Katariina Kankaanpää

Tietosuoja ja tietoturvallisuus riskienhallintavelvoitteina

Johtamisen akateeminen yksikkö
Julkisoikeus
Hallintotieteiden kandidaatti

Vaasa 2025

VAASAN YLIOPISTO
Johtamisen akateeminen yksikkö
Tekijä: Katariina Kankaanpää
Tutkielman nimi: Tietosuoja ja tietoturvallisuus riskienhallintavelvoitteina
Tutkinto: Hallintotieteiden kandidaatti
Oppiaine: Julkisoikeus
Työn ohjaaja: Laura Perttola
Valmistumisvuosi: 2025 **Sivumäärä:** **38**

TIIVISTELMÄ:
Viime vuosien geopoliittiset muutokset, kuten Venäjän hyökkäys Ukrainaan, ovat tehneet Suomen turvallisuusympäristöstä epävakaamman ja paljastaneet kriittisen infrastruktuurin riskit, kuten kaasuputkien ja kaapelien vaurioitumisen. Tämä korostaa tarvetta panostaa infrastruktuurin, palveluiden ja kyberturvallisuuden suojaamiseen sekä hybridiuhkiin reagoimiseen. Riskienhallinta on nykyaikaisen oikeudellisen ja hallinnollisen toiminnan keskeinen osa-alue, erityisesti tietosuojan, tietoturvan ja kyberturvallisuuden näkökulmasta. Lainsäädäntö, kuten tietosuoja-asetus (asetus (EU) 2016/679, GDPR), tietosuojalaki, NIS2-direktiivi ((EU) 2022/2555) sekä kyberturvallisuuslaki, velvoittaa organisaatiot tunnistamaan, arvioimaan ja hallitsemaan riskejä itsenäisesti. Riskienhallinnan tavoitteena on tulevien haitallisten tapahtumien ennakointi, toiminnan jatkuvuuden turvaaminen ja perusoikeuksien toteutuminen. Se kattaa turvallisuuden, tietosuojan, kyberturvallisuuden ja henkilöstöturvallisuuden, ja sen tehokas toteuttaminen edellyttää resursointia, osaamista sekä johdon aktiivista osallistumista.

Tietosuoja-asetus (asetus (EU) 2016/679, GDPR) ja kansallinen tietosuojalaki asettavat organisaatioille riskiperusteisen velvoitteen huolehtia henkilötietojen turvallisuudesta. Lainsäädäntö ei tarjoa yksityiskohtaisia “tee näin” -ohjeita, vaan edellyttää, että organisaatiot itse arvioivat henkilötietojen käsittelyyn liittyvät riskit ja mitoittavat suojatoimet niiden mukaisesti. Tämä sisältää tekniset ja organisatoriset toimet, henkilöstön koulutuksen sekä säännöllisen arvioinnin ja auditoinnin. Tietosuoja liittyy läheisesti perusoikeuksiin, kuten yksityisyyden, kunniaan, yhdenvertaisuuden ja turvallisuuden suojaan. Läpinäkyvyys ja tietojen minimointi ovat keskeisiä periaatteita, ja henkilötietoja saa käsitellä vain perustelluista syistä, tarvittaessa erityistoimin suojaten. Riskien merkityksen osoittaa esimerkiksi Vastaamon tietomurto, jossa puutteellinen riskienhallinta johti vakaviin henkilötietojen loukkauksiin, perusoikeuksien rikkomiseen sekä merkittäviin taloudellisiin ja mainehaittoihin.

Tutkimus osoittaa, että tietosuojan ja tietoturvan toteuttaminen edellyttää laaja-alaista resursointia, koulutusta ja organisaatioiden välistä yhteistyötä. Nykyinen sääntelyn pirstaleisuus, ohjeistusten niukkuus ja oikeuskäytännön puutteet lisäävät haasteita erityisesti julkisella sektorilla. Samalla digitaalisen tietojenkäsittelyn kasvu korostaa tietoturvan merkitystä ja riskiä tietosuojaloukkausten vaikutuksista rekisteröityihin. Tämä osoittaa jatkotutkimustarpeita, sillä turvallisuusuhat muuttuvat yhä kompleksisemmiksi ja lainsäädännön on pysyttävä näiden tarpeiden perässä. Edessä on monia kysymyksiä pirstaleisen lainsäädännön yhtenäistämisessä niin kansallisella kuin kansainvälisellä tasolla.

AVAINSANAT: Julkisuusperiaate, kyberturvallisuus, riskienhallinta, perus-ja ihmisoikeudet, tietosuoja, tietoturva, yksityisyys

Sisällys

1 Johdanto 5

2 Riskienhallinta ja merkitys oikeusjärjestelmässä 8

2.1 Riskienhallinta määrittelyä ja taustaa 8

2.2 Riskienhallintavelvoitteet 10

2.3 Turvallisuus osana riskienhallintaa 13

2.4 Tämän päivän riskienhallintaa 14

3 Tietosuoja ja tietoturvallisuus riskienhallintavelvoitteena 16

3.1 Tietosuoja – perustana EU:n yleinen tietosuoja-asetus 16

3.1.1 Tietosuoja osana perusoikeuksia ja oikeusperiaatteita 20

3.1.2 Tietosuojaan kytkeytyvät haasteet 22

3.2 Tietoturvallisuus 23

4 Johtopäätökset 30

Lähteet 35

Lyhenteet

dnro	diaarinumero
EIS	Euroopan ihmisoikeussopimus
EIT	Euroopan ihmisoikeustuomioistuin
EU	Euroopan Unioni
GDPR	General Data Protection Regulation
HE	Hallituksen esitys
TSA	Tietosuoja-asetus
vp	Valtiopäivät
VPN	Virtual Private Network, virtuaalinen yksityisverkko

1 Johdanto

Riskien tunnistaminen ja hallinta ovat keskeisiä elementtejä oikeudenmukaisen toiminnan varmistamisessa. Riskin käsitteeseen ja riskiperusteiseen lähestymistapaan törmätään nykyisin monenlaisissa oikeudellisissa asiayhteyksissä. Esimerkiksi tietosuojaan ja tietoturvallisuuteen liittyvien lain säädäntöuudistusten myötä erilaiset julkisen ja yksityisen sektorin toimijat ovat nykyisin velvoitettuja arvioimaan tietojenkäsittelyynsä liittyviä riskejä.[1] Riskienhallinta toimii erinomaisena työvälineenä, kun organisaation tulee kehittää omaa turvallisuuttaan parantavia prosesseja, toimenpiteitä ja palveluita. Riskienhallinnan avulla saavutetaan kustannustehokkuutta, kun kehittäminen voidaan ohjata aidosti sellaisten asioiden toteuttamiseen, joilla on merkittävä vaikutus jonkun tunnistetun uhan todennäköisyyden tai vaikutuksen pienentämiseen. [2]

Aiempi oikeudellinen tutkimus riskienhallinnasta ja riskiperusteisuudesta tietosuoja- ja tietoturvavelvoitteiden näkökulmasta on edelleen melko niukkaa. Tässä tutkielmassa tarkastellaan, miten voimassa oleva lainsäädäntö ohjaa riskiperusteista toimintaa erityisesti tietosuojan ja tietoturvallisuuden osalta. Tavoitteena on ymmärtää, miten riskienhallintavelvoitteet ilmenevät julkisen ja yksityisen sektorin rekisterinpitäjien ja käsittelijöiden toiminnassa, ja millaisia oikeudellisia riskejä voi syntyä, jos niitä ei toteuteta asianmukaisesti.

Tutkielma sijoittuu tietosuojalainsäädännön, perusoikeuksien ja hallinnon yleisten velvoitteiden rajapintaan. Keskeisiä oikeuslähteitä ovat Euroopan unionin yleinen tietosuoja-asetus (asetus (EU) 2016/679, GDPR), Euroopan unionin kyberturvallisuusdirektiivi (direktiivi (EU) 2022/2555), kansallinen tietosuojalaki sekä

[1] Seppänen,2024, s.2
[2] Rousku, 2017, s. 3

laki julkisen hallinnon tiedonhallinnasta. Näiden säädösten kautta tarkastellaan riskienhallinnan oikeudellista sisältöä ja sen käytännön velvoitteita.

Tutkielman tavoitteena on vastata seuraaviin tutkimuskysymyksiin:

1. Miten lainsäädäntö ohjaa riskiperusteista toimintaa tietosuojan ja tietoturvan toteuttamisessa?
2. Millaisia oikeudellisia riskejä liittyy tietosuojan ja tietoturvan laiminlyöntiin, ja miten niitä tulisi hallita ennakoivasti?

Tutkielma nojaa oikeusdogmaattiseen tutkimusmetodiin, jossa tarkastellaan voimassa olevaa lainsäädäntöä, oikeuskäytäntöä, lainvalmisteluaineistoa sekä viranomaisten ohjeistuksia. Oikeusdogmatiikka eli lainoppi tuottaa suosituksia siitä, miten viranomaisen tai tuomioistuimen pitää lakia soveltaa.[3] Rajaus kohdistuu Suomen kansalliseen oikeusjärjestykseen ja siihen liittyvään EU-oikeudelliseen sääntelyyn, mutta kansainväliset sopimukset ovat olennainen osa, koska ne vaikuttavat olennaisesti kansalliseen tulkintaan.

Ensimmäisessä pääluvussa käsitellään riskienhallinnan käsitteellistä ja oikeudellista perustaa. Luvussa määritellään, mitä riskienhallinta tarkoittaa oikeudellisena velvoitteena erityisesti julkisen hallinnon ja sääntelyn kontekstissa. Tarkastelussa huomioidaan riskienhallinnan historiallinen kehitys, käsitteellinen rakenne ja sen erityisyys suhteessa muihin normityyppeihin. Lisäksi esitellään, kuinka riskien havaitseminen, arviointi ja hallinta rakentuvat osaksi oikeudellista sääntelyä, ja miten eksplisiittisiä tai implisiittisiä velvoitteet voivat olla.

Toinen pääluku keskittyy tietosuojan ja tietoturvallisuuden sääntelyyn riskienhallintavelvoitteiden näkökulmasta. Luvussa analysoidaan keskeisiä säädöksiä,

[3] Rautiainen ym., 2023, s. 27

kuten yleistä tietosuoja-asetusta (asetus (EU) 2016/679, GDPR), tietosuojalakia ja NIS2-direktiiviä ((EU) 2022/2555), ja sitä, miten ne asettavat nimenomaisia riskienhallintavaatimuksia rekisterinpitäjille ja kriittisen infrastruktuurin toimijoille. Samalla tarkastellaan tietosuojan ja tietoturvan välistä rajankäyntiä sekä näiden käsitteiden perus- ja ihmisoikeudellista ulottuvuutta.

