolmivaiheisella prosessilla, jossa ensi-ilmoitus annetaan 24 tunnin kuluessa, jatkoilmoitus 72 tunnin kuluessa poikkeaman havaitsemisesta ja vielä loppuraportti kuukauden kuluttua ensi-ilmoituksen jättämisestä. Ilmoituskynnys täyttyy sellaisen poikkeaman kohdalla, joka aiheuttaa tai voi aiheuttaa huomattavaa aineellista tai aineetonta vahinkoa luonnollisille henkilöille vaikutuksillaan[164]. Ilmoitus tulee NIS2-direktiivin vaatimusten mukaan jättää CSIRT-yksikölle tai toimivaltaiselle valvovalle viranomaiselle, joka Suomessa on Liikenne- ja viestintävirasto Traficomin yhteydessä toimiva Kyberturvallisuuskeskus. Tietyissä tapauksissa ilmoitus tulee antaa myös muille jäsenvaltioille, jos poikkeama koskee heitä sekä Euroopan kyberturvallisuusvirasto ENISA:lle. NIS2-direktiivi antaa myös mahdollisuuden vapaaehtoiselle ilmoittamiselle, jossa valvovalle viranomaiselle voidaan ilmoittaa läheltä piti-tilanteista sekä haavoittuvuuksista, poikkeamista ja kyberuhista[165].

Yleinen tietosuoja-asetus määrää ilmoittamisesta artikloissa 33 ja 34, joissa erikseen ilmoitusvelvollisuudesta toimivaltaiselle viranomaiselle 72 tunnin kuluessa poikkeaman havaitsemisesta, joka Suomessa on Oikeusministeriön yhteydessä toimiva tietosuojavaltuutettu. Artiklassa 34 on määritelty vielä erikseen tilanteista, joissa rekisterinpitäjän tu-

[164] Andersson 2024, s.196.
[165] HE 57/2024 vp., s.17–18.

lisi ilmoittaa henkilötietojen tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä, erityisesti, jos luonnollisen henkilön oikeudet ja vapaudet ovat todennäköisen riskin kohteena.

Haasteena ilmoitusvelvollisuuksien erilaisuudesta voidaan nostaa erityisesti se, että poikkeaman laatua voi olla vaikeaa tunnistaa kaikissa tilanteissa, jolloin on epävarmaa, pitääkö tapauksesta ilmoittaa vain kyberturvallisuuspoikkeaman mukaisen ilmoitusvelvollisuuden vai tietoturvaloukkauksen mukaisen ilmoitusvelvollisuuden mukaisesti. Epäselvissä tilanteissa on toki mahdollista kysyä neuvoa valvovilta viranomaisilta ja voikin olla parempi tehdä ilmoitus mieluummin varmuudeksi kuin jättää kokonaan tekemättä. Ilmoittamatta jättämisestä voi seurata tapauksesta riippuen seurauksena pahimmillaan jopa hallinnollinen seuraamusmaksu. Vaikka siis ilmoitusvelvollisuus työllistää ja aiheuttaa lisätyötä kaikkine selvityksineen, on varmasti parempi ja toimijan kannalta myös edullisempi ratkaisu ilmoittaa kuin kärsiä taloudelliset seuraukset ilmoittamatta jättämisestä tapauksessa, jossa ilmoitus olisikin pitänyt tehdä. On todennäköistä, että NIS2-direktiivin toimeenpano tulee kasvattamaan ilmoitusten määriä, jolloin raportointiprosessia voisi olla syytä tarkastella uudelleen, jotta sitä voitaisiin yhtenäistää organisaation sisällä yhdessä tietosuojaa koskevien raportointiprosessien kanssa[166].

Ilmoittamisvelvoitetta haastaa vielä erikseen mahdolliset epäselvyydet toimijan roolissa ja siihen liittyvässä vastuussa. Rekisterinpitäjä on tietosuojalainsäädännössä käytännössä se osapuoli, jonka vastuulla on toteuttaa henkilötietojen käsittely niin, että rekisteröidyn yksityisyys ja henkilötietojen suoja on turvattu. Rekisterinpitäjä on siis taho, joka huolehtii rekisteröidyn oikeusturvasta havaitessaan mahdollisen poikkeaman, joka voi aiheuttaa tietoturvaloukkauksen. Lisää haastetta aiheuttaa henkilötietojen käsittelijän rooli ja sen linkittyminen rekisterinpitäjän rooliin, kuten Euroopan unionin tuomioistuimen tapauksen käsittelyssä aiemmin on voitu huomata[167].

[166] Andersson 2024, s.196.
[167] C-210/16, Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388.

Kyberkestävyys- ja kybersolidaarisuussäädökset ovat tärkeä lisä tukemaan NIS2-direktiivin mukaista kyberturvallisuuden vähimmäistason sääntelyä. NIS2-direktiivi keskittyy vaatimuksissaan organisaatioiden toteuttamaan kyberturvallisuuteen, kyberkestävyyssäädös tavaroiden kyberturvallisuuteen ja kybersolidaarisuussäädöksellä pyritään luomaan yhtenäistä rajat ylittävää Euroopan unionin laajuista yhteistyötä, jonka avulla poikkeamiin voitaisiin reagoida, niitä voitaisiin tutkia ja palautua niistä yhteispelillä eri maiden viranomaisten kesken.

Kun pohditaan, miten voidaan varmistaa, että poikkeamista ja tietoturvaloukkauksista annettavat ilmoitukset ovat riittävän oikea-aikaisia ja täsmällisiä, nousee esiin muutamiakin keskeisiä tulkinnallisia haasteita. Yhtenä keskeisenä haasteena erityisesti yleisen tietosuoja-asetuksen puolelta voidaan nostaa tulkinnallinen vaikeus 34 artiklan aikamääreen ”ilman aiheetonta viivästystä” kanssa. Korkeimman hallinto-oikeuden ratkaisussa 2024:115 on punnittu, miten aikamäärettä tulisi tulkita, ja kuinka pitkä aika on sallittua kulua henkilötietojen tietoturvaloukkauksen havaitsemisesta ennen kuin rekisteröidylle on ilmoitettu asiasta. Kyseisessä ratkaisussa tultiin tulokseen, että kyseisen aikamääreen tulkinta antaa mahdollisuuksia tilannekohtaiseen ja intressipunnintaan perustuviin tulkintoihin. Erityisesti rekisterinpitäjätahon rooli yhteiskunnallisesti voi vaikuttaa aikamääreen tulkintaan. Jos siis rekisterinpitäjä toimii jokin julkishallinnollinen taho, voi olla, että sen toimintaa sääntelee jotkin erityislait, kuten julkisuuslaki, joka syrjäyttää tulkinnallisessa ristiriitatilanteessa yleislakina sovellettavan tietosuojalain, voi hyvin olla, että kohdataan haasteita mahdollisen loukkauksen sattuessa sovellettavien oikeussääntöjen tulkinnassa tai mahdollisten ilmoitusvelvollisuuksien ja niiden aikamääreiden soveltamisessa tai soveltamatta jättämisessä.

5.2 Lainsäädännön kehittämistarpeet ja suositukset

NIS2-direktiivin käsitteet tuntuvat osaltaan olevan täsmällisempiä kuin yleisen tietosuoja-asetuksen käsitteet. Erityisesti rekisterinpitäjän ja henkilötietojen käsittelijän määritelmät ja laajat ja suppeat tulkinnat voivat aiheuttaa haasteita, kun pitäisi tunnistaa

vastuualueet. Vastuualueiden määrittäminen on kuitenkin yksi merkittävistä kyberturvallisuuden riskienhallintakeinoista.

Koska NIS2-direktiivi ja yleisen tietosuoja-asetuksen velvoitteet kytkeytyvät toisiinsa merkittävästi useissa tapauksissa, olisi hyvä, jos lainsäätäjällä olisi mahdollisuus yhtenäistää säädösten määrittämiä ilmoitusvelvollisuuksia, jotta se ei olisi niin moniportainen ja hajanainen. Yhtenäinen ilmoittaminen helpottaisi toimijoiden toimenpiteitä poikkeaman sattuessa, vaikkakin säädöksillä on täysin eri valvovat viranomaiset. Kyberturvallisuuslain toimeenpanon myötä organisaatioiden päässä ilmoitukset lisääntyy, jonka myötä raportointiprosessien sujuvuutta ja yhtenäisyyttä voisi olla syytä tarkastella uudelleen erityisesti organisaation näkökulmasta.