2 Riskienhallinta ja merkitys oikeusjärjestelmässä

2.1 Riskienhallinta määrittelyä ja taustaa

Riskillä tarkoitetaan kohtuullisesti tunnistettavissa olevaa uhkaa tai tapahtumaa, jonka seurauksena voi aiheutua menetystä tai vahinkoa, esimerkiksi verkko- ja tietojärjestelmien turvallisuudelle. [4] Riskienhallintaan liittyy myös epävarmuuden huomioon ottaminen. Riski itsessään merkitsee epävarmuuden vaikutusta tavoitteisiin, eli poikkeamaa siitä, mitä on odotettu. Epävarmuus on usein uhka tai vaara, josta voi seurata jotakin negatiivista tai toiminnan kannalta epäedullista. Se voi tarkoittaa myös positiivista mahdollisuutta ja onnistumisen kautta tulevaa hyötyä tai etua, mikäli epävarmuustekijät pystytään minimoimaan tai niiltä osataan välttyä. [5]

Tietosuojatyöryhmä määrittelee *riskinhallinnan* koordinoiduksi toiminnaksi, jolla ohjataan ja valvotaan organisaatiota riskien osalta. Riskin voidaan sanoa aina koostuvan kolmesta tekijästä:

1) tapahtumasta,

2) tapahtuman todennäköisyydestä ja

3) tapahtuman seurauksien vakavuudesta eli tapahtuman aiheuttamasta vahingosta. [6]

Esimerkiksi riski siitä, että henkilötiedot paljastuvat tietomurrossa, koostuu 1) tietomurtotapahtumasta, 2) todennäköisyydestä, että tietoturvan puute on sellainen, että henkilötiedot kyetään vuotamaan, ja 3) siitä vahingosta, joka tietojen vuotamisesta aiheutuu.

> Psykoterapiakeskus Vastaamon tietomurtotapauksessa vuonna 2020 itse tietomurto oli tapahtuma, jossa henkilötietoja vuodettiin. Apulaistietosuojavaltuutetun [7] päätöksestä ilmenee, että ennen vuoden 2020

[4] Andersson, 2018, s. 3
[5] Rousku, 2017, s. 11
[6] Korpisaari ym., 2022, s. 31
[7] TSV 07.12.2021, dnro 1150/161/2021

> tietomurtoa oli tapahtunut jo vuosina 2018 ja 2019 kaksi tietoturvaloukkausta. Vastaamon tietomurrossa tietomurron riskin todennäköisyys oli suuri, koska Vastaamon potilastietojärjestelmässä olleet puutteet suojauksessa eivät olleet lyhytaikaisia tai vähäisiä, vaan kestivät jopa useita vuosia. Tämän puolesta puhuu myös se, että suojausta koskevien perustoimenpiteiden laiminlyömisestä rekisteröidyille aiheutuvien vakavien vahinkojen riski on ollut varsin todennäköinen, ja Vastaamon on täytynyt olla tästä tietoinen. Tietomurron seuraukset olivat vakavia, koska yksilöille aiheutui merkittävää kärsimystä ja identiteettivarkauksien riski kasvoi, organisaation maine tuhoutui ja se joutui konkurssiin, sekä tapaus vaikutti lainsäädäntöön.[8]
>
> Vastaamon olisi tullut tunnistaa potentiaaliset riskit, arvioida niiden todennäköisyys ja vakavuus sekä suunnitella ja toteuttaa tehokkaita toimenpiteitä riskien vähentämiseksi. Valitettavasti Vastaamon kohdalla nämä riskienhallinnan kolme keskeistä vaihetta epäonnistuivat, mikä johti traagisiin seurauksiin.

Riskienhallinta on toimintaa, jolla pyritään siis tunnistamaan ja hallitsemaan organisaation toimintaa haittaavia tekijöitä, estämään haitallisia tapahtumia tai lieventämään niiden seurauksia siten, että riskit pysyvät tasolla, joka ei uhkaa organisaation tavoitteita.[9] Riskienhallinnan tarkoituksena on mahdollistaa organisaation menestyminen, toiminnan jatkuvuuden takaaminen ja tavoitteiden saavuttaminen. Riskienhallinta on järjestelmällistä ja tavoitteellista toimintaa, jolla tuetaan lisäksi organisaation johtamista ja kehittymistä. Riskienhallinta on osa johtamisen ja toiminnan prosesseja sekä suunnittelua ja seurantaa.[10]

Riskin käsite juontaa juurensa keskiajalle, jolloin se liittyi alun perin jumalalliseen suosioon ja sattumaan. Termi esiintyi Euroopassa 1100-luvun lopulla muodoissa *risicum* ja *resicum*, ja sen merkitys alkoi vähitellen siirtyä kohti taloudellista vaihdantaa ja päätöksentekoa epävarmuuden vallitessa. Erityisesti 1800-luvulla positivismi ja oikeudellinen rationalismi muovasivat käsityksiä oikeudesta ja sen tieteellisestä luonteesta. Tämä loi perustan riskien systemaattiselle hallinnalle ja sääntelylle osana oikeusjärjestelmää.[11]

---

[8] TSV 07.12.2021, dnro 1150/161/2021
[9] Andersson, 2018, s. 3
[10] Rousku, 2017, s. 11, s. 12
[11] Seppänen, 2024, s. 17

Vaikka lainsäädännössä ei aiemmin käytetty eksplisiittisesti "riskin" käsitettä, jo 1700–1800-luvuilla oli nähtävissä pyrkimyksiä yhteiskunnallisten vaarojen hallintaan. Riskienhallintavelvoitteet saattoivat sisältyä sääntelyyn epäsuorasti, esimerkiksi onnettomuuksien ehkäisyn tai turvallisuuden varmistamisen muodossa. Hyvinvointivaltion kehittyminen toi mukanaan uudenlaista riskiajattelua, jossa esimerkiksi työtapaturmien hallintaan vastattiin vakuutusmekanismein ja solidaristisen vastuullisuuden keinoin.[12]

Tuorin [13] mukaan oikeus on siirtynyt yhä selvemmin traditionaalisista normeista asiantuntijajärjestelmien suuntaan. Tavanomainen oikeus on positivoitunut eli sen sisältö ei enää perustu ensisijaisesti menneeseen käytäntöön, vaan se rakentuu jatkuvasti päivittyvän tiedon ja riskien ennakoinnin varaan. Näin syntyy uudenlaista "tapaoikeutta", joka on tiiviimmin sidoksissa tulevaisuuden hallintaan kuin menneisyyden perinteisiin.[14]

2.2 Riskienhallintavelvoitteet

Riskienhallinnan avulla voidaan arvioida, millaisia riskejä organisaatio on valmis ottamaan strategisten tavoitteiden asettamisessa ja miten niitä hallitaan tavoitteiden saavuttamiseksi. Tämä on riskiensietokykyä, eli se riskin suuruus, johon organisaatio on valmis sitoutumaan riskien määrittelyn jälkeen.[15]

Riskienhallinta voidaan jäsentää kolmeen vaiheeseen, josta muodostuu riskienhallintavelvoitteet. Riskienhallintavelvoitteita voidaan Seppäsen[16] mukaan pitää oikeusnormeina, jotka velvoittavat kohteenaan olevia toimijoita tunnistamaan, arvioimaan ja hallitsemaan riskejä. Hänen mukaansa velvoitteet jaetaan seuraavasti:

---

[12] Seppänen, 2024, s.18–19
[13] Tuori, 2007, s.74
[14] Tuori, 2007, s.74
[15] Rousku, 2017, s.12, s.15
[16] Seppänen, 2024, s.10

1) Riskin tunnistaminen (risk perception): inhimillistä arvoa uhkaavan ja lopputulokseltaan epävarman tapahtuman olemassaolosta ei voida välttämättä johtaa oikeudellista velvollisuutta havainnoida tai tunnistaa tällaista tapahtumaa
2) Riskin arviointi (risk assessment): vaikka olisi asetettu velvollisuus 1 riskin tunnistamiseen, tästä velvollisuudesta ei voida välttämättä johtaa velvollisuutta arvioida nimenomaisesti sen todennäköisyyttä tai seurausten vakavuutta
3) Riskin hallinta (risk management): vaikka olisi asetettu velvollisuus kohdissa 1 ja 2 mainittuihin riskin tunnistamiseen ja arviointiin, näistä velvollisuuksista ei voida välttämättä johtaa velvollisuutta ryhtyä toimimaan tietyllä tavalla esimerkiksi riskin todennäköisyyden tai seurausten vakavuuden pienentämiseksi.[17]

Seppäsen [18] mukaan, jotta jokin oikeussäännös voitaisiin katsoa sisältävän riskienhallintavelvoitteen, sen tulisi kattaa tavalla tai toisella ainakin yksi edellä mainituista kolmesta osa-alueesta. Hän toteaa Beckiä ja Hutteria seuraten, että riskiajattelun ytimessä on ajatus tulevien katastrofien ennakoimisesta. Ei siis siitä, miten jo tapahtuneisiin onnettomuuksiin reagoidaan. Heti kun riski toteutuu ja muuttuu konkreettiseksi tapahtumaksi, se ei enää ole riski vaan realisoitunut seuraus. Tästä syystä riskienhallintavelvoitteet eroavat selvästi sellaisesta sääntelystä, joka keskittyy menneiden tapahtumien arviointiin tai seurausten korjaamiseen.[19]

Korpisaari ym. [20] sen sijaan näkevät, että kullekin riskille voidaan teoriassa määritellä myös numeerinen arvo kertomalla tapahtuman todennäköisyys ja tapahtuman aiheuttama vahinko keskenään. Käytännössä ei kuitenkaan yleensä ole heidän mukaansa mahdollista arvioida sen enempää vahingon todennäköisyyttä kuin sen suuruuttakaan kovin tarkasti, mutta ajattelutapana tämä auttaa hahmottamaan, minkä kokoisia riskejä on ja miten paljon niiden torjumiseen ja ennalta ehkäisemiseen kannattaa.[21]

---

[17] Seppänen, 2024, s. 10
[18] Seppänen, 2024, s. 10
[19] Seppänen, 2024, s. 10
[20] Korpisaari ym., 2022, s.32
[21] Korpisaari ym., 2022, s.32

Seppänen[22] kuvailee riskienhallintavelvoitteiden keskeiseksi piirteeksi sen, että vastuu riskien tunnistamisesta, arvioinnista ja niihin varautumisesta on sääntelyn kohteena olevalla toimijalla itsellään. Toimijan ei siis riitä pelkkä sääntelyn seuraaminen tai yksittäisten määräysten noudattaminen, vaan hänen tulee itse käyttää omaa harkintaansa riskien hallitsemiseksi. Seppäsen mukaan, jos laki määrittää täsmällisesti, mitä toimenpiteitä tietyn riskin torjumiseksi tulee tehdä, ei kyse ole enää varsinaisesta riskienhallintavelvoitteesta, vaan kyseessä on täsmällinen velvoite, suoritettava toimenpide, jonka sisältö on jo valmiiksi määrätty.[23]

Esimerkki riskienhallintavelvoitteista löytyy työturvallisuuslaista (738/2002). Lain 8 §:ssä säädetään, että työnantajan on huolehdittava työntekijöiden turvallisuudesta ja terveydestä työssä, mutta jätetään pitkälti työnantajan arvioitavaksi, miten tämä toteutetaan käytännössä. Työnantajan on siis tunnistettava työpaikan mahdolliset vaaratekijät, arvioitava niiden todennäköisyys ja vakavuus, ja toteutettava riittävät toimenpiteet näiden riskien ehkäisemiseksi. Lainsäätäjä ei kuitenkaan määrittele yksityiskohtaisesti esimerkiksi, kuinka monta varoituskylttiä pitää olla tai minkälaista suojaustasoa tietyssä työtehtävässä tarvitaan. Nämä asiat jäävät toimijan vastuulle riskinarvioinnin pohjalta. Huomioitavaa on se, että työnantajan velvoitteet ei koske olosuhteita, joita huolellinen toimialansa asiantuntijana toimiva työnantaja ei voi kohtuudella ennakoida tai hallita asianmukaisin toimenpitein.[24]

Tällainen sääntelyn muoto tukee Seppäsen [25] esittämää ajatusta siitä, että riskienhallintavelvoitteet eroavat perinteisestä sääntelystä, jossa määräykset ovat tarkkarajaisia ja eksplisiittisiä. Samalla ne auttavat toimijoita rakentamaan järjestelmällisiä malleja täyttääkseen avoimiksi jätetyt oikeudelliset velvoitteet eräänlaisena meta- tai yhteissääntelynä.

[22] Seppänen, 2024, s. 28
[23] Seppänen, 2024, s. 28
[24] HE 59/2002 vp., s. 29
[25] Seppänen, 2024, s. 29

2.3 Turvallisuus osana riskienhallintaa

Turvallisuus kattaa useita osa-alueita, kuten toiminnan turvallisuuden, tieto- ja kyberturvallisuuden, tietosuojan sekä digitaalisen turvallisuuden laajemmin, samoin kuin varautumisen ja toiminnan jatkuvuuden. Riskienhallinta on keskeinen osa näiden turvaamista ja organisaation päivittäisen toiminnan sekä vaatimustenmukaisuuden varmistamista. Sisäisen valvonnan tehtävänä on huolehtia toiminnan ja talouden laillisuudesta, tehokkuudesta sekä varojen ja omaisuuden turvaamisesta, mistä vastuu kuuluu johdolle. Sisäinen tarkastus arvioi puolestaan sisäisen valvonnan ja riskienhallinnan toimivuutta ja riittävyyttä.[26]

Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristön toiminta on turvattu ja luotettava. Käytännössä kyberturvallisuudella viitataan organisaatioiden ja yhteiskunnan digitalisoitumiseen liittyviin turvallisuushaasteisiin. Kyber-sanan merkitys liittyy usein sähköisessä muodossa olevan tiedon käsittelyyn. Kyberturvallisuus ei ole pelkästään ’’teknistä tietoturvaa’’, vaan käsitteenä se on todella moniulotteinen, ja kyberturvallisuuden merkitys vaikuttaa laajasti leikaten läpi yhteiskunnan organisaatioista kansalaisiin.[27]

Kyberturvallisuussääntelyssä (Kyberturvallisuuslaki 124/2025) riskiperusteisuus on erityisen vahvaa. Valtioneuvoston kanslian[28] ja lain valmistelutöissä[29] ilmenee, että sääntelyllä pyritään luomaan edellytykset parantaa yhteiskunnan kriittisten toimijoiden kyberturvaa sekä laitteiden ja ohjelmistojen sisäänrakennettua turvallisuutta. Digitalisoituminen tuo mukanaan uusia uhkia, mutta myös mahdollisuuksia esimerkiksi tiedustelutoimintaan, joka toteutetaan yhä kehittyneemmin. [30] Samalla

[26] Rousku, 2017, s. 13
[27] Andersson, 2024, s. 56
[28] Valtioneuvoston kanslia, 2024, s. 13–15
[29] HE 27/2025 vp., s. 8
[30] Valtioneuvoston kanslia, 2024, s. 13–15

toimintaympäristön muutos lisää ja monimuotoistaa kyberuhkia ja -riskejä, joihin vastaaminen edellyttää jatkuvaa uhka- ja riskiarviointia sekä riittävää resursointia. [31]

2.4 Tämän päivän riskienhallintaa

Riskienhallintaan ja henkilöstöturvallisuuteen on panostettu merkittävästi eri toimialoilla 2000-luvun aikana, mikä ilmenee muun muassa kansainvälisten salassa pidettävien tietojen vaihtoa ja niiden käsittelyä koskevien sopimusten määrän lisääntymisenä.[32] Valtio toteuttaa riskienhallintaa osana varautumista häiriötilanteisiin ja poikkeusoloihin, ja yhteiskunnan turvallisuusstrategian (2017) mukaan se perustuu riskien ja resurssien arviointiin sekä ennakoivaan viestintään. [33]

KPMG:n 2016 Global CEO Outlook -tutkimuksen mukaan kyberturvallisuus on noussut tutkimukseen osallistuneiden toimitusjohtajien haastatteluiden perusteella kansainvälisten yritysten yhdeksi merkittävimmäksi riskiksi. Muita merkittäviä riskejä kyberriskien jälkeen ovat lainsäädännölliset uhkat, uudet teknologiat, strategiset riskit ja geopoliittiset riski.[34]

Riskienhallinnan toimeenpano perustuu lainsäädäntöön, kuten NIS2-direktiiviin ((EU) 2022/2555), joka asettaa keskeisille toimijoille riskienhallinta- ja poikkeamaraportointivelvoitteita. Toimitusketjujen kyberturvallisuus varmistetaan riskienhallinnan keinoin joko lakisääteisesti tai sopimusperusteisesti.[35] Lisäksi julkisten palveluiden kyberturvallisuutta johdetaan ennakoivasti tilannetietoon perustuen, mikä korostaa jatkuvan riskienhallinnan ja valvonnan merkitystä.[36]

---

[31] Valtioneuvoston kanslia, 2024, s. 40
[32] Paasonen ym., 2022, s. 962
[33] Oikarinen, 2023, s. 284
[34] Andersson, 2018, s. 1
[35] Valtioneuvoston kanslia, 2024, s. 56–57
[36] Valtioneuvoston kanslia, 2024, s. 28

Erityisesti Suomessa henkilöstöturvallisuuden sääntelyn kehitykseen ovat vaikuttaneet Euroopan unionin sääntely sekä työelämän rakenteelliset uudistukset ja yritysten kokemat uudenlaiset turvallisuusuhat, kuten teollisuusvakoilu ja kyberrikokset. [37] Sääntelyssä on pitänyt ottaa huomioon myös Nato-jäsenyyden mukanaan tuomat turvallisuusvelvoitteet, minkä vuoksi esimerkiksi lain esitöissä on todettu tavoitteesta panna Suomessa täytäntöön Naton monenvälinen tietoturvallisuussopimus turvallisuusluokitellun tiedon suojaamiseksi, täydentäen näin olemassa olevaa kansallista sääntelyä. [38]

Riskienhallinnan vaikuttavuuden kannalta keskeistä on riittävä resursointi ja laaja-alainen yhteistyö julkisen hallinnon, yritysten ja muiden yhteisöjen välillä. Kyberturvallisuuden nykyinen resurssitilanne ei Valtioneuvoston kanslian [39]mukaan vielä vastaa tarpeita, mikä korostaa entisestään tehokkaan kansallisen ja kansainvälisen yhteistyön merkitystä. Myös henkilötietojen tietoturvaloukkaukset, jotka voivat aiheuttaa mittavia vaikutuksia ihmisten hyvinvointiin ja yhteiskunnan luottamukseen, alleviivaavat resurssien ja menettelytapojen kehittämisen tarpeen. [40]

[37] Paasonen ym., 2022, s. 962
[38] HE 4/2023 vp., s. 4–7
[39] Valtioneuvoston kanslia 2024, s. 29, 40
[40] Valtioneuvoston kanslia, 2024, s. 18, 54

3 Tietosuoja ja tietoturvallisuus riskienhallintavelvoitteena

Esimerkiksi Venäjän hyökkäys Ukrainaan on tehnyt Suomen turvallisuusympäristöstä pysyvästi epävakaamman. Suurvaltakilpailu ja sodan luoma jännite paljastavat riippuvuuden haavoittuvista toimitusketjuista. Suomen ja Viron välisen kaasuputken ja kaapelin vaurioituminen on osoittanut konkreettisesti kriittisen infrastruktuurin riskit, tässä tapauksessa veden alla. Tämä edellyttää panostamista infrastruktuurin ja palveluiden suojaamiseen, kyberturvallisuuteen, tärkeimpien hyödykkeiden turvaamiseen sekä nopeaan reagointiin hybridiuhkiin.[41]

Tietosuoja kytkeytyy moniin nyky-yhteiskunnassa pinnalla oleviin rinnakkaisiin ilmiöihin. Tietosuoja liittyy läheisesti sananvapauteen, viranomaisasiakirjojen julkisuuteen ja keskusteluun valtion turvallisuudesta ja siihen liittyvistä erilaisista valvontakeinoista. Tietosuoja nousee vääjäämättä esiin myös silloin, kun puhutaan digitaalisista palveluista ja niiden bisnesmalleista, datan jakamisesta ja hyödyntämisestä.[42]

3.1 Tietosuoja – perustana EU:n yleinen tietosuoja-asetus

Tietosuojalla tarkoitetaan yksityisyyden suojaamista henkilötietoja käsiteltäessä. Sillä ei kuitenkaan pyritä ensisijaisesti tietojen salaamiseen vaan suojaamaan yksilön oikeuksia. [43] Tietosuojariskillä tarkoitetaan sellaisia riskejä, joissa henkilötiedon luottamuksellisuus, eheys ja/tai käytettävyys ovat uhattuina.[44]

Tietosuoja-asetus (TSA) on ollut osa Euroopan unionin suurta tietosuojalainsäädännön uudistusta. Uudistus on ollut tarpeellinen informaatioteknologian nopean kehityksen ja jäsenvaltioiden hajanaisten henkilötietojen suojaa koskevien säädösten ja niiden epäyhtenäisen soveltamisen vuoksi.[45] EU :n yleisen tietosuoja-asetuksen (2016/679)