Petteri Orpon hallitus ajaa parhaillaan uudistusta koskien tietosuojaloukkauksista seuraavia hallinnollisia seuraamusmaksuja[168]. Yleisen tietosuoja-asetuksen 83 artiklan 7 kohta on mahdollistanut kansallisen liikkumavaran seuraamusmaksujen määräämiselle julkisille toimijoille, ja kansallisessa tietosuojalain 24§:n 4 momentissa on säädetty, ettei maksua voi kyseisille tahoille määrätä. Nyt kuitenkin hallitus on esityksessään ehdottanut, että uudistuksen myötä myös julkishallinnon toimijalle voitaisiin määrätä hallinnollinen seuraamusmaksu. Asiassa on selkeästi tarvetta päivitykselle, sillä julkishallinnon toiminnoissa on havaittu runsaasti puutteita, joista tietosuojaviranomainen on antanut huomautuksia. Huomautuksia on annettu suhteessa enemmän julkishallinnon toimijoille verrattuna yksityissektorin saamiin, joten tarve jonkinlaiselle julkishallintoon kohdistuvalle ”pelotteelle” on, jotta tietosuojalainsäädäntöä noudatettaisiin ja henkilötietojen suojan turva toteutuisi käsittelyssä, ja jotta julkisen sektorin ja yksityisen sektorin seuraamukset olisivat tasapainossa keskenään.

[168] HE 46/2026 vp.

5.3 Tulevaisuuden näkymät ja suositukset organisaatioiden kyberturvallisuuskäytännöille

NIS2-direktiivi erityisesti asettaa organisaatioille vaatimuksia, jotka organisaatioiden tulee ottaa osaksi toimintaansa. Yksi keskeinen organisaation aktiivisuutta vaativa velvoite on ilmoittaa havaitusta poikkeamasta viranomaiselle. NIS2-direktiivi määrittää poikkeaman ilmoitusajat, joiden puitteissa ilmoitukset tulee jättää. Organisaatioiden olisikin siis hyvä pyrkiä ottamaan huomioon nämä ilmoitusajat muun muassa kaikissa sopimuksissa yhteistyökumppaneidensa kanssa. Organisaation olisi hyvä jättää itselleen pelivaraa ilmoituksen tekemiseen, mikäli sopimuskumppani ilmoittaa havaitsemastaan poikkeamasta. Organisaatio voi siis vaatia esimerkiksi sopimusehtoihin pykälän, jossa määritellään, kuinka nopeasti sopimuskumppanin on ilmoitettava toimijalle havaitsemastaan poikkeamasta, jotta viranomaisen ilmoitusaikatauluissa pysytään.

Myös jo NIS2-direktiivi edellyttää, että toimijan tulee huolehtia toimintaansa sellaiset tekniset valmiudet, jonka avulla mahdollisista poikkeamista tulee automaattisesti ilmoitus heti, kun se on havaittu. Erityisesti julkishallinnon toimijan olisi hyvä huomioida käytössä olevan virka-ajan vaikutus poikkeaman havaitsemiseen ja siihen reagointiin. Olisiko syytä asettaa jonkinlainen päivystäjä, joka on valmiudessa ilmoittamaan havaitusta poikkeamasta viranomaisille ja kutsumaan koolle poikkeaman selvittämiseksi vaadittavat henkilöt? Virka-aikaa soveltaessa on otettava siis huomioon, että virka-ajan vuoksi poikkeaman havaitsemisessa ja selvittelyssä voi olla viivästystä, ellei organisaation käytössä olevat tekniset valmiudet mahdollista automaattista ilmoitusta toimijalle havaitusta poikkeamasta, jotta siihen voitaisiin reagoida mahdollisimman nopeasti.

Sen lisäksi, että organisaation johdon tulee pitää huolta henkilöstön riittävästä tietoturvallisuuden osaamisesta ja kouluttaa henkilöstöä tarvittaessa. Lisäksi organisaatiossa olisi hyvä huolehtia, että koulutetut taidot ovat myös käytännössä hallussa. Organisaatiossa olisi siis hyvä järjestää yhteisiä harjoituksia, joissa harjoitellaan poikkeamatilanteessa toimimista.

Tulevaisuuden näkymiä arvioidessa on mahdotonta sanoa, minkälaiseksi kyberturvallisuusympäristö tulee kehittymään, sillä muun muassa tekoäly on merkittävästi lisännyt jalansijaansa jopa arkipäiväisessä käytössä. Tekoäly saattaa mahdollistaa uudenlaiset tavat kiertää lakia tai tuottaa uusia haasteita kyberturvallisuuden kannalta. Lisäksi on mahdotonta sanoa, millaisia uusia keinoja verkkorikolliset keksivät uuden vaatimuksiltaan tiukemman lain kiertääkseen. Tuleeko uusi lainsäädäntö kestämään aikaa vai onko jo pian tarvetta lain päivittämiselle?