[41] Valtioneuvosto, 2024, s.4
[42] Meller, 2023, s.31
[43] Andersson, 2024, s. 49
[44] Andersson, 2018, s. 3
[45] HaVM 13/2018 vp, s.3

tarkoituksena on henkilötietojen suojaamisen lisäksi tukea vapauden, turvallisuuden, oikeusalueen ja talousunionin kehittämistä, taloudellista ja sosiaalista edistystä, talouksien lujittamista ja lähentämistä sisämarkkinoilla sekä luonnollisten henkilöiden hyvinvointia. [46] Keskeisenä tarkoituksena on henkilötietojen vapaan liikkuvuuden varmistaminen EU:n jäsenvaltioiden välillä ja henkilötietojen käsittelyä sääntelevän lainsäädännön yhdenmukaistaminen EU:n rajojen sisällä. Tietosuoja-asetuksen soveltaminen ei kuitenkaan rajoitu EU:n jäsenvaltioihin, vaan sen alueellinen soveltamisala ulottuu myös kolmansiin maihin. Tietosuoja-asetus jättää jossakin määrin jäsenvaltioille kansallista liikkumavaraa.[47]

Tietosuoja-asetus velvoittaa toteuttamaan asianmukaiset tekniset ja organisatoriset toimet tietoturvan varmistamiseksi, huomioiden uusin tekniikka ja kustannukset. Käsite *asianmukainen turvallisuustaso* ohjaa rankaisemaan organisaatioita, jotka eivät suojaa asiakastietojaan, mutta asiantuntijoiden mukaan se ei tosiasiassa edistä riittäviä parannuksia eikä takaa edes vähimmäistasoa. Epämääräisyys voi johtaa huolimattomuuteen ja tehottomaan tietoturvakulttuuriin, mikä lisää loukkausten riskiä. Myös *uusin tekniikka* -käsitettä on arvosteltu monitulkintaisuudesta. Sen avulla pyritään teknologianeutraalisuuteen, mutta epäselvyys voi johtaa vastuiden kiertämiseen ja velvoitteiden laiminlyöntiin.[48]

EU:n yleisen tietosuoja-asetuksen (2016/679) vuoksi Suomen tietosuojaan liittynyttä sääntelyä jouduttiin muuttamaan, muun muassa henkilötietolaki korvattiin tietosuojalailla (1050/2018). Laki rikoslain 38 luvun 9 ja 10 §:n muuttamisesta (2018/1051) tuli voimaan 1.1.2019. Rikoslain 38 luvun 9 §:n henkilörekisteririkos muutettiin tietosuojarikokseksi. Laajaa henkilötietojen käsittelyä koskenutta kriminalisointia ei enää katsottu perustelluksi, koska tietosuoja-asetuksen mukaisten

[46] Korpisaari ym., 2022, s.41
[47] Lång ja Taka, 2019, s. 64
[48] Akatyev, Han, Hwang, Jang, Kim D., Kim J., Park, Shin, & Yu, 2018, s. 95–96.

hallinnollisten seuraamusmaksujen myötä seuraamusjärjestelmä muuttui perustavanlaatuisesti. [49]

Oikeusasiamiehelle tehdyssä kantelussa [50] käsitellään Vastaamon tietomurtokokonaisuuteen liittyvässä rikosprosessissa, onko tietosuojarikoksella asianomistajia ja miten asianomistaja-asema määräytyy. Syyttäjän mukaan rikoslain 38 luvun 9 §:ssä säädetty tietosuojarikos on luonteeltaan abstrakti vaarantamisrikos, jossa ei välttämättä ole asianomistajaa. Rikoksen tunnusmerkistö täyttyy, kun henkilötietojen käsittelyn turvallisuudessa laiminlyödään EU:n yleisen tietosuoja-asetuksen ja tietosuojalain velvoitteet. Syyttäjän käsityksen mukaan tässä tapauksessa toimitusjohtajan toiminta, eli tietoturvaloukkauksen jälkeen puutteelliset toimet tietojen suojaamiseksi, ei kohdistunut välittömästi keneenkään yksittäiseen henkilöön, eikä siten synnyttänyt asianomistaja-asemaa.

Kantelija on vastineessaan esittänyt, että henkilöt, joiden tietoja ei ollut asianmukaisesti suojattu, olisi katsottava asianomistajiksi aineellisoikeudellisen määritelmän perusteella. Hän on vedonnut EU-tuomioistuimen ratkaisuun C-340/21[51], jossa todettiin, että pelkkä pelko tietojen väärinkäytöstä voi muodostaa aineettoman vahingon. [52] Näin ollen rekisteröidyllä olisi oikeus esittää yksityisoikeudellisia vaatimuksia.

Ratkaisussa kuitenkin todettiin, että syyte kohdistui ainoastaan tietosuojarikokseen ja toimitusjohtajan laiminlyönteihin tietomurron tultua ilmi. Itse tietomurtoa ja tietojen levittämistä koskevat rikosepäilyt käsitellään erikseen, ja niissä rekisteröidyt voivat olla asianomistajan asemassa. Näin ollen tässä vaiheessa ei ollut perusteita katsoa, että tietosuojarikos olisi välittömästi loukannut rekisteröityjen oikeuksia.

Kokonaisuutena ratkaisu nojaa rikoslain 38:9 §:ään sekä yleisen tietosuoja-asetuksen keskeisiin säädöksiin, erityisesti 5 ja 32 artiklan tietoturvavelvoitteisiin. Asianomistaja-asema arvioidaan sen mukaan, kohdistuuko teko suoraan rekisteröidyn oikeuksiin vai jääkö rikos abstraktiksi vaarantamiseksi.[53]

[49] Paasonen ym., 2021, s. 971
[50] EOAK/2261/2023 Oikeusasiamiehen vastaus kanteluun asianomistaja-asema Vastaamo-asiassa, s.15–19
[51] C-340/21, 2023, luku IV ratkaisuehdotus
[52] C-340/21, 2023, luku IV ratkaisuehdotus
[53] EOAK/2261/2023 Oikeusasiamiehen vastaus kanteluun asianomistaja-asema Vastaamo-asiassa, s.15–19

Rikosoikeudellinen vastuu tulee kyseeseen vain tilanteissa, joissa lainvastainen henkilötietojen käsittely ei ole tietosuoja-asetuksen nojalla hallinnollisten seuraamusmaksujen piirissä. Säännös tuleekin sovellettavaksi ainoastaan tilanteessa, jossa henkilö ei toimi rekisterinpitäjän tai henkilötietojen käsittelijän ominaisuudessa. [54] *Rekisterinpitäjä* on taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot, kun taas *henkilötietojen käsittelijä* käsittelee tietoja rekisterinpitäjän lukuun tämän ohjeiden mukaisesti. Keskeinen osapuoli on se luonnollinen henkilö, *ihminen*, jonka henkilötietoja käsitellään. Hänestä asetuksen suomenkielinen käännös käyttää nimitystä *rekisteröity*.[55]

Tietosuojaa määrittävässä 21 artiklassa viitataan henkilötietoja käsittelevän virkamiehen velvollisuuksiin siten, kuin niitä on säännelty Euroopan parlamentin ja neuvoston antamassa asetuksessa (EY) N:o 45/2001. Henkilötietojen käyttöä laittomiin tarkoituksiin tai tietojen välittämistä niihin oikeuttamattomille on artiklan mukaan ”vältettävä”. Kansallisessa oikeudessa voidaan vastaavasti viitata lakiin viranomaisten toiminnan julkisuudesta (621/1999), jossa säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista. [56]

Lähtökohtana on, että esimerkiksi yritys saa käsitellä omia tietojaan vapaasti ja päättää niiden käytöstä. Henkilötietojen suhteen tilanne on päinvastainen. Oletusarvona niiden käsittely on kiellettyä, mutta voidaan sallia perustelluista syistä. Yrityksen on helppo löytää syitä henkilötietojen käsittelyyn. Pelkkä asiakassuhde oikeuttaa käsittelemään siihen liittyviä tietoja, mutta silloinkaan yritys ei saa kerätä eikä käsitellä muita kuin toiminnan kannalta tarpeellisia tietoja. Käsiteltävien tietojen on oltava virheettömiä ja ajan tasalla. Lisäksi asiakkaille on järjestettävä mahdollisuus tarkistaa tietonsa ja oikeus

[54] Paasonen ym., 2021, s. 979
[55] Korpisaari ym., 2022, s.34
[56] Hautamäki, 2004, s. 170

pyytää niiden poistamista. Kun asiakassuhde päättyy ja tiedot muuttuvat tarpeettomiksi, ne pitää poistaa. [57]

Tietosuoja-asetus tarjoaa organisaatioille hyvät edellytykset toimia vastuullisina rekisterinpitäjinä ja henkilötietojen käsittelijöinä. Datan käyttö on uusien innovaatioiden mahdollistaja, kun sitä osataan hyödyntää kestävällä tavalla. Pitkällä tähtäimellä datan vastuullisella hyödyntämisellä on myös suuri taloudellinen arvo organisaatioille. Useissa lausunnoissa katsottiin, että yleinen tietosuoja-asetus on vahvistanut yksityiselämän suojaa ja rekisteröityjen asemaa, lisännyt rekisteröidyn oikeuksia ja selkeyttänyt rekisteröityjen oikeuksien käyttämiseen liittyviä prosesseja. [58]

3.1.1 Tietosuoja osana perusoikeuksia ja oikeusperiaatteita

Yleisen tietosuoja-asetuksen, kuten aikaisemman kansallisen sääntelyn, yhtenä periaatteena on tietojen käsittelyn suunnitelmallisuus käsittelyyn liittyvien riskien ja niiden edellyttämien suojaustoimenpiteiden toteuttamiseksi. Tietojen käsittely tulisi suunnitella palvelemaan ihmistä sekä suhteessa muihin perusoikeuksiin. [59] Perus- ja ihmisoikeudet on turvattu Suomessa perustuslaissa.[60] Valtion ja kuntien viranomaisten tietohallinnon osalta tietosuoja-asetuksen 5 artiklan käsittelyä koskevat periaatteet tietojen käsittelyn lainmukaisuudesta, asianmukaisuudesta ja rekisteröidyn kannalta läpinäkyvästi sekä tietojen käsittelyn minimointi muodostavat henkilötietojen suunnitteluvastuiden ydinalueen. [61]

Läpinäkyvyyden periaatteeseen (TSA 5 artikla) kuuluu, että ihmiset saavat tietää, mitä ja miten heitä koskevia henkilötietoja kerätään, käytetään tai muutoin käsitellään. Tämän takia henkilötietojen käsittelyyn liittyvien tietojen ja viestinnän täytyy olla helposti saatavilla ja ilmaistu selkeällä ja yksinkertaisella kielellä. Läpinäkyvyys ja avoin

[57] Järvinen, 2022, s.25
[58] Kantonen ja Pohjalainen, 2024, s. 14
[59] Oikarinen, 2023, s. 291
[60] HE 1/1998 vp., s. 78
[61] Oikarinen, 2023, s. 292

informointi parantavat tietojen käsittelyn lainmukaisuutta, koska rekisterinpitäjä joutuu informointivelvoitetta toteuttaessaan samalla tarkastelemaan tietosuojakäytäntöjään.[62] Monet viranomaisten hallussa olevat julkiset asiakirjat sisältävät henkilötietoja. Niihin voi kuulua myös yksityiselämän piiriin kuuluvia tietoja. Jos asiakirja on viranomaisten toiminnan julkisuudesta annetun lain (621/1999; julkisuuslaki) mukaan julkinen, viranomainen on pyydettäessä velvollinen antamaan sen. [63] Julkisuusperiaatteen mukainen tiedonsaantioikeus mainitaan perusoikeutena lain esitöissä, ja sitä voidaan rajoittaa vain välttämättömistä syistä. [64]

Julkisuuslainsäädäntö ei suoranaisesti määrittele, mitä tietoja saa julkaista, vaan arviointi tehdään muun lainsäädännön, kuten tietosuoja- ja rikoslain, perusteella. Esimerkiksi julkisista asiakirjoista peräisin olevien tietojen laajamittainen julkaiseminen voi olla tietosuojalainsäädännön vastaista. Lisäksi yksityiselämää koskevien tietojen levittäminen voi täyttää rikoslain (39/1889, RL) 24 luvun 8 tai 8 a §:ssä säädetyn yksityiselämää loukkaavan tiedon levittämisen tunnusmerkistön. Kaikki julkinen tieto ei siis ole sellaisenaan julkaistavissa, vaikka tiedon alkuperä ja sen julkisuus voivat vaikuttaa arviointiin. [65]

Euroopan ihmisoikeustuomioistuimen (EIT) mukaan henkilötietojen suoja on olennainen osa EIS 8 artiklan takaamaa yksityis- ja perhe-elämän suojaa. Artiklan mukainen yksityiselämän suojaaminen edellyttää muun muassa sitä, että ainakin yksityiselämän suojan alaan kuuluvien henkilötietojen keräämisestä, käyttämisestä ja säilyttämisestä säädetään riittävän täsmällisesti. [66] Yksinkertaistaen tietosuoja voidaan nähdä osana yksityisyyden suojaa, mutta pelkkä alisteinen asema ei kuitenkaan tee sille oikeutta. Tietosuoja ulottuu nimittäin yksityisyyden ohella myös muiden perus- ja ihmisoikeuksien turvaamiseen [67] Tietosuojaan läheisesti liittyviä perusoikeuksia ovat yksityiselämän

[62] Korpisaari ym., 2022, s.29
[63] Korpisaari ym., 2022, s.18
[64] HE 30/1998 vp., s. 9
[65] Korpisaari ym., 2022, s.18
[66] Korpisaari ym., 2022, s. 11
[67] Keller, 2023, s. 58

suojan lisäksi oikeus kunniaan (PL 10§), oikeus yhdenvertaiseen kohteluun (PL 6§), oikeus henkilökohtaiseen koskemattomuuteen (PL7§), oikeus ihmisarvoiseen kohteluun (EIS 2 artikla), oikeus turvallisuuteen (EIS 5 artikla) sekä yhdenvertaisuus ja syrjinnän kielto ja oikeus vaikuttaa itseään koskeviin asioihin (Yhdenvertaisuuslaki 8§), uskonnonvapaus ja omantunnon vapaus (PL 11§), sananvapaus ja julkisuus (PL12§). [68]

TSA:n 1 artiklan 2 kohdan mukaan asetuksen tarkoituksena on suojella luonnollisten henkilöiden perusoikeuksia ja -vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan. Esimerkiksi Vastaamon tietomurtotapaus osoitti konkreettisesti, miten henkilötietojen vaarantuminen voi johtaa perusoikeuksien loukkauksiin. Tapauksessa yksityis- ja perhe-elämän suoja (EIS 8 artikla, PL 10 §) vaarantui, potilaat joutuivat alttiiksi sosiaaliselle leimautumiselle ja syrjinnälle, ja heidän asemansa työelämässä saattoi heikentyä. Tapaukseen kytkeytyivät näin myös kunniaan ja ihmisarvoon liittyvät ulottuvuudet sekä yhdenvertaisuuden ja syrjinnän kiellon (PL 6 §, Yhdenvertaisuuslaki 8 §) periaatteet.

3.1.2 Tietosuojaan kytkeytyvät haasteet

Tietosuoja-asetuksen periaatelähtöisyys yhdistettynä ohjeistusten niukkuuteen ja oikeuskäytännön puutteeseen hankaloittavat kuitenkin organisaatioiden työtä tietosuojakysymysten parissa. Ilman konkreettisia tulkintaohjeita sääntelyn 99 artiklaa jäävät kaukaisiksi ja vaikeaselkoisiksi. Abstraktit ilmaisut jäävät kaipaamaan syvyyttä ja sisältöä. [69]

Kantosen ja Pohjalaisen [70] mukaan tietosuojaan liittyvät velvoitteet aiheuttavat merkittävää kuormitusta erityisesti julkisella sektorilla. Tietosuoja-asetuksen noudattaminen vaatii vaativaa asiantuntijatyötä, mikä lisää kustannuksia. Lisäksi

[68] Keller, 2023, s. 88
[69] Lång ja Taka, 2019, s. 71
[70] Kantonen ja Pohjalainen 2024, s. 11

tietosuojasääntelyä, mukaan lukien EU:n asetus, kansallinen laki ja erityislait, pidettiin monimutkaisena ja vaikeasti hallittavana kokonaisuutena. Erityisesti julkisen sektorin toimijat nostivat esiin lainsäädännön pirstaleisuuden, ja vaikeuden yhteensovittaa tietosuojalainsäädäntöä esimerkiksi julkisuuslain kanssa.

Erityisesti henkilötietoja kattaviin lain viranomaisten toiminnan julkisuudesta (621/1999) (jäljempänä julkisuuslaki) mukaisiin tietopyyntöihin vastaaminen on koettu haastavaksi. Haasteiden katsottiin johtuvan oikeuksien vastakkaisista tavoitteista, julkisuuslain päivittämistarpeesta sekä lainsäädännön tulkinnanvaraisuudesta. Julkisuuslain ja tietosuojalainsäädännön yhteensovittamisen todettiin vievän resursseja ja edellyttävän erityistä asiantuntemusta ja soveltamishankaluuksien katsottiin jossain määrin johtaneen ylivarovaisiin tulkintoihin.[71]

Henkilötietolainsäädännön hajanaisuus on aiheuttanut epätietoisuutta yksityisyyttä ja julkisuutta koskevan sääntelyn keskinäisistä suhteista sekä eri viranomaisten toimivaltuuksista informaation käsittelyssä. Lisäksi sääntelyn pirstaleisuus vaikeuttaa tietosuojasääntelyn sisällöllistä osaamista ja oikeaa soveltamista ja siten myös tehokkaaseen informaatiohallintoon siirtymistä.[72] Kritiikkiä sai myös kansallinen ratkaisu, jonka mukaan viranomaisille ei voida määrätä hallinnollista seuraamusmaksua tietosuoja-asetuksen rikkomisesta.[73]

3.2 Tietoturvallisuus

Tietosuojalla tarkoitetaan henkilötietojen suojaamista. Suomen kielen sana *tietosuoja* muistuttaa läheisesti sanaa *tietoturva*, joten ne menevät helposti sekaisin. Molemmat liittyvät sähköisessä muodossa olevien tietojen suojaamiseen, mutta suojan kohde ja tarkoitus ovat erilaisia:

[71] Kantonen ja Pohjalainen, 2024, s. 30
[72] Korpisaari ym., 2022, s. 3
[73] Kantonen ja Pohjalainen 2024, s. 11

- **Tietoturva** suojaa yrityksen omia tietoja, ja sen tavoitteena on yrityksen toiminnan turvaaminen.
- **Tietosuoja** on henkilötietojen suojaamista. Kohteena on ihminen itse, ja tavoitteena on turvata hänen yksityisyyttään, joka on perusoikeus.[74]

Tietosuojalla on myös läheinen liitäntä tietoturvaan. Tietoturva on osa tietosuojaa, ja se varmistaa omalta osaltaan, että henkilötietojen suoja toteutuu asianmukaisella tavalla. Toki tietoturva on myös itsessään laajempi konsepti, eikä se kata pelkästään henkilö-tietojen suojaamista vaan käsittää myös laajemmin yritykselle tai yksilölle tärkeiden tietojen suojan. Suojan piiriin kuuluu siis henkilödatan lisäksi esimerkiksi yrityssalaisuudet. [75] Lain esitöissä on määritelty tietoturvauhan tarkoittavan tyypillisesti ulkopuolelta viestintäverkkoon tai -palveluihin kohdistuvia uhkia, joilla pyritään esimerkiksi saamaan selville käyttäjien tietoja tai ottamaan haltuun tietokoneita palvelunestohyökkäysten toteuttamiseksi taikka ei toivottujen suoramarkkinointiviestien lähettämiseksi.[76] Näkökulma on kyberpainotteinen. [77]

Uutisotsikoissa käytetään sanoja ”kyberturvallisuus” ja ”kyberhyökkäys”, koska ne kuulostavat mediaseksikkäämmiltä kuin vanha ”tietoturvallisuus” tai tylsä ”verkkohyökkäys”. Yleensä kyse on kuitenkin samasta asiasta. [78] Järvinen[79] käyttää kyberturvallisuutta viittaamaan siihen tietoturvaan, joka koskee arjen infrastruktuuria ja maanpuolustusta. Sähkö, vesi, liikenteen ohjaus, terveydenhuolto, kauppa, logistiikka ja monet muut asiat toimivat tietokoneiden ja verkkojen varassa. Jos niiden tietoturva pettää, kyse ei ole vain menetetyistä tiedostoista tai taloudellisista tappioista, vaan vaarassa ovat ihmisten hyvinvointi ja henki.[80]

---

[74] Järvinen, 2022, s.25
[75] Keller, 2023, s. 30
[76] HE 48/2008 vp., s.29
[77] Andersson, 2024, s. 52
[78] Järvinen, 2022, s.16
[79] Järvinen, 2022, s.16
[80] Järvinen, 2022, s.16

Tietoturvallisuudesta ei säädetä itsenäisenä lakina, mutta lainsäädännössä on mainintaa tietoturvasta eri lakien kautta, jotka koskevat tietojen suojaa, tietojärjestelmien turvallisuutta sekä yksityisyyden ja kansallisen turvallisuuden turvaamista. Suomessa keskeisiä lakeja ovat tietosuojalain (1050/2018) lisäksi laki sähköisen viestinnän palveluista (917/2014) ja laki julkisen hallinnon tiedonhallinnasta (906/2019), jotka asettavat velvoitteita viestintäpalvelujen tarjoajille ja viranomaisille tietoturvan varmistamiseksi.[81]