On kiinnostavaa nähdä, mihin keskustelu julkishallintoon kohdistuvista hallinnollisista seuraamusmaksuista etenee, varsinkin, kun hallituksen esitys[169] ja oikeusasiamiehen kommentti[170] tuntuvat olevan hieman erimielisyyksissä toistensa kanssa perusteluineen. Jos julkishallinnolle voidaan määrätä hallinnollisia seuraamusmaksuja jatkossa, on kiinnostavaa nähdä miten käytännössä tuo tulee tapahtumaan, ja miten se tulee vaikuttamaan julkishallinnollisten toimijoiden lakisääteisten tehtävien hoitoon tai talouden tasapainoon. Onko uudistuksella oikeasti positiivisia vaikutuksia rekisteröityjen luottamukseen julkishallintoa kohtaan, kun tämä toimii rekisterinpitäjänä, vai onko uudistuksella todellisuudessa mitään vaikutusta luottamukseen? Voiko uudistus muuttaa kuitenkin suhtautumista negatiivisempaan suuntaan, kun käytännössä julkishallinnolle määrätty hallinnollinen sakko tullaan maksamaan rekisteröidyiltä ja muilta veronmaksajilta kerätyistä verovaroista. Mielestäni oikeusasiamies esitti lausunnossaan hyviä ja tärkeitä perusteita siitä, miten muulla tavalla tietosuojaloukkauksista tai laiminlyönneistä aiheutuneet seuraamukset voitaisiin hallinnollisten seuraamusmaksujen sijaan hoitaa. Potentiaalisena esimerkkinä pidin oikeusasiamiehen esittämän virkarikosoikeudellisen vastuun muuttamista, sillä siinä oikeushenkilöllisyys olisi helpommin sovellettavissa, eikä välttämättä jatkon kannalta aiheuttaisi oikeustapausten näkökulmasta niin mittavia prosesseja kuin mahdollisesti hallinnollisen seuraamusmaksun myötä saattaa olla tulossa.

[169] HE 46/2026 vp.
[170] EOAK/6681/2024.

Lähteet

Oikeuskirjallisuus

Aalto, P. (2025). *EU-oikeus Suomessa*. Alma Insights.

Andersson, J. (2024). *Organisaation hyvä tietoturvan sääntelyjärjestelmä*. [Väitöskirja, Vaasan yliopisto]. Osuva. http://www.urn.fi/URN:ISBN:978-952-395-150-1

Euroopan parlamentti ja neuvosto. (2024). Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös). Euroopan unionin virallinen lehti, L 2847, 1–81. Noudettu 3.3.2025 osoitteesta http://data.europa.eu/eli/reg/2024/2847/oj

Euroopan parlamentti ja neuvosto. (2025). Euroopan parlamentin ja neuvoston asetus (EU) 2025/38, annettu 19 päivänä joulukuuta 2024, toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberuhkien ja poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten ja asetuksen (EU) 2021/694 muuttamisesta (kybersolidaarisuussäädös). *Euroopan unionin virallinen lehti*, L 38, 1–34. Noudettu 3.3.2025 osoitteesta http://data.europa.eu/eli/reg/2025/38/oj

Ferm, T. (2018). Ajankohtaista EU:n hybridiuhkien torjunnasta. *Defensor Legis* N:o 3/2018, 404–419.

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. (2017). *Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset.* Kauppakamari.

Hirvonen, A. (2011). *Mitkä metodit?: opas oikeustieteen metodologiaan*. Noudettu 14.1.2025 osoitteesta https://issuu.com/arihirvonen/docs/mitk__meto-dit_paino

Husa, J. & Pohjolainen, T. (2014). *Julkisen vallan oikeudelliset perusteet: johdatus julkisoikeuteen.* Alma Talent Oy.

Koivumäki, E. & Häkkänen, P. (2018). *Markkinointijuridiikka 2018*. Kauppakamari.

Kolehmainen, A, (2016). *Tutkimusongelma ja metodi lainopillisessa työssä*. Teoksessa T, Mietteinen (toim.) *Oikeustieteellinen opinnäyte – artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodeista ja arvosteluista.* Edilex.

Lindroos-Hovinheimo, S. (2018). Kuka vastaa tietosuojasta? Unionin tuomioistuimen uusimpia näkemyksiä henkilötietojen käsittelijöiden vastuun jakautumisesta. *De fensor Legis*, N:o 5/2018, 757–763.