Sähköisen viestinnän laissa 272 § ja 273 § velvoittavat toimijat torjumaan häiriöitä ja suojaamaan viestintää teknisin toimenpitein, kuitenkin yksityisyyttä ja viestintäsalaisuutta kunnioittaen. Tarvittaessa palvelut tai laitteet, jotka aiheuttavat häiriöitä, voidaan irrottaa verkosta.[82] Laki julkisen hallinnon tiedonhallinasta (906/2019) 13 § korostaa, että tietoturva on otettava huomioon koko tiedon ja järjestelmien elinkaaren ajan. Lisäksi laki velvoittaa mm. turvallisuusluokitteluun (18§), henkilöstön luotettavuuden arviointiin (12§) ja tietoturvavaatimusten huomioimiseen hankinnoissa. Lain tavoitteena on, että tietoon perustuvat julkiset palvelut ja toiminta on mahdollista toteuttaa entistä laadukkaammin, tuloksellisemmin ja tehokkaammin laadukkaan tiedonhallinnan tukemana. Laadukas tiedonhallinta edistää myös tietosuojaa, tietoturvallisuutta ja tietoaineistojen vastuullista hyödyntämistä. Viranomaisten tietoaineistojen hallinnalla edistettäisiin myös julkisuusperiaatteen toteutumista.[83]

EU:ssa on reagoitu muuttuneeseen kybertoimintaympäristöön ottamalla käyttöön Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 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 (NIS2-direktiivi). NIS2-direktiivi

[81] HE 9/2018 vp., s. 4; HE 221/2013 vp., s.7; HE 284/2018 vp., s. 8
[82] HE 221/2013 vp., S. 144–145
[83] HE 284/2018 vp., s.30

yhdenmukaistaa yhteiskunnan kriittisten sektoreiden kyberturvallisuusriskienhallinta- ja raportointivelvoitteiden vähimmäistasoja.[84] Suomi toimeenpanee velvoitteet osana kansallista lainsäädäntöä muun muassa 2025 voimaan tulleella kyberturvallisuuslailla (127/2025).[85]

EU:n NIS2-direktiivi vahvistaa erityisesti kriittisten toimialojen kyberturvallisuutta. Artikla 21 edellyttää kattavaa riskienhallintaa ja toimenpiteitä, kuten varmuuskopiointia, henkilöstöturvaa ja toimitusketjun hallintaa.[86] Artikla 23 taas velvoittaa ilmoittamaan merkittävistä kyberpoikkeamista viranomaisille nopeasti, ja tarvittaessa myös tiedottamaan käyttäjiä.[87]

NIS2-direktiivin lisäksi yleinen tietosuoja-asetus asettaa velvoitteet henkilötietojen käsittelyyn liittyvien tietoturvaloukkausten ilmoittamisesta. Jos tietoturvaloukkaus tapahtuu, 33 artikla velvoittaa ilmoittamaan siitä valvontaviranomaiselle 72 tunnin kuluessa, ellei riskiä katsota vähäiseksi. 34 artiklan mukaan myös rekisteröityjä on informoitava ilman aiheetonta viivytystä, mikäli loukkaus todennäköisesti aiheuttaa korkean riskin heidän oikeuksilleen tai vapauksilleen.[88] Esimerkiksi Vastaamon tietomurrossa selvisi jälkeenpäin, että jo vuosina 2018 ja 2019 psykoterapiakeskuksessa tapahtui mahdollisia tietoturvaloukkauksia, joita ei raportoitu.[89] Vastaamon toimitusjohtajan Ville Tapion mukaan IT-järjestelmänvalvojat olivat saattaneet poistaa palomuurin käytöstä ilman VPN-suojaa. Näin ollen ainoaksi suojaksi jäi salasana palvelimelle.[90] Vastaamon 2020 tietomurron ilmitulon myötä selvinneet aiemmat tietoturvaloukkaukset jäivät tapahtumahetkellä niin valvontaviranomaisen kuin rekisteröityjen tietämättömiin ja rikkoi räikeästi yllä mainittuja artikloita.[91]

---

[84] Valtioneuvoston päätös huoltovarmuuden tavoitteista (568/2024), 2024, s.8
[85] HE 57/2024 vp., s. 7
[86] HE 57/2024 vp., s. 15
[87] HE 57/2024 vp., s. 17
[88] Järvinen, 2022, s.28
[89] Ghanbari, H., & Koskinen, K., 2024, s. 4
[90] Looi ym., 2025, s.108
[91] TSV 07.12.2021, dnro 1150/161/2021; luku 2.2.5. tietoturvaloukkauksesta ilmoittaminen

Nykykäytännön ongelma on erityisesti riski siitä, että yleisessä mittakaavassa merkityksellisiä tietoturvaloukkauksia jää vaille viranomaisten tarkoituksenmukaista ja perusteltua huomiota.[92] Koska nykyään valtaosa henkilötietojen käsittelystä tapahtuu digitaalisesti, asianmukaisesti hoidetulla tietoturvalla on valtava merkitys tietosuojan ja yksityisyyden suojan toteutumisessa. Suurin osa tietosuojaa koskevasta uutisoinnista koskee nimenomaan tietoturvan pettämistä eli tietoturvaloukkauksia. Tietoturva-puutteista johtuneet tietoturvaloukkaukset korostuvat myös tietosuojaviranomaisten ratkaisukäytännössä.[93]

Kansallinen tietosuojalaki pohjautuu suoraan tietosuoja-asetukseen ja täydentää sen soveltamista Suomessa. [94] Tietosuoja-asetuksen 32 artikla edellyttää, että rekisterinpitäjän ja käsittelijän on toteutettava riittävät tekniset ja organisatoriset toimet henkilötietojen suojaamiseksi. Näitä ovat esimerkiksi salaus, järjestelmien vikasietoisuus ja jatkuva toiminnan arviointi. Turvallisuustason tulee vastata käsittelyyn liittyviä riskejä. Erityisesti TSA 9 artikla kieltää arkaluontoisten tietojen käsittelyn ilman erityisiä suojatoimia.

> Tietosuojavaltuutetun ratkaisussa[95] (15.11.2022, 4022/171/22) Terveydenhuollon toimijan toimitusjohtajalta varastettiin tietokonelaukku, joka sisälsi kannettavan tietokoneen, kaksi ulkoista kiintolevyä sekä henkilötietoja sisältäviä paperiasiakirjoja. Tapahtuman seurauksena arviolta noin 3 000 rekisteröidyn tiedot saattoivat vaarantua. Loukkaus koski erityisesti terveystietoja, jotka kuuluvat erityisesti EU:n yleisen tietosuoja-asetuksen mukaan erityisiin henkilötietoryhmiin ja edellyttävät erityistä suojaamista.
>
> Apulaistietosuojavaltuutetun arvioinnissa keskeinen oikeudellinen kysymys oli, oliko rekisterinpitäjä toteuttanut henkilötietojen suojaamiseksi riittävät tekniset ja organisatoriset toimenpiteet yleisen tietosuoja-asetuksen 32 artiklan mukaisesti. Artikla edellyttää, että henkilötietojen käsittelyssä otetaan huomioon käsittelyyn

[92] Lång ja Taka, 2019 s. 60
[93] Keller, 2023, s. 56
[94] HE 9/2018 vp., s. 4
[95] TSV 15.11.2022, dnro 4022/171/22

liittyvät riskit ja toteutetaan niiden perusteella asianmukaiset suojatoimet, kuten tietojen salaus.

Arvionsa perusteella apulaistietosuojavaltuutettu katsoi, että rekisterinpitäjä ei ollut toiminut asetuksen edellyttämällä tavalla. Pelkkä salasanasuojaus ei riittänyt estämään pääsyä tietokoneelle tallennettuihin tietoihin, sillä salaamattomaan massamuistiin on mahdollista päästä useilla teknisillä menetelmillä. Ulkoiset kiintolevyt olivat vieläkin haavoittuvampia, koska ne voitiin liittää suoraan toiseen laitteeseen ja niiden sisältö oli helposti tarkasteltavissa. Myös paperiasiakirjojen käsittelyä pidettiin tietoturvan kannalta puutteellisena, sillä ne sisälsivät arkaluonteisia potilastietoja.

Näin ollen rekisterinpitäjän menettely katsottiin yleisen tietosuoja-asetuksen 32 artiklan vastaiseksi. Apulaistietosuojavaltuutettu antoi rekisterinpitäjälle huomautuksen yleisen tietosuoja-asetuksen 58 artiklan nojalla. Tapauksen perusteella korostuu, että erityisesti terveydenhuollon toimijoiden on huolehdittava henkilötietojen suojaamisesta korkeatasoisesti ja otettava käyttöön esimerkiksi laitteiden ja tietovälineiden salaus, sillä muutoin rekisteröityjen yksityisyys voi vaarantua vakavasti.[96]

Sosiaali- ja terveystietojen toissijaisen käytön laissa (552/2019) eli toisiolaissa sovelletaan yleistä tietosuoja-asetuksen 1 §, jossa henkilötietoja käsitellään muissa käyttötarkoituksissa kuin ne on alun perin tallennettu. Tällaisia muotoja ovat esimerkiksi tilastointi, opetus ja tutkimus. Toisiolain 18 §:ssä määritellään yleiset tietoturvavaatimukset, kun henkilötietoja käsitellään kyseisen lain nojalla. Tärkeää on varmistaa tietoturvallisuus riskienhallinnalla, pääsynhallinnalla, aktiivisella valvonnalla sekä noudattamalla tietoturvallisuuden ja tietosuojan toteutuksesta ja valvonnasta vastaavan viranomaisen määräyksiä ja ohjeita. Erityistä huomiota on kiinnitettävä käyttörajoitusten sekä salassapitovelvoitteen toteuttamiseen.

Itä-Suomen Hallinto-oikeuden[97] (27.09.2023 2139/2023) tapauksessa arvioitiin, oliko Findata voinut velvoittaa tutkijan siirtämään tutkimusaineistonsa CSC:n

[96] TSV 15.11.2022, dnro 4022/171/22

[97] Itä-Suomen HAO 27.09.2023, dnro 2139/2023

auditoimaan Sensitive Data Desktop -käyttöympäristöön, vaikka aineisto perustui ennen sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (toisiolaki) voimaantuloa myönnettyihin tietolupiin. Tutkija katsoi nykyisen käyttöympäristönsä olevan riittävän tietoturvallinen ja siirtovaatimuksen vaarantavan tutkimuksen jatkumisen.

Hallinto-oikeus katsoi, että toisiolain tietoturvavaatimukset koskevat myös aiemmin myönnettyihin lupiin perustuvaa aineistoa, koska lain siirtymäsäännösten tarkoituksena on ollut turvata tutkimuksen jatkuminen vain määräajan. Toisiolain 18, 20 ja 25 §:ssä säädetään, että aineistoa saa käsitellä ainoastaan tietoturvallisessa käyttöympäristössä, ja valittaja ei ollut osoittanut oman ympäristönsä täyttävän nämä edellytykset.

Ratkaisussa painotettiin myös perusoikeuksien tasapainottamista. Tietoturvallisen käyttöympäristön vaatimus turvaa perustuslain 10 §:ssä säädetyn yksityiselämän suojan, eikä se ollut ristiriidassa tutkimuksen vapautta koskevan perustuslain 16 §:n 3 momentin kanssa. Lisäksi hallinto-oikeus totesi, että siirron työmäärällä tai kustannuksilla ei ollut merkitystä lain soveltamisen kannalta.

Näin ollen hallinto-oikeus hylkäsi valituksen ja katsoi Findatan voineen edellyttää aineiston siirtämistä tietoturvalliseen käyttöympäristöön. Ratkaisu oli lainvoimainen ja perustui yleisen tietosuoja-asetuksen 9 artiklan 1 ja 2 kohdan j alakohtaan, toisiolain 18, 20, 25, 38 ja 60 §:ään sekä perustuslain 10 ja 16 §:ään.[98]

[98] Itä-Suomen HAO 27.09.2023, dnro 2139/2023

4 Johtopäätökset

Riskienhallinta on olennainen osa organisaatioiden tietoturvan kehittämistä ja ylläpitämistä. Sitä tukevat erilaiset viitekehykset ja lainsäädäntö, jotka ohjaavat riskiperusteista toimintaa.[99] Tietoturvan sääntelyjärjestelmässä riskiä on käsitelty monitahoisesti joko tietoturvallisuuteen tai kyberturvallisuuteen liittyvinä riskeinä taikka tietosuojaan liittyvinä henkilötietojen käsittelyn riskeinä.[100] Riskienhallinta toteutuu käytännössä tietoturvasuunnitelmien ja -toimenpiteiden muodossa.[101] Tarve turvallisuuden kehittämiselle on kasvanut toiminnan digitalisoituessa ja teknologisten sekä yhteiskunnallisten uhkien muuttuessa nopeasti.[102] Esimerkiksi tietosuojaan ja tietoturvallisuuteen liittyvien lainsäädäntöuudistusten myötä erilaiset julkisen ja yksityisen sektorin toimijat ovat nykyisin velvoitettuja arvioimaan tietojenkäsittelyynsä liittyviä riskejä.[103]

Tietosuojan ja tietoturvan toteuttaminen edellyttää nykyisessä sääntely-ympäristössä ennen kaikkea riskiperusteista ajattelua. Tietosuoja-asetus (asetus (EU) 2016/679, GDPR), tietosuojalaki ja NIS2-direktiivi ((EU) 2022/2555) eivät tarjoa yksityiskohtaisia ratkaisuja, vaan velvoittavat organisaatiot itse arvioimaan toimintaansa liittyvät riskit ja mitoittamaan suojaustoimet niiden mukaisesti. Tämä korostaa johdon vastuuta ja ennakoivaa otetta, jossa tietosuoja ja tietoturva eivät ole kertaluonteisia velvollisuuksia, vaan jatkuvaa riskien tunnistamista, arviointia ja hallintaa.[104]

Riskienhallintavelvoite eroaa täsmällisistä lakisääteisistä velvoitteista siten, että se ei anna valmiita ohjeita yksittäisten riskien torjumiseksi, vaan siirtää vastuun riskien tunnistamisesta, arvioinnista ja hallinnasta toimijalle itselleen.[105] Jos laki määrittää

[99] Andersson, 2018, s. 3
[100] Andersson, 2024, s. 55
[101] Voutilainen, 2006, s. 21
[102] Rousku, 2017, s. 3
[103] Seppänen, 2024, s. 2
[104] Rousku, 2017, s. 11, s. 12
[105] Seppänen, 2024, s. 28

tarkasti, mitä toimenpiteitä tietyssä tilanteessa on tehtävä, kyse ei enää ole riskienhallintavelvoitteesta, vaan konkreettisesta, ennalta määrätyn sisällön omaavasta lakisääteisestä velvoitteesta.[106]

Yhtenä keskeisenä periaatteena tietosuoja-asetuksessa on riskiperustainen lähestymistapa, johon liittyy riskien arviointi ja ongelmien ennaltaehkäisy. Esimerkiksi TSA 25 artiklan mukaan riskit on otettava huomioon sisäänrakennettua ja oletusarvoista tietosuojaa toteutettaessa. TSA 32 ja 24 artiklat vaativat, että niin rekisterinpitäjän kuin henkilötietojen käsittelijänkin on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. TSA 34 artikla puolestaan edellyttää, että ihmisille on ilmoitettava, jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin heidän oikeuksilleen ja vapauksilleen.[107]

TSA 35 artikla velvoittaa rekisterinpitäjää arvioimaan henkilötietojen käsittelyn vaikutuksia yksilön oikeuksiin ennen käsittelyn aloittamista.[108] Henkilötietojen tietoturva on varmistettava kaikissa olosuhteissa ja koko tiedon elinkaaren ajan. Mitä laajempaa henkilötietojen käsittely on, sitä enemmän tulee puntaroida mahdollisia riskejä ja pyrkiä ennaltaehkäisemään niiden toteutumista.[109] Erityisesti laajassa tai arkaluonteisessa käsittelyssä yritykselle asetetaan velvoite nimittää tietosuojavastaava. Hänen roolinsa liittyy sisäiseen ohjaukseen ja neuvontaan, mutta varsinainen vastuu tietosuojan toteutumisesta on toimivalla johdolla ja hallituksella.[110] TSA 5 artikla määrittelee henkilötietojen käsittelyn perusperiaatteet, joka käsittää lainmukaisuuden, tarkoitussidonnaisuuden, minimoinnin, täsmällisyyden, säilytyksen rajoittamisen ja turvallisuuden. Niiden kautta riskienhallinta ja rekisteröidyn perusoikeudet toteutuvat. Rekisterinpitäjällä on lisäksi osoitusvelvollisuus, mikä tekee periaatteista konkreettisia velvoitteita eikä vain ohjaavia linjauksia.

---

[106] Seppänen, 2024, s. 29
[107] Korpisaari ym., 2022, s. 30
[108] Oikarinen, 2023, s. 293
[109] Järvinen, 2022, s.26
[110] Järvinen, 2022, s.26

Tutkimuksen tulokset osoittavat, että riskiperusteinen lähestymistapa on keskeinen tietosuojan ja tietoturvan sääntelyssä. EU:n yleinen tietosuoja-asetus (asetus (EU) 2016/679, GDPR), tietosuojalaki ja NIS2-direktiivi ((EU) 2022/2555) ja kyberturvallisuuslaki edellyttävät, että organisaatiot arvioivat itse tietojenkäsittelyyn liittyvät riskit ja mitoittavat suojatoimenpiteet niiden mukaan. Lainsäädäntö ei yksityiskohtaisesti määrää teknisiä tai organisatorisia toimenpiteitä, vaan korostaa toimijoiden omaa harkintaa ja vastuuta. Tämä riskiperusteisuus konkretisoituu erityisesti silloin, kun käsitellään arkaluonteisia henkilötietoja, kuten niin kutsutussa Vastaamo-asiassa ja tietosuojavaltuutetun ratkaisemassa (15.11.2022, 4022/171/22) terveydenhuollon toimijan toimitusjohtajan varastetun tietokonelaukun -tapauksessa voidaan laiminlyöntien seurauksista nähdä.

Vastaamon tietomurto osoittaa konkreettisesti, miten puutteellinen tietoturva voi johtaa sekä yksilöiden vakavaan oikeuksien loukkaamiseen että laajamittaisiin yhteiskunnallisiin seurauksiin. Vastaamo sai tietosuojavaltuuteltua valtavat sakot ja yritys asetettiin myöhemmin myös konkurssiin. Laiminlyöntien seuraukset voivat olla siis sekä oikeudellisesti että taloudellisesti merkittäviä. Hallinnolliset seuraamusmaksut voivat nousta jopa kymmeniin miljooniin euroihin, minkä lisäksi rikosoikeudelliset seuraamukset, vahingonkorvausvastuu sekä maineen menettäminen voivat uhata koko organisaation toimintakykyä.[111] Tapaus on kirjoitushetkellä vielä hovioikeudessa kesken, mutta on selvää, että vaikutukset ovat valtavat myös yksilöllisellä tasolla rekisteröidyillä. Pelkkä pelko omasta turvallisuudesta ja sen heikkenemisestä voi vaikuttaa ihmisen hyvinvointiin ja luoda stigmaa henkilökohtaisten tietojen paljastumisesta.[112]

Ennakoiva riskienhallinta tarjoaa kuitenkin keinot näiden seurausten välttämiseen tai ennen kaikkea vähentämiseen. Tehokkaat tekniset ja organisatoriset suojaustoimet, henkilöstön koulutus ja tietoisuuden vahvistaminen sekä säännölliset auditoinnit luovat

[111] TSV 07.12.2021, dnro 1150/161/2021
[112] C-340/21, 2023, luku IV ratkaisuehdotus

perustan tietoturvalliselle toimintakulttuurille. Keskeistä on, että organisaatiot ymmärtävät tietosuojan liittyvän paitsi yksityiselämän suojaan myös laajempiin perus- ja ihmisoikeuksiin sekä yhteiskunnan kokonaisturvallisuuteen.

Itä-Suomen hallinto-oikeuden (27.9.2023, 2139/2023) [113] ratkaisu Findatan vaatimuksesta siirtää tutkimusaineisto tietoturvalliseen käyttöympäristöön osoittaa, että riskienhallinta edellyttää myös lainsäädännön aktiivista seuraamista ja sen muutoksiin reagoimista. Toisiolain soveltaminen takautuvasti aiempiin lupiin perustuvaan aineistoon korosti sitä, että riskienhallinta ei rajoitu vain teknisiin ja organisatorisiin suojauksiin, vaan kattaa myös velvoitteen mukauttaa toiminta uuteen sääntelyyn yksityiselämän suojan ja perusoikeuksien turvaamiseksi. Näin riskiä arvioidaan jatkuvana prosessina, kuten esimerkiksi tietosuoja-asetuksen 32 artikla edellyttää.