Mäenpää, O. (2017). *Yleinen hallinto-oikeus*. Alma Talent Oy.

Mäenpää, O. (2020). *Julkisuusperiaate*. Alma Talent Oy.

Mäenpää, O. (2023). *Hallinto-oikeus*. Alma Talent Oy.

Neuvonen, R. (2019). *Viestintä- ja informaatio-oikeuden perusteet*. Kauppakamari. 2. uudistettu painos. Noudettu 11.12.2024 osoitteesta https://kauppakamaritieto-fi.proxy.uwasa.fi/ammattikirjasto/teos/viestinta-ja-informaatio-oikeuden-perusteet#kohta:Viestint((e4)-((20)ja((20)informaatio-oikeuden((20)perusteet

Ojajärvi, O. (2022). *Ihmiskeskeinen tiedonhallinta – tiedollisesta itsemääräämisoikeudesta omadata-ajatteluun?.* Liikejuridiikka 2/2022, s.102–131.

Pilke, A. (2022, 28. tammikuuta). *Suomalaisia diplomaatteja vakoiltu haittaohjelmalla – ulkoministeriö: Vakava tapaus, tulkitsemme laittomaksi tiedusteluksi*. Yle. Noudettu 27.4.2025 osoitteesta: https://yle.fi/a/3-12292218

Saarenpää, A. & Riekkinen, J. (2023). *Oikeusinformatiikan perusteet*. Lapin yliopisto. Noudettu 11.12.2024 osoitteesta https://lauda.ulapland.fi/bitstream/handle/10024/65315/978-952-337-347-1.pdf?sequence=1&isAllowed=y

Seppänen, J. (2024). *Riskin käsitteen ja oikeudellisen sääntelyn suhde oikeusteoreettisena kysymyksenä*. Edilex-sarja 2024/3. Edilex.

Sisäministeriö (2025). Harvaan asuttujen alueiden turvallisuus 2025: Tilanneraportti turvallisuudesta harvaan asutuilla alueilla. *Sisäministeriön julkaisuja* 3/2025. https://urn.fi/URN:ISBN:978-952-324-966-0

Talus, K., Penttinen, S.J. (2016) *Eurooppaoikeudelliset oikeuslähteet ja niiden tulkinta oikeustieteellistä opinnäytettä kirjoittaessa.* Teoksessa T., Mietteinen (toim.) *Oikeustieteellinen opinnäyte – artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodeista ja arvosteluista.* Edilex.

Ulkoministeriö (2022). *Ulkoministeriö on saanut selvitettyä siihen kohdistuneen vakoilutapauksen.* Noudettu 27.4.2025 osoitteesta https://um.fi/ajankohtaista/-/asset_publisher/gc654PySnjTX/content/ulkoministerio-on-saanut-selvitettya-siihen-kohdistuneen-vakoilutapauksen

Valtioneuvosto (2020). *Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko*. Noudettu 27.4.2025 osoitteesta: valtioneuvosto.fi/delegate/file/78665

Valtioneuvosto (2022). *Ajankohtaisselonteko turvallisuusympäristön muutoksesta*. Valtioneuvoston julkaisuja 18/2022. https://urn.fi/URN:ISBN:978-952-383-772-0

Valtioneuvosto (2024). Suomen kyberturvallisuusstrategia 2024-2035. Valtioneuvoston kanslian julkaisuja 11/2024. Noudettu 3.3.2025 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165860/VNK_2024_11.pdf?sequence=1&isAllowed=y

Valtiovarainministeriö (2016). *EU-tietosuojan kokonaisuudistus – VAHTI-raportti*. 1/2016. Julkisen hallinnon ICT. Noudettu 26.4.2025 osoitteesta: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/75065/VAHTI-raportti%201_2016.pdf?sequence=1

Voutilainen, T. (2023). *Digitaalisten palvelujen sääntely*. Alma Talent Oy.

Virallislähteet

HE 57/2024 vp. Hallituksen esitys Eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi.

HE 9/2018 vp. Hallituksen esitys Eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

HE 46/2026 vp. Hallituksen esitys Eduskunnalle tietosuojalain ja henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain seuraamussäännösten muuttamiseksi.

Kotimainen oikeuskäytäntö

KHO:2024:115

KHO:2022:131

Ylimpien lainvalvojien ratkaisut

EOAK/6681/2024 Viranomaisia koskevat seuraamukset tietosuojalainsäädännön rikkomisesta.

Euroopan unionin oikeuskäytäntö

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH (C-210/16)