Vastaamon tietomurto olisi voitu estää, jos riskien arviointi olisi ollut jatkuvaa ja järjestelmän suojausten puutteet havaittu ajoissa. Johto olisi voinut varmistaa auditoinneilla ja aktiivisella valvonnalla, että perustason tekniset suojaukset, kuten salaus ja pääsynhallinta, olivat kunnossa, mikä olisi estänyt vuosia jatkuneet haavoittuvuudet. [114] Tietokonelaukun katoamistapauksessa taas ennakointi olisi tarkoittanut käytännön suojatoimia, kuten kannettavan tietokoneen ja kiintolevyjen vahvaa salausta sekä ohjeistusta siitä, miten paperimuotoisia asiakirjoja saa kuljettaa. Jos henkilöstö olisi koulutettu tietoturvasta ja riskien seuraukset arvioitu etukäteen, yli 3 000 henkilön terveystiedot eivät olisi joutuneet vaaralle alttiiksi.[115]

Riskienhallinnan vaikuttavuus edellyttää riittävää resursointia ja laaja-alaista yhteistyötä julkisen hallinnon, yritysten ja muiden toimijoiden välillä. Nykyiset resurssit kyberturvallisuudessa eivät vielä vastaa tarpeita, ja henkilötietojen

[113] Itä-Suomen HAO 27.09.2023, dnro 2139/2023
[114] TSV 07.12.2021, dnro 1150/161/2021
[115] TSV 15.11.2022, dnro 4022/171/22

tietoturvaloukkaukset voivat merkittävästi heikentää ihmisten hyvinvointia ja yhteiskunnan luottamusta. [116]Tietosuoja-asetuksen periaatelähtöisyys, niukka ohjeistus ja puutteellinen oikeuskäytäntö vaikeuttavat organisaatioiden työtä, ja abstraktit sääntelyilmaisut jäävät helposti vaikeaselkoisiksi. [117] Erityisesti julkinen sektori kokee tietosuojavelvoitteet kuormittavina. Tietosuoja-asetuksen, kansallisen lain ja erityislakien kokonaisuus on monimutkainen ja pirstaleinen, mikä vaikeuttaa sääntelyn soveltamista ja yhteensovittamista esimerkiksi julkisuuslain kanssa. [118] Henkilötietopyyntöihin vastaaminen ja eri viranomaisten toimivaltuudet aiheuttavat epätietoisuutta, mikä voi johtaa ylivarovaiseen toimintaan.[119] Koska suurin osa henkilötietojen käsittelystä on digitaalista, tietoturvalla on keskeinen merkitys yksityisyyden ja tietosuojan toteutumisessa. Tietoturvaloukkaukset muodostavat merkittävän osan tietosuojakritiikistä ja korostuvat myös viranomaisten ratkaisukäytännössä.[120]

Tutkimukseni tarkastelee jatkuvasti muuttuvaa ilmiötä, jossa maailmanpoliittinen tilanne ja teknologian nopea kehitys synnyttävät uusia, entistä monimutkaisempia riskienhallinnan ja tietoturvan haasteita. Tämä edellyttää sekä lainsäätäjiltä että organisaatioilta proaktiivista otetta, jotta tietoturvakäytännöt voivat vastata muuttuviin uhkiin ajantasaisesti ja ennakoivasti. Tutkimus nostaa esiin tarpeen syventää ymmärrystä siitä, miten lainsäädäntö, organisaatiotason riskienhallinta ja teknologiset ratkaisut voidaan sovittaa yhteen kestäväksi kokonaisuudeksi. Jatkotutkimukselle on erityisen paljon tilaa ennakoivien mekanismien kehittämisessä, jotta uhkiin voidaan reagoida ennen niiden kriisiytymistä.

[116] Valtioneuvoston kanslia 2024, s. 29, 40
[117] Lång ja Taka, 2019, s. 71
[118] Kantonen ja Pohjalainen, 2024, s. 11
[119] Korpisaari ym., 2022, s. 3
[120] Keller, 2023, s. 56

Lähteet

Andersson, J. (2018). Kyberrikokset tuomioistuimissa – tarkastelussa rikoslain 38 luvun mukaiset tieto- ja viestintärikokset. *Edilex 2018/4*. Noudettu 8.6.2025 osoitteesta https://www-edilex-fi.proxy.uwasa.fi/artikkelit/18528.pdf

Andersson, J. (2024). Organisaation hyvä tietoturvan sääntelyjärjestelmä. Noudettu 21.8.2025 osoitteesta https://osuva.uwasa.fi/server/api/core/bitstreams/c8164e24-6384-4352-ba90-56da7d703f5d/content

Akatyev, N.; Han, C.; Hwang, J.; Jang, Y.; Kim, D.; Kim, J.; Park, S.; Shin, H. & Yu, W. (2018). A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. Digital Investigation, vol. 24, Supplement, March 2018. s. 93–100, DFRWS 2018 Europe – Proceedings of the Fifth Annual DFRWS Europe. Elsevier Ltd. 2018. Noudettu 18.8.2025 osoitteesta https://doi.org/10.1016/j.diin.2018.01.012

Ghanbari, H., & Koskinen, K. (2024, heinäkuuta 6). When data breach hits a psychotherapy clinic: The Vastaamo case. *Journal of information technology teaching cases.* Noudettu 3.8.2025 osoitteesta https://journals-sagepub-com.proxy.uwasa.fi/doi/epdf/10.1177/20438869241258235

Hautamäki, V.-P. (2004). *Hyvän hallinnon toteuttaminen*. Edita. Noudettu 5.6.2025 osoitteesta https://www-edilex-fi.proxy.uwasa.fi/artikkelit/2680.pdf

Järvinen, P. (2022). *Yrityksen tietoturvaopas*. Kauppakamari. Noudettu 30.7.72025 osoitteesta https://kauppakamaritieto-fi.proxy.uwasa.fi/ammattikirjasto/teos/yrityksen-tietoturvaopas-2022#kohta:Yrityksen((20)tietoturvaopas

Kantonen, S., & Pohjalainen, A. (2024). EU:n yleisen tietosuoja-asetuksen soveltamiskokemuksia Suomessa. Lausuntotiivistelmä. *Oikeusministeriö*. Noudettu 4.6.2025 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165679/OM_2024_18_ML.pdf

Keller, M. (2023). Mitä on tietosuoja. Alma Talent. Noudettu 30.7.2025 osoitteesta https://verkkokirjahylly.almainsights.fi/teos/CACBIXETEB#kohta:Mit((e4)((20)on((20)tietosuoja?/piste:txE

Korpisaari, P., Pitkänen, O., & Warma-Lehtinen, E. (2022). *Tietosuoja*. Alma Talent. Noudettu 30.7.2025 osoitteesta https://verkkokirjahylly.almainsights.fi/teos/CAIBCXETEB#/kohta:Johdanto/piste:tJDO

Looi, J. C., Allison, S., Bastiampillai, T., Maguire, P. A., Kisely, S., Reutens, S., & Looi, R. C. (2025, helmikuuta). Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers. *Australasian psychiatry: bulletin of the Royal Australian and New Zealand College of Psychiatrists*, 106–110. Noudettu 3.8.2025 osoitteesta https://journals.sagepub.com/doi/pdf/10.1177/10398562241291340

Lång, J., & Taka, A.-M. (2019). *TIETOSUOJA-ASETUKSEN SOVELTAMINEN KÄYTÄNNÖSSÄ – KATSAUS ENSIMMÄISEEN VUOTEEN*. 55–74. Noudettu 5.6.2025 osoitteesta https://www-edilex-fi.proxy.uwasa.fi/viestintaoikeuden-vuosikirja/201870004.pdf

Oikarinen, T. (2023). Julkisen hallinnon tietohallinnon suunnitteluvelvoitteet. *Edilex*, 255–328. Noudettu 7.6.2025 osoitteesta https://www-edilex-fi.proxy.uwasa.fi/oikeustiede/199860004.pdf

Paasonen, J., Lindfors, H., & Vainio, J. (2022). *Turvallisuusselvitys vai turha selvitys?* 962–980. Noudettu 8.6.2025 https://www-edilex-fi.proxy.uwasa.fi/defensor_legis/1000850006.pdf

Paasonen, J., Luomala, M., & Aaltonen, M. (2021). Kyberrikokset tuomioistuimissa – tarkastelussa rikoslain 38 luvun mukaiset tieto- ja viestintärikokset. *DEFENSOR LEGIS*, 966–987. Noudettu 8.6.2025 osoitteesta https://www-edilex-fi.proxy.uwasa.fi/defensor_legis/250670013.pdf

Rautiainen, P., Kostiainen, A., Kurki, V., Soininen, N., & Määttä, T. (2023). *Oikeus ja sen tutkiminen*. Tampere: Vastapaino. Noudettu 3.6.2025 osoitteesta https://www.ellibslibrary.com/reader/9789523971127

Rousku, K. (2017, toukokuuta 7). *Ohje riskienhallintaan*. Valtiovarainministeriö. Noudettu 30.5.2025 osoitteesta http://urn.fi/URN:ISBN:978-952-251-862-0

Seppänen, J. (2024). *RISKIN KÄSITTEEN JA OIKEUDELLISEN SÄÄNTELYN SUHDE OIKEUSTEOREETTISENA KYSYMYKSENÄ*. Noudettu 30.5.2025 osoitteesta https://www.edilex.fi/artikkelit/100006.pdf

Tuori, K. (2007). *Oikeuden ratio ja voluntas*. Noudettu 30.5.2025 osoitteesta https://verkkokirjahylly-almainsights-fi.proxy.uwasa.fi/teos/JAIBHXCTDG#kohta:74

Valtioneuvosto. (2024). *Suomen kyberturvallisuusstrategia 2024–2035.* Noudettu 6.6.2025 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165860/VNK_2024_11.pdf?sequence=1&isAllowed=y

Valtioneuvosto. (2024). *Valtioneuvoston päätös huoltovarmuuden tavoitteista 568/2024*. (2024, lokakuuta 29). Noudettu 30.7.2025 osoitteesta https://www.finlex.fi/api/media/statute/2024/mainPdf/main.pdf?timestamp=2024-10-24T00%3A00%3A00.000Z

Voutilainen, T. (2006). *HYVÄ TIETOHALLINTO JA SEN SÄÄNTELY VIRANOMAISTOIMINNASSA*. Noudettu 30.5.2025 osoitteesta https://www-edilex-fi.proxy.uwasa.fi/artikkelit/3648.pdf

Virallislähteet

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

HE 27/2025 vp. Hallituksen esitys edukunnalle laieksi kyberturvallisuuslain ja julkisen hallinnon tiedonhallinnasta annetun lain 3 §:n muuttamisesta

HE 284/2018 vp. Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi

HE 4/2023 vp. Hallituksen esitys eduskunnalle tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen ja turvallisuussääntöjen

hyväksymiseksi ja voimaansaattamiseksi sekä Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanomiseksi

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

HE 59/2002 vp. Hallituksen esitys Eduskunnalle työturvallisuuslaiksi ja eräiksi siihen liittyviksi laeiksi

HE 30/1998 vp. Hallituksen esitys Eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi

HE 1/1998 vp. Hallituksen esitys Eduskunnalle uudeksi Suomen Hallitusmuodoksi

HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta

HE 48/2008 vp. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta

HaVM 13/2018 vp.

Oikeustapaukset

EUT tapaus VB v. Natsionalna agentsia za prihodite (14.12.2023).

Ylimpien laillisuusvalvojien ratkaisut

EOAK/2261/2023 7.11.2024

TSV 07.12.2021, dnro 1150/161/2021

TSV 15.11.2022, dnro 4022/171/22

Itä-Suomen HAO 27.09.2023, dnro 2139/2023